REGLAMENTO DE EVIDENCIAS DIGITALES DEL EXCELENTÍSIMO AYUNTAMIENTO DE CARTAGENA

EXPOSICIÓN DE MOTIVOS

En los actuales entornos digitales se generan miles de datos de manera permanente, algunos reglados y bien conocidos; otros aleatorios, automatizados y no siempre bajo control. Todos ellos son susceptibles de constituir evidencia digital, es decir, información que puede ser utilizada a efectos de auditoría interna o, si procede, como testimonio ante un tribunal. Por ello, procede codificar adecuadamente los mecanismos para su producción, en el caso de datos reglados; para su identificación, tanto en el caso de datos reglados como no reglados; para su gestión y conservación, cuando resulte pertinente; y para el tratamiento preventivo y reactivo de los mismos, si éstos quedan puestos en un compromiso derivado, ya del propio funcionamiento habitual de los entornos digitales contemporáneos, ya de actuaciones inintencionadas o maliciosas orientadas a destruir tales datos, o al menos a cuestionar la validez de los mismos.

El legislador ha sido cuidadoso al respecto, previendo la gestión y la conservación de evidencias digitales, tanto en 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, modificado por el 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; como en el 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. Fuera del

Edificio Administrativo
C/. San Miguel nº 8
C.P. 30201
Teléfono 968128872

ámbito legislativo, el Centro Criptológico Nacional ha publicado varias guías enfocadas sobre la utilización de buenas prácticas en la gestión de evidencias digitales y las organizaciones dedicadas a la publicación de normas de mercado, como la Organización Internacional de Normalización (ISO) o la Asociación Española de Normalización y Certificación (Aenor) han sido exhaustivas al respecto.

Puesto que una adecuada identificación, gestión, tratamiento y conservación de las evidencias digitales generadas por las actuales tecnologías de la información y de las comunicaciones, así como de los peligros que las acechan, resulta esencial como testimonio de los derechos y las obligaciones de las organizaciones y para la defensa de sus intereses, el Ayuntamiento de Cartagena, sobre la base de las disposiciones y normas técnicas mencionadas, se dota del pertinente mecanismo reglamentario, que debe servir para abordar del mejor modo posible esta nueva realidad que a todos nos envuelve. De manera muy precisa, dada la complejidad de la misma, el presente Reglamento toma en consideración el hecho de que la responsabilidad de la gestión de las evidencias digitales no puede recaer sólo sobre una persona, un cargo, un órgano o una unidad, por lo que, haciendo uso del principio de diferenciación funcional, articula un conjunto de equipos interdisciplinares y colaborativos, que a su vez serán objeto de aprobación reglada.

El presente Reglamento se estructura en cuatro capítulos, tres disposiciones adicionales, una disposición final, un anexo de carácter normativo y un apartado de referencias bibliográficas. El primer capítulo – Disposiciones generales – codifica el objeto y el alcance del presente Reglamento, así como sus límites y sus ámbitos

subjetivos y objetivos de aplicación. De igual modo, define el concepto de evidencia digital y su tipología en el contexto del Ayuntamiento de Cartagena.

El segundo capítulo – El Esquema Institucional de Metadatos – establece la obligatoriedad del mismo, en tanto mecanismo reglado de generación de evidencias digitales, con base en el artículo 27 del "Reglamento de Política de Gestión de Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena". También se aplica a la articulación del procedimiento para la definición de un perfil de aplicación en el Ayuntamiento del Esquema de Metadatos para la Gestión de Documentos Electrónicos (e-EMGDE) de la Administración General del Estado.

El tercer capítulo – La auditoría de seguridad – responde a lo preceptuado en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, proponiendo por tanto los mecanismos que deben regir la recogida de evidencias digitales a efectos de auditoría de seguridad en el Ayuntamiento y sus entidades vinculadas o dependientes.

El cuarto capítulo – La gestión de ciberincidentes – define los mecanismos que deben estar en vigor para recolectar evidencias digitales en los supuestos de situaciones anormales, inintencionadas o maliciosas, y de ataques a los sistemas de información del Ayuntamiento. De igual modo, define los procedimientos para diseminar y conservar tales evidencias.

La Disposición Adicional Primera armoniza la auditoría de seguridad codificada en el artículo 34 del Real Decreto mencionado con la prevista en el 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. La Disposición Adicional Segunda prevé un plan de formación para los empleados municipales. La Disposición Adicional Tercera incorpora al Glosario de Administración Electrónica reglado en la "Ordenanza Municipal de Administración Electrónica del Excmo. Ayuntamiento de Cartagena" la terminología utilizada en el presente Reglamento.

La Disposición Final identifica el procedimiento de modificación y revisión del presente Reglamento, así como su fecha de entrada en vigor.

Por último, en Anexo I, de carácter normativo, se formula el modelo de cláusula de confidencialidad que deben suscribir las personas o las organizaciones implicadas en el tratamiento de evidencias digitales.

Las referencias bibliográficas recogen los textos que se han utilizado para la redacción del presente Reglamento.

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. Es objeto del presente Reglamento definir y ordenar el modo en que se producen, gestionan y mantienen evidencias digitales en el ámbito del Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes, con el fin de dejar traza identificable de todas las actuaciones que se ejecutan en

entornos electrónicos, de tal modo que, de ser preciso, puedan ser utilizadas ante un tribunal o con otros fines de auditoría interna o externa.

2. Quedan fuera del alcance del presente Reglamento las prácticas para la determinación de evidencia con fines forenses, en la medida en la que no forman parte del ámbito competencial del Ayuntamiento y sus entidades vinculadas o dependientes, ello sin perjuicio del deber de cooperación con las administraciones competentes.

3. El presente Reglamento se promulga para dar satisfacción a lo previsto en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como en los Anexos II y III del mismo. De igual modo, da satisfacción a lo previsto en el artículo 22.4 del 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 y a lo preceptuado en el artículo 2.5 del "Reglamento sobre Política de Firma y Sello Electrónicos y de Certificados del Excelentísimo Ayuntamiento de Cartagena".

Artículo 2. Ámbito de aplicación subjetivo.

El presente Reglamento será de aplicación a las entidades que integran la Administración Municipal:

a) Los órganos administrativos del Ayuntamiento de Cartagena.

b) Cualesquiera organismos públicos y entidades de derecho público vinculados al Ayuntamiento de Cartagena o dependientes del mismo.

c) Las entidades de derecho privado vinculadas al Ayuntamiento de Cartagena o dependientes del mismo, que quedarán sujetas a lo dispuesto en las normas del presente Reglamento que específicamente se refieran a las mismas y, en todo caso, cuando ejerzan potestades administrativas.

