INFORME 25/2024

AYUNTAMIENTO DE BADALONA

CONTROLES BASICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

INFORME 25/2024

AYUNTAMIENTO DE BADALONA
CONTROLES BASICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

Edición: mayo de 2025

Documento electrónico etiquetado para personas con discapacidad visual

Páginas en blanco insertadas para facilitar la impresión a doble cara

Autor y editor:

Sindicatura de Cuentas de Cataluña
Vía Laietana, 60
08003 Barcelona
Tel. +34 93 270 11 61
sindicatura@sindicatura.cat
www.sindicatura.cat

Publicación sujeta a depósito legal de acuerdo con lo previsto en el Real decreto 635/2015, de 10 de julio

ÍNDICE

ABREVIACIONES

CBCS	Control básico de ciberseguridad
ENS	Esquema Nacional de Seguridad
GPF-OCEX	Guía práctica de fiscalización de los órganos de control externo
TIC	Tecnologías de la información y la comunicación

1. INTRODUCCIÓN

1.1. INFORME

La Sindicatura de Cuentas, como órgano fiscalizador del sector público de Cataluña, de acuerdo con la normativa vigente y en cumplimiento de su Programa anual de actividades, ha emitido este informe de seguridad limitada relativo a los controles básicos de ciberseguridad del Ayuntamiento de Badalona (excluidos los entes dependientes) en el ejercicio 2023.

Esta auditoría de sistemas de la información, de carácter limitado, se ha centrado en la revisión de los 8 controles básicos de ciberseguridad (CBCS) que establece la Guía práctica de fiscalización (GPF-OCEX) 5313, Revisión de los controles básicos de ciberseguridad, aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12 de noviembre de 2018.

Los controles básicos de ciberseguridad que incluye esta guía se detallan en el siguiente cuadro:

Cuadro 1. Controles básicos de ciberseguridad

Control	
CBCS 1	Inventario y control de dispositivos físicos
CBCS 2	Inventario y control de *software* autorizado y no autorizado
CBCS 3	Proceso continuo de identificación y corrección de vulnerabilidades
CBCS 4	Uso controlado de privilegios administrativos
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores
CBCS 6	Registro de la actividad de los usuarios
CBCS 7	Copias de seguridad de datos y sistemas
CBCS 8	Cumplimiento de legalidad

Fuente: GPF-OCEX 5313.

El objetivo general de la fiscalización es proporcionar una evaluación sobre el diseño[1] y la eficacia operativa[2] de estos 8 controles mediante la identificación de deficiencias de control interno que puedan afectar negativamente la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y activos de la entidad, y la identificación de incumplimientos normativos relacionados con la ciberseguridad.

1. La evaluación del diseño de un control implica que el auditor considere si el control, individualmente o en combinación con otros controles, es capaz de prever de forma eficaz, detectar o corregir, la materialización de los riesgos previstos. Es decir, es capaz de cumplir el objetivo del control.

2. El auditor comprueba que el control existe y que la entidad lo está utilizando.

Para dar cumplimiento a este objetivo se han revisado unos tipos de elementos que forman parte de la infraestructura de tecnología de información general y que dan servicio a todos los procesos de gestión de la entidad, los cuales son fundamentales para el buen funcionamiento de los sistemas de información y ciberseguridad:

- Controlador de dominio
- *Software* de virtualización
- Equipos de usuario (una muestra)
- Elementos de la red de comunicaciones
- Elementos de seguridad

Dada la gran amplitud, complejidad y diversidad de sistemas, después de la revisión prevista en los procedimientos de la GPF-OCEX 5313, para los CBCS 4 y CBCS 6 se ha focalizado la revisión en las aplicaciones que sustentan los procesos de gestión contable y presupuestaria y la gestión tributaria y recaudatoria.

En cuanto al ámbito temporal del trabajo, las conclusiones se refieren a la situación a 19 de junio de 2024, fecha sobre la cual se han calculado los índices de madurez que figuran en el informe.

