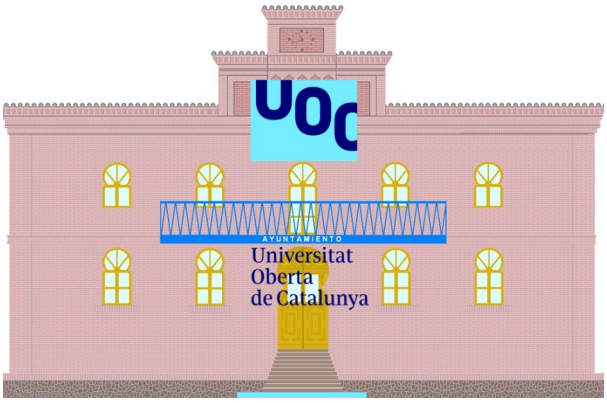

Procedimientos de Auditorías Internas del Ayuntamiento de la Universitat Oberta de Catalunya

Índice

1. Objetivo de la Auditoría

El Ayuntamiento de la Universitat Oberta de Catalunya tiene por objeto de la auditoría mantener el cumplimiento a la norma ISO/EIC 27001:2013, específicamente a su artículo 9.2 "Auditoría Interna" y de lo establecido en el RD 3/2010, específicamente en el artículo 34 y en el Anexo III, y verificar el cumplimiento de los requisitos establecidos en los capítulos II y III y en los Anexos I y II del ENS.

El objetivo ha sido consensuado entre el equipo auditor y el Ayuntamiento de la Universitat Oberta de Catalunya y permite emitir una opinión independiente y objetiva, basada en los principios de integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia, sobre este cumplimiento de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera, y atender a las observaciones que pudiera haber identificado el Equipo Auditor y en su caso, posibilitar el mantenimiento de la correspondiente Certificación de Conformidad, tal y como dispone la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.

Comprobar que el SGSI del Ayuntamiento de la Universitat Oberta de Catalunya cumple con los procesos y requisitos del Ayuntamiento y que estos se han integrado con los requisitos de la seguridad de la información con el fin de mantener al Ayuntamiento certificado en la norma ISO/EIC 27001:2013.

El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados, es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

2. Alcance

Esta Auditoría se aplicará a los sistemas de información del Ayuntamiento de la Universitat Oberta de Catalunya, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS) y del estándar ISO/IEC 27001:2013.

Este proceso incluye la planificación, ejecución, reporte y seguimiento de las auditorías internas del SGSI del Ayuntamiento de la Universitat Oberta de Catalunya y aplica a todos los departamentos dentro del ámbito de la seguridad de la información de la organización.

3. Roles y responsabilidades.

El Ayuntamiento de la Universitat Oberta de Catalunya con el fin de que el proceso de auditoría interna sea rápido y flexible define el siguiente equipo auditor en cumplimiento con lo establecido en el ENS y la ISO/EIC 27001:2013. Se garantiza que este equipo dispone de los conocimientos suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de la auditoría y forma parte de una entidad de certificación del ENS acreditada según se indica en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad".

Con el fin de asegurar su independencia y objetividad el equipo auditor será totalmente independiente al Ayuntamiento de la Universitat Oberta de Catalunya y a todos sus proveedores de servicios o sistemas que puedan ser objeto de la auditoría. Este equipo estará supervisado por el Representante de gestión de seguridad de la información y el Responsable de auditoría que sí pertenecerán al Ayuntamiento.

3.1. Representante de gestión de seguridad de la información (ISMR)

Según la Política de Seguridad del Ayuntamiento de la Universitat Oberta de Catalunya es responsabilidad del Comité de Seguridad promover la realización de las auditorías periódicas y de protección de datos que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

Se nombra al Comité de Seguridad como representante de gestión de seguridad de la información (ISMR) sus funciones son:

- Apoyar el trabajo del Responsable del programa de auditoría y del equipo auditor.
- Revisar el informe de auditoría interna junto con el Auditor Jefe con el fin de tomar las acciones correctivas y preventivas necesarias y planificar las siguientes auditorías.
- Mantener la confidencialidad en los resultados de la auditoría.

3.2. Responsable del programa de auditoría

Según la Política de Seguridad del Ayuntamiento de la Universitat Oberta de Catalunya es responsabilidad del Responsable de Seguridad gestionar las revisiones externas o internas del sistema promoviendo auditorías periódicas de obligado cumplimiento en ENS o ISO/EIC:27001:2013.