Artículo 3. Ámbito de aplicación objetivo.

El presente Reglamento se aplicará a todos aquellos servicios, productos, plataformas, procesos, dispositivos y otros canales y medios electrónicos en uso en el Ayuntamiento y sus entidades vinculadas o dependientes.

Artículo 4. Definiciones.

1. A los efectos del presente Reglamento se entiende por evidencia digital la información o los datos, almacenados o transmitidos en formato binario, y en los que se puede confiar como evidencia ante un tribunal o con fines de auditoría.

2. A los efectos del presente Reglamento, la evidencia digital puede ser de dos tipos:

    a) Evidencia generada en el curso normal de los procesos electrónicos del Ayuntamiento y sus entidades vinculadas o dependientes. Esta evidencia queda recogida en el Esquema Institucional de Metadatos previsto en el artículo 27 del "Reglamento de Política de Gestión de

Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena". La suma de todos los historiales de eventos de todas las entidades que participan en las aplicaciones, plataformas y servicios del Ayuntamiento y sus entidades vinculadas o dependientes constituye la pista de auditoría del Ayuntamiento, que tiene carácter obligatorio e inmodificable. Las aplicaciones, plataformas y servicios que no dispongan de tal pista de auditoría habrá de adecuarse a lo dispuesto en el presente Reglamento o ser reemplazadas.

b) Evidencia generada por acontecimientos fuera de la normalidad, inintencionados o maliciosos, en el transcurso del funcionamiento del Ayuntamiento y sus entidades vinculadas o dependientes. Esta evidencia queda recogida, además de en el Esquema Institucional de Metadatos mencionado en el apartado anterior, en las pistas de auditoría de los sistemas informáticos en uso en el Ayuntamiento y sus entidades vinculadas o dependientes, en las bitácoras y los ficheros de log de los mismos, y en cualquier otro soporte o dispositivo en el que quede traza del anormal acontecimiento que debe ser auditado e investigado. Los sistemas que no recojan traza de lo acontecido habrán de adecuarse a lo dispuesto en el presente Reglamento o ser reemplazados.

CAPÍTULO II

El Esquema Institucional de Metadatos

Artículo 5. El Esquema Institucional de Metadatos.

1. El Esquema Institucional de Metadatos del Ayuntamiento de Cartagena es el instrumento de que éste se dota para generar y mantener información acerca del contenido, el contexto, la estructura, el comportamiento y la apariencia de los documentos y otros objetos digitales, a efectos de una mejor gestión de los mismos y, en consecuencia, de una recolección más detallada de evidencia acerca de las circunstancias de su producción, gestión y conservación.

2. De conformidad con lo previsto en el previsto en el artículo 27 del "Reglamento de Política de Gestión de Documentos Electrónicos del Excelentísimo Ayuntamiento de Cartagena", el Esquema Institucional de Metadatos estará basado en el Esquema de Metadatos para la Gestión de Documentos Electrónicos (e-EMGDE), de la Administración General del Estado, del cual se elaborará un perfil de aplicación de obligado cumplimiento por todas las unidades del Ayuntamiento y de sus entidades vinculadas o dependientes.

3. Los metadatos de historial de eventos de todas las entidades que pueblan los sistemas en uso en el Ayuntamiento y sus entidades vinculadas o dependientes constituyen la pista de auditoría de tales sistemas, de modo que deben permanecer inalterados y estar sujetos a especial protección.

4. De la elaboración del perfil de aplicación del Esquema Institucional de Metadatos se ocupará un grupo de trabajo compuesto por los técnicos en tecnologías de la información y de las comunicaciones propuestos por los servicios pertinentes y designados por la Alcaldía o quien tenga las

competencias delegadas en materia de Administración Electrónica, y por Letrado municipal, Técnico de Administración General y Técnico en Administración electrónica pertenecientes al Grupo de Proyecto para el Impulso de la Administración Electrónica regulado en la "Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena". A meros efectos informativos y con el único objeto de facilitar la redacción del perfil de aplicación por parte de dicho grupo de trabajo, será de aplicación el Esquema de Metadatos para la Gestión del Documento Electrónico de la Administración General del Estado.

5. El Esquema Institucional de Metadatos se revisará con una periodicidad al menos anual y siempre que la evolución de las tecnologías de la información y de las comunicaciones así lo aconseje.

CAPÍTULO III

La auditoría de seguridad

Artículo 6. Desarrollo y ejecución de la auditoría.

1. La auditoría debe realizarse de una forma metodológica que permita identificar claramente:

    a) El alcance y objetivo de la misma.

    b) Los recursos necesarios y apropiados para su realización.

c) Las debidas comunicaciones con los órganos del Ayuntamiento y de sus entidades vinculadas o dependientes que soliciten la auditoría, si ésta no se lleva a cabo de oficio.

d) La planificación preliminar o los requisitos de información previos al desarrollo del programa de auditoría, y a la ejecución de las pruebas que se consideren necesarias.

e) El establecimiento de un programa detallado de auditoría con las revisiones y pruebas de auditoría previstas.

f) La presentación de los resultados individuales de las pruebas a las personas involucradas en estos resultados, para su confirmación sin valoraciones con respecto a los resultados finales.

g) La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos 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.

h) La confección, presentación y emisión formal del Informe de Auditoría.

2. 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.

3. Para una consecución eficaz de la auditoría, el equipo auditor verificará que las medidas de seguridad para el sistema auditado se ajustan a lo preceptuado en los artículos 4 y 11 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.

Artículo 7. Definición del alcance y objetivo de la auditoría.

1. El alcance y el objetivo de la auditoría deben estar claramente definidos, documentados y consensuados entre el equipo auditor y el órgano del Ayuntamiento o de sus entidades vinculadas o dependientes que la haya solicitado, si ésta no se lleva a cabo de oficio.

2. Habida cuenta de que las redes de comunicaciones y sistemas del Ayuntamiento y sus entidades vinculadas o dependientes tienen interconexiones con entidades públicas y privadas, debe definirse claramente el alcance de la auditoría y el límite de la misma.