Además de valorar el índice de madurez de estos 8 controles, el trabajo efectuado se ha ampliado con la valoración de la gobernanza de la ciberseguridad que ejercen los órganos de gobierno y de las acciones llevadas a cabo por el Ayuntamiento para cumplir el Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Este trabajo se enmarca en el eje estratégico 1, de mejora del proceso de fiscalización y el impacto de los informes en los servicios públicos, incluido en el Plan estratégico de la Sindicatura 2022-2028, por el que se incorporan auditorías de sistemas de la información en el programa anual de actividades de la institución. Para llevar a cabo esta auditoría se han contratado servicios a una empresa especializada en seguridad informática y el personal de la Sindicatura ha dirigido y supervisado el trabajo.[3]

En el apartado 3, Conclusiones, se incluyen las conclusiones a las que se ha llegado a partir del trabajo llevado a cabo, y en el 4, Recomendaciones, están las recomendaciones sobre mejoras en la gestión de las actividades desarrolladas en algunos de los aspectos que se han puesto de manifiesto durante la realización del trabajo.

3. De acuerdo con lo previsto en el artículo 46 de la Ley 18/2010, de 7 de junio, de la Sindicatura de Cuentas, y en el apartado 10 de la GPF-OCEX 5311, hasta que en las plantillas de los órganos de control externo no se incorporen auditores de sistemas de información y expertos en ciberseguridad, se dispone del recurso de contratar a expertos externos y a profesionales especializados.

Dado el carácter limitado de la revisión, su objetivo no es emitir una opinión de seguridad razonable sobre la confianza que merece el sistema auditado en relación con el nivel de ciberseguridad implantado. Sin embargo, la auditoría proporcionará información relevante sobre el grado de ciberseguridad y ciberresiliencia de la entidad y sobre posibles acciones de mejora aconsejables.

1.2. ENTE FISCALIZADO

1.2.1. Actividades y organización

El municipio de Badalona es un ente local cuyas competencias y funciones se rigen por el Decreto legislativo 2/2003, de 28 de abril, por el que se aprueba el texto refundido de la Ley municipal y de régimen local de Cataluña, y por la Ley del Estado 7/1985, de 2 de abril, reguladora de las bases del régimen local, y por otras disposiciones específicas y complementarias.

El Ayuntamiento dispone de un reglamento orgánico municipal propio que regula el régimen organizativo y de funcionamiento de sus órganos.

a) Órganos de gobierno y entes dependientes del Ayuntamiento

Los órganos de gobierno con competencias decisorias del Ayuntamiento de Badalona son el Pleno, la Junta de Gobierno Local, el alcalde y los tenientes de alcalde.

Como órganos complementarios, en el ejercicio fiscalizado, disponía de los siguientes: las comisiones informativas, la Comisión Especial de Cuentas, la Junta de Portavoces, el Defensor de la Ciudadanía, la Junta Local de Seguridad y diferentes consejos creados en el ejercicio de la autonomía organizativa de la que dispone el Ayuntamiento para crear órganos municipales.

En lo que a los entes dependientes se refiere, en el ejercicio 2023 el Ayuntamiento tenía constituidos 3 organismos autónomos, 6 sociedades mercantiles y 1 fundación; además, tenía adscrito 1 consorcio.

Estos entes eran los siguientes:

- Patronato de la Música de Badalona
- Museo de Badalona
- Instituto Municipal de Servicios Personales
- Badalona Comunicació, SA
- Badalona Serveis Assistencials, SA
- Badalona Cultura, SL

- Ens de Gestió Urbanística, SA
- Marina de Badalona, SA
- Reactivació Badalona, SA
- Fundació Badalona Capital Europea del Bàsquet
- Consorcio Badalona Sur

b) Departamento de Informática y Tecnologías de la Información

La misión del Departamento de Informática y Tecnologías de la Información (TIC) es la definición, planificación y ejecución de la estrategia tecnológica del Ayuntamiento de Badalona, incluyendo los organismos autónomos. Esta estrategia, alineada con el objetivo estratégico de la organización de adecuar los servicios municipales a las necesidades y las demandas reales de los ciudadanos, está orientada a cumplir los siguientes objetivos:

- Mejorar el servicio al ciudadano mediante el uso de la tecnología.
- Optimizar y modernizar los procesos internos mediante la incorporación de tecnología.
- Actuar como elemento integrador y dinamizador en el Ayuntamiento en materia de tecnologías.
- Optimizar los recursos municipales disponibles.
- Potenciar el uso de las nuevas tecnologías a la ciudad.
- Colaborar con el resto de las administraciones públicas.