Se nombra al Responsable de Seguridad como Responsable del Programa de Auditorías, sus funciones son:

- Definir el Proceso de Auditoría y presentarlo al Comité de Seguridad para conseguir los recursos necesarios.

- Informar en caso de metodología White/Grey Box al departamento de Informática y al Concejal del área y planificar conjuntamente el Proceso de Auditoría.
- Liderar el proceso de contratación del servicio de auditoría interna redactando los pliegos necesarios y convirtiéndose en el Responsable del Contrato. Para que los licitadores puedan ofrecer precios ajustados el Responsable del Programa de Auditoría ofrecerá a las posibles empresas adjudicatarias, bajo firma del modelo de acuerdo de confidencialidad, un resumen aproximado de la información relativa al punto 4.1. de este documento, también especificará la duración del contrato, que se establece en 3 años, y la cantidad de auditorías a incluir atendiendo al punto 6 de este documento “Programa de Auditorías”.
- Durante el proceso de auditoría ser el nexo de unión con la empresa auditora y en caso de necesidad convocar la reunión del ISRM con el equipo auditor.
- Supervisar el Programa de Auditoría y redactar las modificaciones o mejoras necesarias.
- Asegurar que todo el equipo auditor así como los expertos técnicos firmen y acepten el modelo de acuerdo de confidencialidad (Anexo D).

3.3. Equipo Auditor.

3.3.1. Auditor Jefe

El Auditor Jefe o líder del equipo auditor deberá asegurar que dispone de los conocimientos técnicos necesarios para abordar la auditoría de una forma eficiente según los objetivos y el alcance del proceso interno de auditorías del Ayuntamiento de la Universitat Oberta de Catalunya. Sus funciones son:

- Garantizar que se realizan las acciones necesarias, en la etapa preliminar, para que todos los integrantes del equipo entiendan y conozcan la estructura organizativa y técnica del sistema a auditar, los servicios que presta, y el objetivo y el alcance de la auditoría.
- Asegurar que todos los auditores conocen el RD 3/2010 y la norma ISO/EIC 27001:2013 y, en la medida de las tareas asignadas, los requisitos de seguridad de otra legislación aplicable, y en particular, la relativa a tratamiento de datos de carácter personal.
- Desarrollar el Plan de Auditoría Interna.
- Llevar a cabo el plan de auditoría previsto y aprobado, y que las desviaciones al programa, o sus modificaciones, están debidamente fundamentadas y registradas sus modificaciones.
- Coordinar el calendario de la auditorías.
- Mantener informado al ISRM y en particular al Responsable del programa de Auditoría, reportando no-confirmades críticas inmediatamente.
- Consolidar todos los hallazgos de la auditoría y preparar el informe de auditoría interna que será presentado en tiempo de un modo claro e inteligible, será imprescindible un resumen ejecutivo.
- Dirigir y documentar todas las reuniones mantenidas con la organización.

3.3.2. Auditor/es Subordinado/s

El Auditor Jefe podrá disponer de auditores subordinados que, además de ayudarle en las tareas que se les encomienden, serán los principales encargados de las labores de campo, de comprobar que se cumplen las pautas acordadas, de la elaboración de comunicados informativos así como de la redacción de guías de de buenas prácticas. Estos auditores permitirá al auditor jefe centrarse en labores más de diseño, planificación y evaluación.

3.3.3. Expertos técnicos.

Los expertos técnicos no formarán parte en sí mismo del equipo auditor aunque podrán ser solicitados por el equipo en caso de duda sobre diseño de un control en un procedimiento o para la ejecución de una prueba especialmente técnica. Serán también será totalmente independientes al Ayuntamiento de la Universitat Oberta de Catalunya y a todos sus proveedores de servicios o sistemas que puedan ser objeto de la auditoría.

4. Procedimiento

El Ayuntamiento de la Universitat Oberta de Catalunya ha creado un programa de auditoría del SGSI que contiene todas las auditorías programadas para todo el calendario de vigencia de las certificaciones. Esto incluirá el cronograma de auditorías internas, auditorías de proveedores, auditorías a realizar por clientes y auditorías de terceros, según corresponda.

Las auditorías internas se programarán al menos una vez al año o a petición cuando se produzcan cambios sustanciales en los sistemas de información. El Auditor Líder supervisará la actividad del Equipo de Auditoría. La empresa auditora notificará las distintas acciones a cada departamento del Ayuntamiento involucrado en el proceso de auditoría interna con al menos tres días hábiles de antelación.