3. Como parte de la definición del alcance de la auditoría, deben identificarse los elementos organizativos, físicos y lógicos que abarca, incluidos:

    a) Política de Seguridad.

    b) Valoración de la información y los servicios, junto con la determinación de la categoría del sistema.

    c) Política de Firma y Sello Electrónicos y Certificados, y servicios que utilizan estas técnicas.

d) Información, servicios y demás recursos sujetos a la auditoría.

e) Tipo de datos que se manejan así como la normativa que les sea de aplicación.

f) Órgano responsable y personal afectado por la auditoría.

g) Conexiones externas con otros organismos públicos o privados.

h) Legislación que afecta al sistema de información auditado.

4. Si existe alguna información que, por indicación del Responsable del Sistema, del Servicio o del de Seguridad, no está accesible a los auditores, y ni siquiera al Jefe del equipo de auditoría, éste debe evaluar si ello supone una limitación para realizar la auditoría. Si es así, y se decide continuar con el proceso de auditoría, esta limitación debe reflejarse en el Informe de Auditoría.

5. 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 para el cumplimiento del Esquema Nacional de Seguridad, procedimientos de actuación, o posibles recomendaciones de productos concretos de software, entre otros.

Artículo 8. El equipo auditor.

1. 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 suficientes para asegurar la adecuada y ajustada realización de la auditoría.

2. El equipo de auditores deberá estar dirigido y tutelado siempre por un Jefe del equipo de auditoría, cuyas funciones principales son la supervisión de todo el proceso de auditoría, la garantía de la exactitud de los hechos, la adecuación de las recomendaciones mencionadas en el Informe de Auditoría y la preservación de las evidencias de la misma.

3. El Jefe del equipo de auditoría, responsable de gestionar las tareas de auditoría, deberá probar como mínimo:

    a) 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 de al menos cuatro años, en auditoría de tecnologías de la información.

    b) Conocimientos de seguridad y gestión de riesgos de seguridad, mediante certificación o experiencia probada de al menos cuatro años en estos elementos.

    c) Conocimiento de los requisitos establecidos en 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.

d) 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 del 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, entre otros.

4. El resto del equipo puede no cumplir con los requisitos definidos 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 de la asignación de tareas al resto del equipo, incluidos los expertos, corresponde al Ayuntamiento, o en su caso a la organización privada o pública que aporte el equipo de auditoría, previo informe del Jefe del equipo.

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 conforme con el "Reglamento de Protección de Datos del Excelentísimo Ayuntamiento de Cartagena" y según modelo que figura en Anexo I, de carácter normativo, del presente Reglamento.

6. Dado el carácter interdisciplinar de la auditoría, el equipo auditor debe contar al menos con los siguientes perfiles:

   a) Un experto en tecnologías de la información y las comunicaciones.

   b) Un experto con conocimientos jurídicos.

c) Un experto en Procedimiento Administrativo.

d) Un experto en administración electrónica, gestión de documentos electrónicos y conservación a largo plazo.

e) Cualquier otro que el Jefe del equipo de auditoría estime pertinente en función del sistema auditado.

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

a) Si el equipo de auditoría es interno, éste deberá ofrecer garantía suficiente y demostrable de su independencia y objetividad.

b) 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 de Auditoría, y consecuentemente, de los resultados de la misma. El programa de auditoría debe establecer con claridad la responsabilidad y asignación de las funciones de cada integrante del equipo auditor.

c) Sean auditores externos o internos, o un equipo mixto, la propiedad de los documentos de trabajo y de las evidencias, así como la responsabilidad de la emisión del Informe de Auditoría y su contenido deben ser siempre inequívocas, tanto en la apertura de la auditoría, como en su informe final. En cualquier caso, la propiedad de los

documentos de trabajo y de las evidencias corresponderá al Ayuntamiento.

d) Si la realización de la auditoría ha sido encargada a un equipo externo, privado o público, los integrantes deberán firmar las preceptivas cláusulas de confidencialidad, incluyendo las cláusulas aplicables de la legislación de protección de datos de carácter personal, de conformidad con el modelo que se incluye en el Anexo I, de carácter normativo, del presente Reglamento.

e) Si la auditoría es liderada por un equipo de auditoría interna, pero con la incorporación de expertos independientes, éstos también deben firmar dicha cláusula de confidencialidad.

8. 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 autenticidad, fiabilidad, exactitud, integridad, identidad, completitud, disponibilidad, confidencialidad y trazabilidad de la información tratada, almacenada o transmitida por el sistema auditado. Por tanto, cualquier componente del sistema que pueda ofrecer traza de que las mencionadas propiedades de la información existen o, por el contrario, han sido puestas en compromiso, debe ser objeto de examen y éste debe quedar documentado en el Informe de Auditoría.

Artículo 9. Planificación preliminar de la auditoría.

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

    a) Establecer y desarrollar el programa de auditoría.

    b) Concretar los conocimientos necesarios del equipo de auditoría.

    c) Definir la agenda de revisiones, reuniones y entrevistas.

    d) Definir las revisiones y pruebas a realizar.

    e) Adjudicar las tareas a los componentes del equipo de auditores y expertos.

2. Si se realiza una auditoría conjunta con la requerida por los artículos 96 y 110 del 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, se debe identificar qué medidas de seguridad entran en el alcance de esta última.

3. La documentación mínima a requerir para concretar la planificación en detalle de la auditoría es:

    a) Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.

b) Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.

c) Identificación de los responsables de la información, de los servicios, de la seguridad y del sistema.

d) Descripción detallada del sistema de información a auditar: software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares.

e) Identificación de la categoría del sistema según el Anexo I 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.

f) Niveles de seguridad definidos.

g) Política de Seguridad.

h) Política de Firma y Sello Electrónicos y de Certificados de la Administración, si se emplean estas tecnologías.

i) Normativa de seguridad.

j) Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.

k) Informes de análisis de riesgos.

l) Declaración de Aplicabilidad.

m) Decisiones adoptadas para gestionar los riesgos.

n) Relación de las medidas de seguridad implantadas.

o) Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas.

p) 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.

q) Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.

r) 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.

4. 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 tales responsables.

5. 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.

Artículo 10. Programa de auditoría.