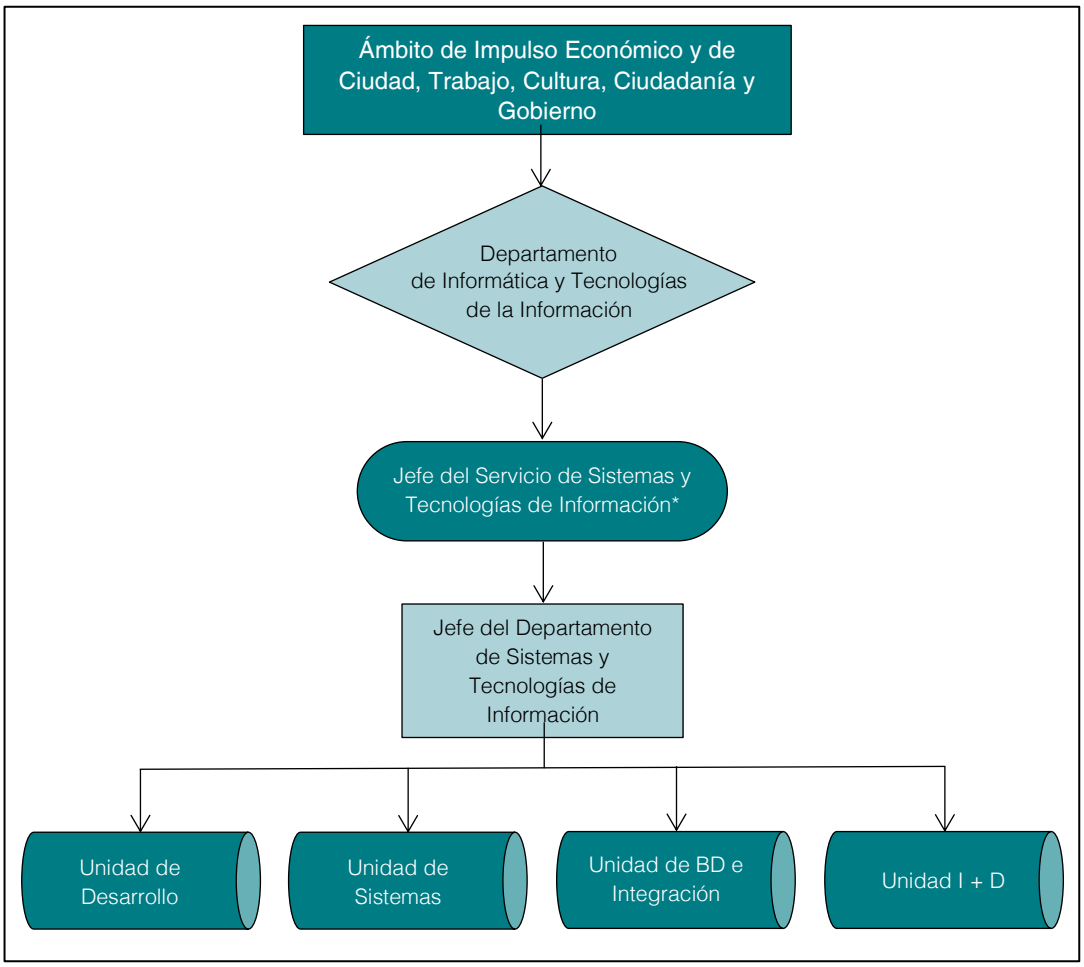
El Departamento es el encargado de desarrollar todos los objetivos del servicio, así como los definidos por el coordinador de informática y TIC. Las funciones específicas del Departamento son:

- Diseñar, proponer e implementar la estrategia en materia TIC del Ayuntamiento de Badalona.
- Análisis de proyectos en materia TIC, necesidades y costes, tanto en el ámbito de *hardware* como en el de *software*.
- Realizar propuestas de actualización y consultoría a los diferentes departamentos, empresas municipales y organismos autónomos de los diferentes sistemas de información.
- Elaborar e implementar propuestas de sistemas de comunicación, telefonía y telecomunicaciones.
- Estudios de viabilidad y valoración de nuevos proyectos en materia TIC.
- Implementar proyectos que fomenten las TIC en la ciudad de Badalona.
- Dirección técnica de los equipos de trabajo en las implantaciones de proyectos en materia TIC.