4.1. Planificación preliminar de la Auditoría

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

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

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

- Este documento firmado por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de auditoría interna.
- Organigrama de los servicios o áreas afectadas, con descripción de funciones y responsabilidades.
- Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.
- Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones y similares).
- Categoría del sistema según el Anexo I del ENS, incluyendo los criterios de identificación y valor de los niveles de las dimensiones de seguridad que serán de aplicación al sistema.
- La Política de Seguridad.
- La Política de Firma Electrónica y Certificados.
- La Normativa de Seguridad.
- Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
- Informes con el desarrollo y resultado de la apreciación del riesgo, incluyendo la identificación de escenarios de riesgo, su análisis y evaluación.
- La Declaración de Aplicabilidad.
- Decisiones adoptadas para tratar los riesgos.
- Relación de las medidas de seguridad implantadas por requisitos legales o como resultado de la apreciación del riesgo.
- Relación de registros de actividad en lo relativo a las medidas de seguridad implantadas y estado de implantación.
- Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría, como podría ser el informe de la auditoría bienal de protección de datos de carácter personal, o de auditorías previas con el mismo objetivo y alcance que la auditoría a comenzar.
- Informes de seguimiento de deficiencias detectadas en auditorías previas de seguridad, y relacionadas con el sistema a auditar.
- Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.
- Sistemas de métricas.

Esta documentación será facilitada al Auditor Jefe quien preparará el Plan de Auditoría para su aprobación por el ISMR, este plan será flexible con la finalidad de permitir cambios basados en la retroalimentación recibida durante la ejecución de la auditoría interna. En la elaboración del plan se definirá como mínimo lo siguiente:

- Resumen ejecutivo.
- Objetivo y alcance de la auditoría interna.
- Departamentos y responsabilidades individuales afectadas.
- Equipo auditor y asignación de tareas.
- Canal oficial de comunicación entre el equipo auditor y la empresa auditora.
- Tipología de los sistemas de la información a auditar.
- Selección de medidas a auditar (ENS, ISO/EIC 27001:2013 e ISO/EIC 27002:2013).
- Planificación con fechas exactas y lugares de la auditoría.
- Fecha de entrega del informe de auditoría.

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

4.2. Reunión previa a la Auditoría

Asistentes: Responsable del programa de Auditoría y Auditores Jefes de las empresas licitadoras.

Fecha: antes de publicar la licitación.

Objetivos: verificar el alcance y los objetivos para elaborar el Plan de Auditoría. Verificar que se disponen de todos los recursos (especialmente documentación) y logística.

Paso previo: seleccionar hasta tres empresas y planificar junto con el departamento de Contratación para que habilite todo lo necesario para la realización de una consulta preliminar de mercado acorde a los requisitos establecidos en la nueva Ley de Contratos del Sector Público (artículo 115).

4.3. Reunión de Inicio de Auditoría

Asistentes: el ISMR al completo y el Auditor Jefe de la empresa licitadora ganadora.

Fecha: después de la adjudicación de la licitación y de haber facilitado al Auditor Jefe el resto de la documentación necesaria para la elaboración de un Plan de Auditoría.

Objetivos: exponer el propósito y el alcance de la auditoría al ISMR, aprobar el Plan de Auditoría y clarificar detalles que deban ser detallados antes de iniciar la auditoría interna.

4.4. Ejecución de la Auditoría

La auditoría se llevará a cabo mediante el empleo de numerosos checklists, en concreto:

- Cheklist de auditoría interna: contiene elementos particulares de la organización a auditar.
- Checklist de requerimientos de ISO/IEC 27001:2013.
- Checklist de controles de ISO/IEC 27002:2013.
- Checklist de pruebas de ENS (RD 3/2010 Anexos I y II), en concreto los relativos a la Gestión del Riesgo, el marco organizativo y la segregación de funciones, el marco operacional, las medidas de protección, la declaración de aplicabilidad, los procesos de mejora continua de la seguridad y la aplicación de los modelos de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos. Se permitirá el empleo del checklist de la guía CCN-STIC 808 del CCN.

Los hallazgos serán encontrados mediante el empleo de entrevistas, revisión de documentación y observación de las actividades y las condiciones en las áreas objeto de la auditoría.

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 realizarán preguntas donde la respuesta, afirmativa o negativa según el caso, esté implícita en la pregunta, salvo para confirmar los hallazgos de conformidad o de no conformidad con los criterios de auditoría obtenidos a partir de las evidencias. Se ponderarán las respuestas de las entrevistas, pudiendo dar lugar a la realización de pruebas complementarias que no estaban previstas.