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

    a) Los criterios organizativos del órgano responsable del sistema auditado y la descripción de las funciones del personal afectado por este sistema.

    b) Los elementos de la seguridad que pueden auditarse mediante la revisión de documentación, observación, o entrevistas.

    c) El Documento de Seguridad previsto en el Reglamento de Protección de Datos y Documento de Seguridad del Excelentísimo Ayuntamiento de Cartagena.

    d) La selección de medidas de seguridad a verificar en cuanto a su cumplimiento tal y como han sido aprobadas.

    e) Las revisiones que deben 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. 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.

f) Las evidencias que se espera obtener en cada prueba y cuáles son ineludibles para documentar la realización de la prueba.

g) 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.

2. Si existen informes recientes de auditorías previas, internas o externas, que hayan incluido la revisión de elementos afectados por la auditoría en curso, éstos podrán considerarse en la planificación y no repetir pruebas, siempre y cuando:

   a) 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.

   b) Estas auditorías previas hayan tenido el grado de independencia objetiva y cualificación, similar al requerido para la realización de la auditoría prevista en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Los elementos a incluir en la planificación de la auditoría, como elementos mínimos a considerar, son los siguientes, teniendo como referencia el Anexo II del Real Decreto mencionado en el apartado anterior:

    a) Análisis y gestión de riesgos, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: sustentación metodológica del análisis de riesgos realizado, su coherencia y documentación, y verificación del inventario de activos. A tal fin se hará uso de una metodología contrastada a nivel nacional o internacional, de la que se dará cuenta explícita.

    b) El marco organizativo y la segregación de funciones, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: 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 por tales normas, y por políticas y procedimientos. A los efectos de una evaluación más representativa, se debe entrevistar no sólo a cargos jerárquicos, sino también a otro personal de forma aleatoria.

    c) El marco operacional: control de accesos, explotación, servicios externos, continuidad del servicio, y monitorización del sistema, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: evaluación 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.

d) La Declaración de Aplicabilidad que recoge las medidas de seguridad del Anexo II del Real Decreto mencionado en el apartado anterior que son relevantes para el sistema de información sujeto a la auditoría, cuyos tipos de pruebas podrán ser, de manera no exhaustiva: 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.

e) Los procesos de mejora continuada de la seguridad, cuyos tipos de prueba podrán ser, de manera no exhaustiva: evaluación del ciclo de madurez del sistema de gestión de la seguridad del sistema de información auditado, criterios para la revisión y agenda de mejoras.

f) La aplicación de los modelos de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes, de conformidad con lo previsto en el Anexo V del Real Decreto mencionado en el apartado anterior y en la Disposición adicional segunda de la Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena, según una muestra seleccionada de éstos.

4. Para definir la tipología de pruebas a realizar, el equipo auditor podrá utilizar guías y cuestionarios de auditoría disponibles en asociaciones y colectivos de auditores, y las guías STIC proporcionadas por el Centro Criptológico Nacional que sean de aplicación al sistema auditado.

5. 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:

    a) Lista del personal que ha dejado el organismo recientemente.

    b) Copia del registro de incidencias.

    c) Copia del registro de actividad de los usuarios.

    d) Registros de formación del personal afectado por el sistema auditado.

6. 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.

Artículo 11. Revisiones y pruebas de auditoría.

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

    a) 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.

b) 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 la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, en relación a la evidencia a la que deban servir a efectos de verificación.

c) La muestra seleccionada de medidas o documentación debe ser suficiente y relevante para satisfacer el 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.

d) 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 en 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 y si previenen realmente los riesgos identificados en el análisis de riesgos.

e) 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.

f) Las entrevistas no se plantearán de forma inductiva, sino abierta. Es decir, no se deben realizar preguntas donde la respuesta, afirmativa o negativa según el caso, esté implícita en la pregunta.

g) Se ponderarán las respuestas de las entrevistas, pudiendo haber lugar a la realización de pruebas complementarias que no estaban previstas.

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

a) 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.

b) 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; o, si hay incidencias a incluir en el informe, se sustente claramente el incumplimiento persistente o una indiscutible deficiencia de seguridad, y no 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.

c) La revisión de documentación, incluido el análisis de riesgos, deberá documentarse con las conclusiones de la revisión, y las posibles aclaraciones recibidas posteriormente.

d) Las conclusiones, o la información recogida en una entrevista, para poder ser considerada como evidencias de auditoría, deberá ser plasmada en actas comunicadas a las personas entrevistadas.

e) Los correos electrónicos, en la medida que involucren a varias personas dentro del alcance de la auditoría, y se disponga del acuse de recibo, podrán servir, en determinados casos, como prueba de auditoría, previa autorización del titular de la cuenta o mediando orden judicial.

f) Las pruebas de observación, como las de seguridad física, deberán estar documentadas ya sea a través de fotografías, documentación similar, o comunicaciones escritas puntuales al Responsable de Seguridad.

g) 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.

h) 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 digitales, deberán someterse a las Normas Técnicas de Interoperabilidad que resulten de aplicación.

i) 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 de manera permanente, debidamente referenciados y archivados, así como custodiados y protegidos en el archivo electrónico único del Ayuntamiento.

Artículo 12. Elaboración y presentación de los resultados de revisiones y pruebas de auditoría.

1. 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.

2. Todos los resultados de pruebas, relacionados entre sí o que se refieran a una misma deficiencia o debilidad, serán agrupados para el informe, aun cuando se incluya un detalle de las deficiencias de forma individual, en un anexo al Informe de Auditoría.

3. En relación con los requisitos del Título VIII del 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, cuando haya una divergencia contrastable entre la aplicación de éstos y los 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, resultando un incumplimiento del primero, se debe indicar con claridad esta situación, ya que los requisitos del Real Decreto 1720/2007 son prioritarios, en la medida en la que desarrollan una ley orgánica.

4. Si bien el objetivo principal es la verificación del cumplimiento aceptable del Real Decreto 3/2010 mencionado en el apartado anterior, 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, como las identificadas en el Capítulo IV del presente Reglamento, deberá comunicarlo.

Artículo 13. Presentación del Informe de Auditoría.

1. Una vez confirmados los hechos y deficiencias resultado de las revisiones y pruebas de auditoría, deberá presentarse un Informe de Auditoría al Responsable del Sistema y al Responsable de Seguridad. 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.

2. 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.

3. El Informe de Auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el Real Decreto 3/2010 mencionado en el artículo anterior, 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.