- Dirigir y coordinar las medidas de seguridad en materia informática.
- Tratar las modificaciones necesarias en los sistemas de información a fin de adecuar los sistemas informáticos del Ayuntamiento a la normativa vigente en materia TIC (Ley orgánica de protección de datos, el Esquema Nacional de Seguridad y otros que sean aplicables).
- Asistencia en materia TIC a los diferentes departamentos del Ayuntamiento.
- Asesorar y coordinar técnicamente proyectos en materia de ciudades inteligentes.

En el ejercicio 2023 el número de plazas asignadas a esta unidad era de 14, ocupadas con 11 funcionarios de carrera, 1 funcionario interino y 2 laborales. La dependencia y la organización básica de la unidad se muestra en el siguiente gráfico:

Gráfico 1. Organigrama funcional del Departamento de Informática y Tecnologías de la Información



Fuente: Elaboración propia a partir de los datos facilitados por el Ayuntamiento.

* La plaza de jefe del Departamento de Sistemas y Tecnologías de la Información se creó con la modificación de la Relación de puestos de trabajo aprobada definitivamente el 29 de diciembre de 2023 con la publicación en el *Boletín Oficial de la Provincia* y se cubrió el 1 de julio de 2024.

2. METODOLOGÍA

Los resultados del trabajo se han evaluado de acuerdo con lo previsto en el apartado 7 de la GPF-OCEX 5313 teniendo en cuenta el análisis y la evaluación de los CBCS a 2 niveles.

Por cada control global la guía define una serie de subcontroles, de cada uno de los cuales se ha extraído una valoración en función de las pruebas de auditoría y evidencias obtenidas sobre su eficacia, y se han cualificado de la siguiente forma:

Cuadro 2. Valoración de cada subcontrol

Nivel	Descripción
Control efectivo	• Cubre al 100% el objetivo de control y: - El procedimiento está formalizado (documentado y aprobado) y actualizado. - El resultado de las pruebas realizadas para verificar implementación y eficacia operativa ha sido satisfactorio.
Control bastante efectivo	• En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y: - Se sigue un procedimiento, aunque puede no estar formalizado o presentar aspectos de mejora (detalle, nivel de actualización, etc.). - Las pruebas realizadas para verificar la implementación son satisfactorias. - Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.
Control poco efectivo	• Cubre de forma muy limitada el objetivo de control y: - Se sigue un procedimiento, aunque puede no estar formalizado. - El resultado de las pruebas de implementación y eficacia operativa es satisfactorio. • Cubre en líneas generales el objetivo de control, pero: - No se sigue un procedimiento claro. - Las pruebas realizadas para verificar la implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos, aunque no son generalizados).
Control no efectivo o no implementado	• No cubre el objetivo de control. • El diseño cubre el objetivo de control, pero el resultado de la revisión realizada pone de manifiesto que la implementación o la eficacia operativa del control no son satisfactorias (se han detectado incumplimientos significativos y generalizados).

Fuente: GPF-OCEX 5330.[4]

Una vez revisados los resultados obtenidos en los subcontroles de cada CBCS y teniendo en cuenta su importancia relativa para el cumplimiento del objetivo del control, se han evaluado los 8 controles aplicando el modelo de nivel de madurez de los procesos ponderado

4. Para llevar a cabo el trabajo se ha empleado la GPF-OCEX 5330 aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12 de noviembre de 2018. Esta GPF ha sido modificada después de la finalización del trabajo de campo, y la última versión fue aprobada el 26 de junio de 2024. Esta nota es válida para todas las referencias que se hacen de esta GPF en el informe.

en una escala de cero a 100. En el siguiente cuadro se detallan los niveles de madurez de los procesos.