Ante la ausencia de determinada medida, se investigará y analizará si existen otras medidas compensatorias, y en su caso, se evaluará la eficacia de estas últimas. Cuando se haya evaluado la implantación y efectividad de una medida de seguridad sin detectar no conformidades, se proseguirá con el plan de auditoría, asumiendo, por tanto, su conformidad.

Las 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.

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) se mantendrán como mínimo durante los dos siguientes años, debidamente referenciados y archivados, así como custodiados por el ISMR y protegidos.

Cuando el auditor, en el curso de sus observaciones, descubra una irregularidad significativa de fácil resolución o una vulnerabilidad crítica, puede informar inmediatamente al Responsable de la Seguridad para que tome las medidas correctivas oportunas sin esperar al informe final de auditoría.

4.5. Elaboración y presentación de los hallazgos

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

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.

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

Se clasificarán todos los hallazgos atendiendo a la siguiente tipología:

- No conformidad mayor: Se documentará una “No Conformidad Mayor” cuando se detecten “No Conformidades Menores” en relación con cualquiera de los preceptos contenidos en el RD 3/2010, de 8 de enero, o en el Marco organizativo, o en alguno de los subgrupos que integran el Marco operacional o las Medidas de protección (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, Monitorización del Sistema, Protección de las Infraestructuras, Gestión del Personal, Protección de Equipos, Comunicaciones, Soportes de Información, Aplicaciones Informáticas, Información o Servicios) que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados. También cuando se detecte una deficiencia mayor en el SGSI perteneciente a uno o más elementos de ISO/EIC 27001:2013 no implementados. Estas no conformidades tienen un impacto directo en la seguridad de la información, específicamente en la preservación de la confidencialidad, integridad y disponibilidad de los activos de información. Requiere atención y corrección inmediata por parte de la organización, se planificará revisión de la auditoría inmediata para este punto de control una vez tomadas medidas paliativas.
- No conformidad menor: Se documentará una “No Conformidad Menor” ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos. También cuando se detecte una deficiencia menor en el SGSI dado que uno o más elementos se encuentran implementados sólo parcialmente. Requiere atención y corrección inmediata por parte de la organización, se planificará una revisión de la auditoría para este punto de control en el espacio de un mes máximo.
- Observación: Se documentará una Observación cuando se encuentren evidencias de, una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por ISO/EIC 27001:2013, pueda, en la actualidad o

en el futuro, derivar en un problema. Requiere atención y corrección por parte de la organización, se revisará en la próxima auditoría interna planificada.

- Posibilidad de Mejora: se tratan de sugerencias de mejora encontradas que pueden o no ser implementadas por el Ayuntamiento.

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

- Fecha de emisión del informe.
- Una sección de alcance, detallando su extensión y limitaciones, e incluyendo el objetivo de la auditoría, con la debida identificación del sistema o sistemas auditados.
- Breve descripción del proceso metodológico aplicado para realizar la auditoría.
- Identificación de la documentación revisada.
- Indicación de si ha habido alguna limitación en la realización de la auditoría, que impidan al equipo auditor formarse una opinión sobre determinados criterios de la auditoría, incluidas medidas de seguridad.
- Una sección de informe ejecutivo resumiendo los puntos fuertes, las debilidades (resumen de las no conformidades y observaciones) y oportunidades de mejora, e incluyendo un resumen general del grado de cumplimiento.
- Acciones correctivas y preventivas llevadas a cabo durante la auditoría interna y fecha en que se produjeron.
- Acciones de revisión para las no conformidades y las observaciones, así como la definición de su seguimiento.
- 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 incluirá como anexo las contestaciones del Responsable de la Seguridad a los comentarios vertidos en el informe, o las acciones que se tomarán para solucionar las deficiencias, si las hubiera.

El Informe de Auditoría será firmado por el Auditor Jefe, e indicará los participantes en el equipo de auditoría en un anexo o a continuación de su firma.

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

4.6. Reunión de Fin de Auditoría.

Asistentes: el ISMR al completo y el Auditor Jefe de la empresa licitadora ganadora.

Fecha: al finalizar la auditoría.

Objetivos: presentar el Informe de Auditoría al Responsable del Sistema y al Responsable de la Seguridad (ambos pertenecientes al ISMR), según el RD 3/2010 los informes de auditoría serán

analizados por el Responsable de Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las acciones correctivas adecuadas. Conseguir recursos por parte de la dirección de la empresa para corregir los no-conformes y las observaciones.