4. El informe incluirá las no conformidades encontradas durante la realización de la auditoría.

5. El informe incluirá una opinión acerca de si:

    a) 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.

    b) Existen procedimientos para la resolución de conflictos entre dichos responsables.

    c) Se han designado personas para dichos roles a la luz del principio de separación de funciones.

    d) Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

e) Se ha realizado un análisis de riesgos, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del Real Decreto 3/2010 mencionado en el artículo anterior.

f) Se cumplen las medidas de seguridad descritas en el citado Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

g) Existe un sistema de gestión de mejora continua.

6. Si la auditoría se realizara conjuntamente con la requerida por los artículos 96 y 110 del 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, es necesario que el Informe indique con claridad cuándo una deficiencia de seguridad o incumplimiento, o una mejora recomendada está, individualmente, relacionada con ambas normas, o bien con una en concreto.

7. El Informe de Auditoría se podrá presentar en formato audiovisual. No obstante, este Informe siempre deberá entregarse en soporte electrónico y debidamente firmado. El esquema del Informe incluirá como mínimo:

a) Fecha de emisión del informe.

b) Una sección de alcance, limitaciones al alcance, y objetivo de la auditoría, con la debida identificación del sistema auditado.

c) Breve descripción del proceso metodológico aplicado para realizar la auditoría.

d) Identificación de la documentación revisada.

e) Identificación de la tipología de pruebas realizadas.

f) Las fechas de comienzo y final del trabajo de campo, ya sean reuniones o revisiones técnicas, realizado durante el proceso de auditoría.

g) 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.

h) 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.

8. 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.

9. 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 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.

10. 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.

11. 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.

12. 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.

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

CAPÍTULO IV

La gestión de ciberincidentes

Artículo 14. Definición de ciberincidente.

A los efectos del presente Reglamento, se entiende por ciberincidente toda acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información, la propia información que trata o los servicios que presta. Se trata, por tanto, de un incidente relacionado con la seguridad de las Tecnologías de la

Información y las Comunicaciones que se produce en el Ciberespacio. Sin ánimo de exhaustividad, pueden considerarse ciberincidentes circunstancias tales como los ataques a sistemas de tecnologías de la información y de las comunicaciones, el fraude electrónico, el robo de identidad, o el abuso del Ciberespacio.

Artículo 15. Gestión de ciberincidentes.

1. Un ciberincidente consta de las siguientes fases, cuya gestión es responsabilidad del Equipo de Respuesta a Ciberincidentes (ERC) que se formaliza en los apartados 2 a 4 del presente artículo:

    a) Fase de preparación: el Ayuntamiento debe contemplar la creación y formación de un Equipo de Respuesta a Ciberincidentes, y la utilización de las herramientas y recursos necesarios. Para ello, atendiendo a lo dispuesto en los Anexos I y II 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, y previo el correspondiente análisis de riesgos, deben haberse identificado y desplegado un determinado conjunto de medidas de seguridad, si bien también debe tomarse en consideración el hecho de que, incluso tras la implantación de tales medidas, persistirá un riesgo residual, o apetencia del riesgo, que también debe ser gestionado.

    b) Fase de detección, análisis y notificación: el Ayuntamiento debe implantar las antedichas medidas con el objeto de detectar posibles brechas de seguridad de los sistemas de información en el conjunto del

Ayuntamiento y sus entidades vinculadas o dependientes; así como para proceder a su análisis, en la fase de detección, análisis y notificación, desencadenando los procesos de notificación a los que hubiere lugar.

c) Fase de contención, erradicación y recuperación: ante la presencia de un ciberincidente, el Equipo de Respuesta a Ciberincidentes, atendiendo a la peligrosidad del mismo, deberá intentar, en primera instancia, mitigar su impacto, procediendo después a su eliminación de los sistemas afectados y tratando finalmente de recuperar el sistema al modo de funcionamiento normal. Durante esta fase se debe persistir cíclicamente en el análisis de la amenaza, de cuyos resultados se deben desprender paulatinamente nuevos mecanismos de contención y erradicación.

d) Fase de actividad post-ciberincidente: tras el ciberincidente, el Jefe del Equipo de Respuesta a Ciberincidentes, emitirá un informe a la Alcaldía o Concejal que tenga delegadas las competencias en Administración electrónica, sobre el Ciberincidente que detallará su causa originaria y su coste, especialmente en términos de compromiso de la información y de impacto en los servicios prestados, y las medidas que el Ayuntamiento debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

2. Para la adecuada gestión de las fases mencionadas se hará uso de la Guía CCN-STIC 403 Gestión de Incidentes de Seguridad.

3. El Ayuntamiento conformará un Equipo de Respuesta a Ciberincidentes, compuesto por técnicos en Tecnologías de la Información y de las Comunicaciones y en Administración Electrónica, así como por Letrado Consistorial, Técnico de Administración General y Técnico de Administración electrónica pertenecientes al Grupo de Proyecto para el impulso de la Administración electrónica, con las funciones que se derivan del presente Reglamento.

4. El Equipo de Respuesta a Ciberincidentes debe ser formalmente designado por resolución de Alcaldía o del Concejal competente en materia de Tecnologías de la Información y de las Comunicaciones y de Administración Electrónica.

5. El Equipo de Respuesta a Ciberincidentes estará dirigido por un Jefe de Equipo, cuyas funciones principales son la supervisión de todas las fases de gestión del ciberincidente, el informe post-ciberincidente y el aseguramiento de la comunicación continuada entre todos los miembros del Equipo, así como con terceras partes, si procede.

6. En todo caso, ante la sospecha de que un ciberincidente puede ocurrir, ha ocurrido o está ocurriendo, se informará al Sistema de Alerta Temprana de Red SARA (SAT- SARA) o al Sistema de Alerta Temprana de Internet (SAT-INET), del Centro Criptológico Nacional, según proceda.

Artículo 16. Clasificación de los ciberincidentes.

1. Los ciberincidentes se clasificarán de acuerdo con una taxonomía que tome en consideración como mínimo los siguientes factores:

a) Tipo de amenaza: código dañino, intrusiones, fraude, etc.

b) Origen de la amenaza: Interna o externa.

c) Categoría de seguridad de los sistemas afectados.

d) Perfil de los usuarios afectados, su posición en la estructura organizativa del Ayuntamiento y, en consecuencia, sus privilegios de acceso a información sensible o confidencial.

e) Número y tipología de los sistemas afectados.

f) Impacto que el incidente puede tener sobre el todo del Ayuntamiento y sus entidades vinculadas o dependientes, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y la imagen pública.

g) Requerimientos legales y reguladores.