Cuadro 3. Niveles de madurez

Nivel	Índice	Descripción
0 – Inexistente	0	Esta medida no está siendo aplicada en este momento.
1 – Inicial / *ad hoc*	10	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempo de respuesta. El éxito del nivel 1 depende de si se tiene personal de alta calidad.
2 – Repetible, pero intuitivo	50	Los procesos siguen una pauta regular cuando diferentes personas realizan determinados procedimientos, pero no hay procedimientos escritos ni actividades formativas. La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. El resultado es imprevisible si se dan nuevas circunstancias. Todavía existe un riesgo significativo de exceder las estimaciones de coste y tiempo.
3 – Proceso definido	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas. Se dispone de un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la coherencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Existe normativa establecida y procedimientos para garantizar una reacción profesional ante los incidentes. Se realiza un mantenimiento regular. Las posibilidades de éxito son elevadas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es más que buena suerte: debe trabajarse. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
4 – Gestionado y medible	90	La Dirección controla y mide el seguimiento de los procedimientos y adopta medidas correctoras cuando es conveniente. Se dispone de un sistema de medidas y métricas para conocer el seguimiento (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.

Nivel	Índice	Descripción
		En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3 la confianza es solo cualitativa.
5 – Optimizado	100	Se siguen buenas prácticas en un ciclo de mejora continua. El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándolos como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el funcionamiento de los sistemas a base de una mejora continua de los procesos a partir de los resultados de las medidas y los indicadores.

Fuente: GPF-OCEX 5313.

Para determinar el nivel de madurez mínimo requerido hay que tener presente que a los sistemas de las tecnologías de la información y la comunicación de los organismos del sector público obligados al cumplimiento del ENS se les asigna una categoría en función de la valoración del impacto que tendría sobre la organización un incidente que afectara la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

- Conseguir sus objetivos
- Proteger los activos a su cargo
- Cumplir con sus obligaciones diarias de servicio
- Respetar la legalidad vigente
- Respetar los derechos de las personas

Con el fin de poder determinar el impacto que un incidente de este tipo tendría sobre la organización, y poder establecer la categoría del sistema, deben tenerse en cuenta las 5 dimensiones de seguridad que los controles de ciberseguridad deben garantizar: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La categoría de un sistema de información en materia de seguridad modula el equilibrio entre la importancia de la información que gestiona, de los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, con el criterio del principio de proporcionalidad.

Los niveles mínimos de exigencia o de madurez requeridos por el ENS en función de la categoría de cada sistema son los siguientes:

Cuadro 4. Nivel de madurez exigido a las categorías de sistemas

Categoría del sistema	Nivel mínimo de exigencia/madurez requerida
Básica	N2 – Reproducible, pero intuitivo (50%)
Media	N3 – Proceso definido (80%)
Alta	N4 – Gestionado y medible (90%)

Fuente: Guía de seguridad de las TIC. CCN-STIC-824. Informe nacional del estado de seguridad de sistemas TIC.

Los sistemas auditados en esta fiscalización, teniendo en cuenta los servicios y la información que gestionan y de acuerdo con el criterio del ENS, deberían considerarse como una categoría de seguridad media.

Por lo tanto, se ha analizado si los resultados obtenidos de acuerdo con el modelo de nivel de madurez alcanzan el nivel mínimo de exigencia requerido, que en este caso es el N3, Proceso definido, y un índice de madurez del 80%.

La guía CCN-STIC-824[5] presenta una serie de indicadores de madurez y de cumplimiento que permiten aportar información resumida sobre el estado de la seguridad en los organismos públicos. Estos indicadores se han adaptado para poderlos aplicar a los trabajos de revisión de los 8 CBCS para permitir evaluar el estado de las medidas de seguridad del ente auditado.

Los indicadores son los siguientes:

- Índice de madurez, que sintetiza, en tanto por ciento, el nivel de madurez alcanzado por la entidad respecto del conjunto de controles de ciberseguridad.
- Índice de cumplimiento, que también evalúa el nivel de madurez obtenido, pero en relación con la exigencia aplicable en cada caso según la categoría del sistema. Es decir, compara el índice de madurez alcanzado con el nivel mínimo que se exige para esta categoría en el ENS. Para esta fiscalización el nivel mínimo exigido es el N3, Proceso definido, con un porcentaje del 80%.