5. Seguimiento y cierre de la auditoría.

Es obligación del Ayuntamiento de la Universitat Oberta de Catalunya dar respuesta a las no conformidades y observaciones encontradas. Estas respuestas serán acciones correctivas de mutuo acuerdo con el equipo auditor.

El auditor jefe comprobará la implementación de las acciones correctivas y preventivas y las agregará a las revisiones del Informe de Auditoría, se empleará un procedimiento simplificado del Plan de Auditoría para la verificación de la efectividad de las medidas.

En caso de que las medidas utilizadas no se encuentren implementadas en la fecha de revisión de los controles, el auditor jefe acordará una nueva comprobación atendiendo a la criticidad de la misma y las circunstancias del Ayuntamiento.

La auditoría no se considerará completa o cerrada hasta que todas las acciones correctivas o preventivas hayan sido implementadas y revisadas por el Auditor Jefe.

6. Programa de Auditorías.

6.1 ENS

La categorización de los sistemas de información atendiendo a lo dispuesto en el ENS establece distintos tiempos para las realización de auditorías según la categoría sea BÁSICA, MEDIA o ALTA:

- Básica: Requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada dos años o cuando se produzcan modificaciones sustanciales en el sistema. La autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.
- Media o Alta: Precisarán de una auditoría formal para mantenimiento de certificación de la conformidad al menos cada dos años, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria.

La planificación completa podrá ser encontrada en el Plan de Mejora de la Seguridad documentado y adjunto al Plan de Adaptación al ENS.

6.2 ISO/EIC 27002:2013

Se planifica a tres años que es el periodo de vigencia de la certificación. Por simplicidad, ahorro de costes y flexibilidad no se revisarán los 14 dominios del estándar en cada una de las auditorías internas realizadas, siendo libre la adaptación de esta propuesta por parte del Auditor Jefe a las fechas que él estime pero realizando al menos una auditoría anual y cumpliendo los intervalos que se especifican para cada uno de los dominios del estándar:

Nombre: A.5 Políticas de Seguridad de la Información.

Alcance: el propio SGSI.

Objetivos: comprobar que las políticas sean aprobadas, publicadas y comunicadas a los empleados y a los terceros relacionados con el Ayuntamiento de la Universitat Oberta de Catalunya.

Planificación: Cada 3 años ó siempre que en el Ayuntamiento se produzca un cambio/necesidad significativa que conlleve modificación de las políticas para la seguridad de la información.

Nombre: A.6 Organización de la seguridad de la información

Alcance: Organización interna, dispositivos móviles y teletrabajo.

Objetivos: Controles para garantizar que el Ayuntamiento organice las funciones y asigne responsabilidades en la seguridad de la información.

Planificación: Anual, no planificar la auditoría en meses de festividad o vacacionales.

Nombre: A.7 Seguridad relativa a los recursos

Alcance: recursos humanos y proveedores

Objetivos: Controles a todos los recursos humanos relacionados con el Ayuntamiento de la Universitat Oberta de Catalunya ya sea a su contratación, durante su empleo o a su extinción contractual para garantizar la seguridad de la información.

Planificación: Anual, no planificar la auditoría en meses de festividad o vacacionales.

Nombre: A.8 Gestión de Activos

Alcance: los activos físicos de la empresa, el Inventario.

Objetivos: Controles que garanticen la preservación de los activos del Ayuntamiento de la Universitat Oberta de Catalunya.

Planificación: Anual, posibilidad de revisión parcial en tiempo real con tecnología RFID empleando el sistema Wifi del Ayuntamiento.

Nombre: A.9 Control de Acceso

Alcance: Disponibilidad de la Información.

Objetivos: Controles sobre el acceso a los medios de información ya sean físicos (sala de servidores) o lógicos (permisos de usuarios).

Planificación: Anual, no planificar la auditoría en meses de festividad o vacacionales.

Nombre: A.10 Criptografía

Alcance: Confidencialidad e Integridad de la Información.

Objetivos: Controles de criptografía que protejan la información del Ayuntamiento de filtraciones.

Planificación: Anual, no planificar la auditoría en meses de festividad o vacacionales.

Nombre: A.11 Seguridad física y del entorno

Alcance: Áreas Seguras y Equipamiento

Objetivos: Controles que prevengan accesos físicos, daños e interferencias contra las instalaciones o los activos del Ayuntamiento, así como interrupciones en las líneas de negocio del mismo.