2. El Jefe del Equipo de Respuesta a Ciberincidentes debe determinar, a partir de la combinación de uno o varios de estos factores, la decisión de crear un ciberincidente, su peligrosidad y las prioridades de actuación.

3. Todos los ciberincidentes detectados se clasificarán de acuerdo con la siguiente taxonomía:

CLASIFICACIÓN DE LOS CIBERINCIDENTES		
Clase de Ciberincidente	**Descripción**	**Tipo de ciberincidente**
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus
		Gusanos
		Troyanos
		Spyware
		Rootkit
		Ransomware (secuestro informático)
		Herramienta para Acceso Remoto (Remote Access Tool o RAT)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Denegación [Distribuida] del Servicio DoS / DDoS
		Fallo (Hardware/Software)
		Error humano
		Sabotaje

Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de vulnerabilidades (scanning)
		Sniffing
		Ingeniería social
		Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	Compromiso de cuenta de usuario
		Defacement (desfiguración)
		Cross-Site Scripting (XSS)
		Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados
		Inyección SQL
		Spear Phishing
		Pharming
		Ataque de fuerza bruta
		Inyección de Ficheros Remota
		Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware

Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información
		Modificación y borrado no autorizado de información
		Publicación no autorizada de información
		Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing
		Uso de recursos no autorizado
		Uso ilegítimo de credenciales
		Violaciones de derechos de propiedad intelectual o industrial
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura)
		Acoso/extorsión/ mensajes ofensivos
		Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por	Abuso de privilegios por usuarios

	violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Acceso a servicios no autorizados
		Sistema desactualizado
		Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	

Artículo 17. Detección de ciberincidentes.

1. Dada la dificultad para determinar con precisión en todos los casos si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad, el Jefe del Equipo de Respuesta a Ciberincidentes valorará dos tipos de fuentes, si se dispone de ellas: los precursores y los indicadores, entendiéndose como precursor un indicio de que puede ocurrir un incidente en el futuro; y como indicador un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

2. De igual modo, dado que la mayoría de los ataques no tienen precursores identificables o detectables, desde la perspectiva del objetivo, debe prestarse especial atención a precursores tales como las entradas en los ficheros de log de los servidores web, con los resultados de un escáner de vulnerabilidades; el anuncio de un nuevo fragmento de software o secuencia de comandos, dirigido a atacar una vulnerabilidad que podría estar presente en los sistemas del Ayuntamiento; o las amenazas explícitas procedentes de grupos o entidades concretos, anunciando ataques a organizaciones objetivo. En cualquier caso, tales fuentes no tienen carácter exhaustivo.

3. En ausencia de precursores identificables, se prestará también especial atención a la existencia de indicadores como el sensor de intrusión de una red, que emita una alerta cuando ha habido un intento de desbordamiento de búfer contra un servidor de base de datos; las alertas generadas por software antivirus; la presencia de un nombre de archivo con caracteres inusuales; un registro en los ficheros de log sobre un cambio no previsto en la configuración de un host; los ficheros de log de una aplicación; las advertencias de reiterados intentos fallidos de identificación desde un sistema externo desconocido; la detección de un número importante de correos electrónicos rebotados con contenido sospechoso; una desviación inusual del tráfico de la red interna, etc.

4. Puesto que la determinación de si un evento en particular es en realidad un ciberincidente constituye, en ocasiones, una cuestión de apreciación y juicio, debe intercambiarse la información del supuesto ciberincidente entre los diferentes miembros del Equipo de Respuesta a Ciberincidentes.

Artículo 18. Peligrosidad de los ciberincidentes.

1. Además de tipificar los ciberincidentes dentro de un determinado grupo o tipo, la gestión de los mismos exige determinar la peligrosidad potencial que el ciberincidente posee. Para ello, deben fijarse ciertos criterios de determinación de la peligrosidad con los que comparar las evidencias que se disponen del ciberincidente, en sus estadios iniciales.

2. A efectos del presente Reglamento, la peligrosidad de un ciberincidente dado se asignará a uno de una escala de cinco valores. Esta escala, de menor a mayor peligrosidad, es la que se muestra a continuación.

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

3. En lo que concierne al nivel de peligrosidad de los ciberincidentes, éste se determinará a partir de los criterios que se muestran en el siguiente cuadro.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	Ciberespionaje	- Amenazas Avanzadas Persistentes (APTs), campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa,en cantidad considerable y en poco tiempo.

MUY ALTO	**Interrupción de los Servicios de Tecnologías de la Información y las Comunicaciones / Exfiltración de datos / Compromiso de los servicios**	Códigos dañinos confirmados de Alto Impacto(RAT, troyanos enviando datos, rootkit, etc.) Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	**Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación**	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL.	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	**Logro o incremento significativo de capacidades ofensivas /** **Desfiguración de páginas web / Manipulación de información**	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP (Internet Protocol)sospechosas. - Escáneres de vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información . - Capacidad para tomar el control de algún sistema.

BAJO	**Ataques a la imagen / menosprecio / Errores y fallos**	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Artículo 19. Nivel de impacto del ciberincidente.

1. El impacto de un ciberincidente en el Ayuntamiento o sus entidades vinculadas o dependientes debe determinarse evaluando las consecuencias que tal ciberincidente ha tenido en sus funciones, en sus activos o en los individuos afectados. Por tanto, el Equipo de Respuesta a Ciberincidentes priorizará la gestión de los mismos de conformidad, aunque no de manera exclusiva, con los siguientes criterios:

    a) Impacto Funcional del Ciberincidente: El Equipo de Respuesta de Ciberincidentes debe considerar la forma en que el ciberincidente puede impactar en la funcionalidad de los sistemas afectados.

    b) Impacto del ciberincidente en la información o los servicios: Puesto que los ciberincidentes pueden afectar a la confidencialidad y la integridad de la información tratada por el Ayuntamiento o sus entidades vinculadas o dependientes, o a la disponibilidad de los servicios prestados, el Equipo de Respuesta a Ciberincidentes debe considerar el modo en que el ciberincidente puede impactar en el desenvolvimiento competencial del Ayuntamiento o en su imagen pública.

c) Recuperación del ciberincidente: Puesto que el tipo de ciberincidente y la superficie de activos atacada determinará el tiempo y los recursos que deben destinarse a la recuperación, el Equipo de Respuesta a Ciberincidentes, con la ayuda oportuna de otras unidades del Ayuntamiento, si procede, debe considerar el esfuerzo necesario para regresar a la situación pre-ciberincidente y su oportunidad.