Gobernanza de la ciberseguridad

A efectos de este trabajo, se entenderá por gobernanza de la seguridad de la información y las comunicaciones el conjunto de responsabilidades y actividades realizadas por los órganos de gobierno con el objetivo de proporcionar una dirección estratégica en esta materia,

5. Guía de seguridad de las TIC. CCN-STIC-824. Informe nacional del estado de seguridad de sistemas TIC.

garantizando que se alcancen los objetivos, verificando que el riesgo se gestione adecuadamente y comprobando que los recursos se utilizan de modo responsable.

Los principales elementos de una buena gobernanza de la ciberseguridad se incluyen, implícitamente, en el ENS y en la normativa relativa a la protección de datos de carácter personal, y ambas normas se revisan en el CBCS 8.

Aun así, dada la importancia que tiene para la ciberresiliencia, se destaca de forma explícita la evaluación que la Sindicatura hace de la gobernanza existente basándose en la implicación de los órganos de gobierno y analizada a partir de lo previsto en la GPF-OCEX 5314, Gobernanza de la ciberseguridad y su auditoría. Se destacan los siguientes aspectos:

- La existencia de políticas de seguridad de la información aprobadas por los órganos de gobierno y su revisión periódica.
- La disposición de normativa y procedimientos de seguridad debidamente aprobados y comunicados a las partes interesadas.
- La asignación de roles y de responsables en materia de seguridad. El responsable de la información y del servicio pueden ser la misma persona, pero debe ser diferente del responsable de la seguridad y del sistema.
- La existencia de un comité de seguridad de la información.
- Recursos humanos y materiales destinados a mejorar los controles de la ciberseguridad.

3. CONCLUSIONES

La Sindicatura de Cuentas de Cataluña, en virtud de lo dispuesto por su ley de creación, de acuerdo con lo previsto en el Programa anual de actividades, de conformidad con los principios fundamentales de fiscalización de los órganos de control externo y las normas internacionales de auditoría adaptadas al sector público, ha fiscalizado con una seguridad limitada los controles básicos de ciberseguridad del Ayuntamiento de Badalona con el alcance y la metodología descritos en el apartado 1.1 y el apartado 2 de este informe, respectivamente.

En los siguientes apartados se incluyen las conclusiones más significativas que se han puesto de manifiesto con motivo del trabajo de seguridad limitada realizado, en los aspectos de ciberseguridad.

1) Índice de madurez

La fiscalización realizada y los indicadores reflejan la situación a 19 de junio de 2024. El grado de control en la gestión de los CBCS, de acuerdo con el alcance señalado en el apartado 1.1, llega a un índice de madurez del 51,38%, que corresponde a un nivel N2, Repetible, pero intuitivo. Es decir, los procesos siguen una pauta regular cuando distintas personas realizan determinados procedimientos, pero no existen procedimientos escritos ni actividades formativas.

Los resultados de las conclusiones sobre el nivel de madurez se fundamentan en los procesos teóricos, en los procedimientos aprobados y también en la verificación de su aplicación práctica, considerando los subcontroles que configuran cada CBCS. Los resultados se muestran detalladamente en el siguiente cuadro:

Cuadro 5. Índice de madurez, nivel de madurez e índice de cumplimiento

Control		Índice de madurez (%)	Nivel de madurez*	Índice de cumplimiento (%)
CBCS 1	Inventario y control de dispositivos físicos	65,00	N2	81,25
CBCS 2	Inventario y control de *software* autorizado y no autorizado	60,00	N2	75,00
CBCS 3	Proceso continuo de identificación y corrección de vulnerabilidades	45,00	N1	56,25
CBCS 4	Uso controlado de privilegios administrativos	38,00	N1	47,50
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	35,00	N1	43,75
CBCS 6	Registro de la actividad de los usuarios	30,00	N1	37,50
CBCS 7	Copias de seguridad de datos y sistemas	70,00	N2	87,50
CBCS 8	Cumplimiento de legalidad	68,00	N2	85,00
Índice general		**51,38**	**N2**	**64,22**

Fuente: Elaboración propia.

* Hay 6 niveles de madurez, que se identifican y se definen en el cuadro 3.