Planificación: Anual o siempre que exista un cambio de infraestructura física y del entorno.

Nombre: A.12 Seguridad en las operaciones

Alcance: Instalaciones de procesamiento de la Información eliminando del alcance todos los elementos que sean de poca importancia.

Objetivos: Controles técnicos sobre los sistemas de información.

Planificación: Anual, en periodos de baja carga de trabajo.

Nombre: A.13 Seguridad en las comunicaciones

Alcance: Red de Comunicaciones.

Objetivos: Controles para redes internas, externas, medios de transmisión, soportes, mensajería…

Planificación: Anual, en periodos de baja carga de trabajo.

Nombre: A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Alcance: Sistemas de Información

Objetivos: Control del ciclo de vida completo de los sistemas de información tanto propios como subcontratados.

Planificación: Anual, en periodos de baja carga de trabajo.

Nombre: A.15 Relación con los proveedores

Alcance: Personal externo a la organización

Objetivos: Controles para el personal externo al Ayuntamiento que tenga acceso a los sistemas de información.

Planificación: Anual.

Nombre: A.16 Gestión de Incidentes de la seguridad de la información

Alcance: Departamento de Seguridad Informática

Objetivos: Evaluar el modo en el que se están gestionando los incidentes de seguridad de la información por parte del departamento de informática.

Planificación: Anual y también después de que se produzca un Incidente de seguridad de la información que haya tenido un impacto negativo-grave en el Ayuntamiento.

Nombre: A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Alcance: Plan de continuidad de Negocio

Objetivos: Controles que demuestren que se dispone de las herramientas necesarias para dar respuesta a las amenazas que pueda sufrir el Ayuntamiento.

Planificación: Cada 3 años ó siempre que en el Ayuntamiento se produzca un cambio/necesidad significativa que conlleve modificación de las políticas para la seguridad de la información.

Nombre: A.18 Cumplimiento

Alcance: Aspectos legales y normativos

Objetivos: Controles que permitan evaluar el cumplimiento de las obligaciones legales, normativas, contractuales, etc. relacionadas con la seguridad de la información.

Planificación: Anual y en casos excepcionales cuando sucedan cambios legislativos express.

ANEXO A. Requisitos para el equipo Auditor

El equipo auditor deberá estar dirigido y tutelado siempre por un Auditor Jefe también llamado Líder del equipo auditor, cuyas funciones principales son la supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionados en el informe, así como preservar las evidencias de la auditoría.

El Auditor Jefe, responsable de gestionar las actividades de auditoría, deberá probar como mínimo:

- Acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos 4 años, en auditoría de tecnologías de la información.
- Conocimientos de seguridad y gestión de riesgos de seguridad (certificación y experiencia probada de al menos 4 años en estos elementos).
- Conocimiento de los requisitos del RD 3/2010.
- Conocimientos en ISO/EIC 27001:2013 e ISO/EIC 27002:2013.

El resto del equipo puede no cumplir con los requisitos para el Auditor Jefe, no obstante, debe tener alguna preparación previa tanto en seguridad como en auditoría de los sistemas de información, dependiendo de, y en consonancia, con las responsabilidades asignadas. La responsabilidad por la asignación de tareas al resto del equipo, incluyendo a los expertos, corresponde a la organización (privada o pública) que aporte el equipo de auditoría.

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

Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad. En anexo D se propone un modelo.

ANEXO B. Incorporación expertos técnicos al equipo de Auditoría

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

Entre estos expertos técnicos también es posible que sea necesario incluir profesionales con perfiles especializados tales como: expertos con conocimientos jurídicos, expertos en Procedimiento Administrativo, expertos en archivística, gestión documental y conservación a largo plazo, expertos con conocimientos relativos a la gestión de documentos y archivos electrónicos, y otros que se estimen pertinentes en función del sistema auditado.

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

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.

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 con el Reglamento (UE) 2016/679

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

Cuando el sistema auditado tenga por objeto el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto el tratamiento de datos personales, se tendrá en cuanta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. A partir de dicha fecha en todo momento se informará al Delegado de Protección de Datos en calidad de responsable de la

supervisión del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

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

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.

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

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

ANEXO D. Modelo de Acuerdo de Confidencialidad

En la Universitat Oberta de Catalunya, DISPONGO:

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

Datos de carácter personal

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

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

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

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

Información del sistema de información auditado

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.

DOCUMENTO FIRMADO ELECTRÓNICAMENTE