2. Estos criterios pueden cambiar si en el transcurso del proceso de su gestión se modificasen las circunstancias o conocimiento que se tiene del ciberincidente.

3. El nivel de impacto potencial de un ciberincidente se determinará de conformidad con los criterios establecidos en el siguiente cuadro:

Nivel	Descripción
I0 – IRRELEVANTE	No hay impacto apreciable sobre elsistema No hay daños reputacionalesapreciables
I1 – BAJO	La categoría más alta de los sistemas de información afectadoses baja El ciberincidente precisa para resolverse menos de 1jornada/persona Daños reputacionales puntuales, sin ecomediático
I2 – MEDIO	La categoría más alta de los sistemas de información afectadoses media Afecta a más de 10 equipos con información cuya máximacategoría es baja El ciberincidente precisa para resolverse entre 1 y 10jornadas/persona Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios decomunicación)

I_3 – ALTO	La categoría más alta de los sistemas de información afectadoses alta Afecta a más de 50 equipos con información cuya máximacategoría es baja Afecta a más de 10 equipos con información cuya máximacategoría es media El ciberincidente precisa para resolverse entre 10 y 20jornadas/persona Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros
I_4 – MUY ALTO	Afecta a sistemas clasificados con nivel reservado Afecta a más de 100 equipos con información cuya máxima categoría es baja Afecta a más de 50 equipos con información cuya máximacategoría es media Afecta a más de 10 equipos con información cuya máximacategoría es alta El ciberincidente precisa para resolverse entre 20 y 50jornadas/persona Daños reputacionales a la imagen del Gobierno local, de la Administración Municipal, o de cualquier otro Ejecutivo o Administración Afecta apreciablemente a actividades oficiales o misiones en el extranjero Afecta apreciablemente a una infraestructuracrítica
I_5 - CRÍTICO	Afecta a sistemas clasificadoscon nivel secreto Afecta a más de 100 equipos con información cuya máxima categoría es media Afecta a más de 50 equipos con información cuya máximacategoría es alta Afecta a más de 10 equipos con información clasificada con nivel reservado El ciberincidente precisa para resolverse más de 50jornadas/persona Afecta apreciablemente a la seguridadnacional Afecta gravemente a una infraestructuracrítica

Artículo 20. Documentación de los ciberincidentes.

1. El Equipo de Respuesta a Ciberincidentes debe documentar el desarrollo del ciberincidente y las acciones que se han llevado a cabo en cada momento, correspondientes a las fases de detección, contención, erradicación y recuperación.

2. El documento mencionado debe contener al menos tanto nivel de detalle como el que la Guía de Seguridad de las Tecnologías de la Información y las Comunicaciones CCN-STIC-817: Esquema Nacional de Seguridad: Gestión de Ciberincidentes prevé para el seguimiento y la tipificación de las causas de los mismos, a cuyo fin se elaborarán los oportunos modelos normalizados.

3. De igual modo, se hará uso de las métricas y los indicadores codificados en la mencionada Guía.

Artículo 21. Recolección y custodia de evidencias.

1. Aunque el motivo principal para la recolección de las evidencias de un ciberincidente es ayudar a su resolución, también puede ser necesaria para iniciar procesos de naturaleza legal. Por tanto, debe documentarse claramente cómo se han obtenido y custodiado las evidencias, siempre conforme a lo dispuesto en la legislación vigente. De resultar necesario, el Equipo de Respuesta a Ciberincidentes requerirá informe interno a la Asesoría Jurídica, el Centro de Proceso de Datos, el Grupo de Proyecto para el Impulso de la Administración Electrónica, la Policía Judicial, o cualquier otro que estime

pertinente; así como a terceras partes externas especializadas, como otras Fuerzas y Cuerpos de Seguridad o la Fiscalía para la Criminalidad Informática.

2. Debe mantenerse un registro detallado de todas las evidencias, que incluya como mínimo:

    a) La identificación de la información, por ejemplo, la localización, el número de serie, número de modelo, el nombre de host, dirección MAC (Media Access Control) y direcciones IP (Internet Protocol) de los ordenadores afectados.

    b) Nombre, cargo y teléfono de cada persona que ha recogido o gestionado evidencias durante la investigación del ciberincidente.

    c) Fecha y hora de cada ocasión en la que ha sido tratada cada evidencia.

    d) Ubicaciones donde se custodiaron las evidencias.

3. Debe comenzarse el acopio de evidencias tan pronto como se detecte un ciberincidente, obteniendo inmediatamente, siempre que sea posible, una instantánea del sistema atacado, dejándolo inaccesible y garantizando su integridad, antes de tratar las copias que se realicen del sistema atacado con diferentes tipos de herramientas que, de otro modo, podrían alterar parte de la información o el estado de los sistemas comprometidos.

4. De manera reglamentaria, el Ayuntamiento redactará y aprobará las normas que deben regir la custodia y la conservación de evidencias digitales, que como mínimo habrán de satisfacer los mismos requisitos que se determinen para el

archivo electrónico único, así como definir los mecanismos de custodia de los componentes físicos de las evidencias, como discos duros, otras herramientas de almacenamiento, dispositivos móviles o sistemas que hayan sido puestos en compromiso.

Artículo 22. Intercambio de información y comunicación de ciberincidentes.

1. Además de la preceptiva notificación de los ciberincidentes al CCN-CERT, el Ayuntamiento se comunicará siempre que sea necesario con terceros, y específicamente con Fuerzas y Cuerpos de Seguridad y medios de comunicación social. El resto de las comunicaciones con otros actores se llevarán a cabo a través del CCN-CERT, en su función de Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas.

2. Independientemente de lo anterior, el Equipo de Respuesta a Ciberincidentes debe analizar con las unidades pertinentes del Ayuntamiento o sus entidades vinculadas o dependientes, y particularmente con la Asesoría Jurídica, el Grupo de Proyecto para el impulso de la administración electrónica, el Centro de Proceso de Datos y con la unidad con competencias en relaciones institucionales, los criterios y procedimientos de información a terceros ante la ocurrencia de un ciberincidente. De lo contrario, podría darse el caso de que información confidencial contenida en la información de los ciberincidentes pueda entregarse a terceros no autorizados, lo cual, además de representar un daño a la imagen del Ayuntamiento y una falta grave de incumplimiento legal,

podría dar lugar a la exigencia de responsabilidad patrimonial de la entidad, por daños y perjuicios ocasionados a terceros.

3. La coordinación y el intercambio de información con los organismos adecuados debe contribuir al fin de fortalecer la capacidad del Ayuntamiento, así como de otras administraciones, para responder con eficacia a los ciberincidentes.

4. En la medida en que la capacidad de responder a ciertos ciberincidentes puede que requiera el uso de herramientas que no estén disponibles para el Ayuntamiento, éste debe aprovechar su red de intercambio de información de confianza para externalizar de manera eficaz el análisis del ciberincidente a los recursos de terceros que sí tienen las capacidades técnicas adecuadas para gestionar adecuadamente el ciberincidente.

DISPOSICIONES ADICIONALES

Primera. Concurrencia con el Título VIII del 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

1. El alcance establecido para la auditoría en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, no tiene como objeto auditar o verificar el cumplimiento de las medidas de seguridad establecidas por el artículo 96 del Título VIII del 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. Si el sistema de información auditado según el Real Decreto 3/2010 tratase datos de carácter personal, el equipo auditor podrá solicitar una copia de la auditoría preceptiva según el Real Decreto 1720/2007.

2. No obstante, si durante la realización de la auditoría a la que es aplicable el presente Reglamento se identificase algún incumplimiento manifiesto del Real Decreto 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 sean realizadas por el mismo equipo de auditoría, es necesario tener en cuenta, los aspectos comunes y diferenciados:

    a) El Título VIII del Real Decreto 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.

    b) Los criterios para la categorización de los sistemas y el establecimiento de los niveles de seguridad en el Real Decreto 3/2010 (grado de perjuicio o impacto en el sistema o en las personas), son diferentes de los criterios seguidos en el Real Decreto 1720/2007 (tipología de datos tratados, almacenados o a los que se tiene acceso, 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.

c) Como buenas prácticas de seguridad, el Real Decreto 3/2010 y el Real Decreto 1720/2007 coinciden en que debe existir una Política de Seguridad y un Documento de seguridad, aprobados por el Ayuntamiento y comunicados a todo el personal afectado. En el espíritu del Real Decreto 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.

d) La actividad también puede ser determinante, en algunos casos, en la aplicación de las medidas de seguridad. Así, el artículo 81 del Real Decreto 1720/2007 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 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.

e) El Real Decreto 1720/2007 requiere determinadas medidas de seguridad, según el nivel aplicable, que pueden no derivarse necesariamente del preceptivo análisis de riesgos realizado según el Real Decreto 3/2010, y

que por lo tanto, podrían no estar previstas como medidas a implantar siguiendo los requisitos de este último. A continuación se mencionan algunas de las medidas que deben estar en esta situación:

i. Para los ficheros de cualquier nivel, se debe verificar semestralmente la fiabilidad de las copias de respaldo, de conformidad con el artículo 94.

ii. La recuperación de datos se considera una incidencia de seguridad, de conformidad con el artículo 100 y para los niveles medio y alto, requiriendo asimismo el registro de determinada información.

iii. El registro de accesos, de conformidad con el artículo 103 y para el 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.

iv. Si bien el cifrado en comunicaciones sólo se exige categóricamente para los ficheros que requieren medidas de nivel alto, su transmisión electrónica debe evitar su divulgación también para el nivel medio.

v. En relación al control de accesos, el Real Decreto 1720/2007, de conformidad con su artículo 91 requiere la definición de perfiles de acceso.

vi. La auditoría requerida por el artículo 96 del Real Decreto 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.

4. 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.

5. Consecuentemente, dado que estas dos normas son concurrentes en una gran mayoría de las medidas de seguridad a adoptar, 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.

Segunda. Formación.

El Ayuntamiento planificará y emprenderá las oportunas acciones formativas para que todos sus empleados, a los niveles pertinentes, estén informados, cumplan y hagan cumplir el presente Reglamento.

Tercera. Glosario.

Los términos utilizados en el presente Reglamento se incorporarán al Glosario de Administración Electrónica previsto en la "Ordenanza Municipal de Administración Electrónica del Excmo. Ayuntamiento de Cartagena".

DISPOSICION FINAL

Primera. Entrada en vigor.

El presente Reglamento será objeto de aprobación y publicación de acuerdo con los trámites legales oportunos, se publicará en la sede electrónica del Ayuntamiento y en su portal de transparencia y entrará en vigor en el plazo establecido en el artículo 70.2 y 65 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, a partir de su publicación en el Boletín Oficial.

ANEXO I: MODELO DE ACUERDO DE CONFIDENCIALIDAD (normativo)

Los contenidos de los modelos de confidencialidad que se incluyen en este Anexo, tendrán la consideración de requisitos mínimos. Las responsabilidades de su aplicación, en relación a sus respectivos equipos involucrados, en cualquier medida, en la auditoría, corresponden tanto al Ayuntamiento como a los equipos de auditoría y a los responsables de los sistemas de información auditados.

Datos de carácter personal

Las tareas de auditoría a realizar no conllevan necesariamente el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios, es posible que se tenga acceso a los mismos. Estos servicios no se encuadran exactamente en la figura de "encargado del tratamiento" establecida en el artículo 3

de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Sin embargo, sí podría considerarse aplicable el artículo 83 del 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.

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 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y del 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, 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 o 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 Ayuntamiento, 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.

XXXX 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.

E-EMGDE: ESQUEMA DE METADATOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS (informativo)

El Esquema de Metadatos para la Gestión de Documentos Electrónicos (Documentación complementaria a la Norma Técnica de Interoperabilidad de Política de Gestión de documentos electrónicos), tiene carácter meramente informativo y debe servir para la elaboración del perfil de aplicación, de obligado cumplimiento, previsto en el artículo 5.2 del presente Reglamento.

REFERENCIAS

Guía de seguridad CCN-STIC-802: Esquema Nacional de Seguridad: Guía de Auditoría: Guía de Seguridad de las Tecnologías de la Información y las Comunicaciones. Centro Criptológico Nacional, 2010

Guía de seguridad de las Tecnologías de la Información y las Comunicaciones CCN-STIC-817: Esquema Nacional de Seguridad: Gestión de Ciberincidentes

ISO/IEC 27037: Information technology: Security techniques: Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization, 2012