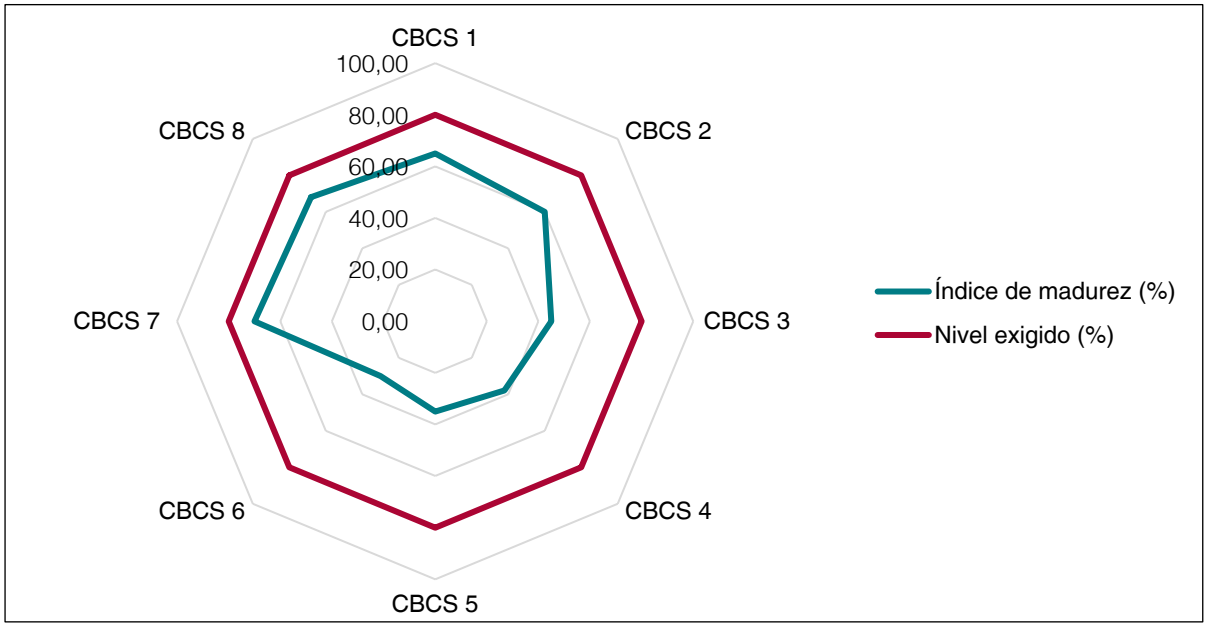
El índice de cumplimiento general de los CBCS es del 64,22%, que es el resultado de comparar el índice de madurez alcanzado con el nivel requerido del sistema de acuerdo con el ENS, que, tal y como se ha dicho, para esta fiscalización es el nivel N3.

Hay que tener en cuenta que la política de seguridad y los procedimientos se han aprobado entre el inicio de las actuaciones y el análisis de las evidencias, por lo que los niveles de madurez de algún control han sido superiores por este hecho. Por otro lado, la Comisión de Seguridad también se ha constituido después del inicio de actuaciones. En el análisis indi-

vidual de cada CBCS se ha tenido en cuenta si lo que se había aprobado era lo que se estaba aplicando en el momento del control de las evidencias.

En el siguiente gráfico se presenta el índice de madurez de cada CBCS respecto del objetivo previsto según lo que el ENS requiere:

Gráfico 2. Índice de madurez y objetivos de los CBCS



Fuente: Elaboración propia.

Como se puede observar, ninguno de los controles alcanza un índice de madurez del 80%, y el CBCS 7, Copias de seguridad de datos y sistemas, es el que más se acerca al nivel exigido, ya que alcanza un índice de madurez del 70% y de cumplimiento del 87,50%. La peor situación es la del CBCS 6, Registro de la actividad de los usuarios, con un índice de madurez del 30% y de cumplimiento del 37,50%.

En el caso del CBCS 3, Proceso continuo de identificación y corrección de vulnerabilidades, el CBCS 4, Uso controlado de privilegios administrativos, el CBCS 5, Configuraciones seguras del *sotfware* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y el CBCS 6, Registro de la actividad de los usuarios, el nivel de madurez alcanzado es el N1, que significa que el proceso existe, pero no se gestiona.

El nivel alcanzado de los controles revisados muestra una efectividad insuficiente. Hay que tener en cuenta que el Ayuntamiento debería tener una categoría del sistema de nivel medio, que corresponde a un nivel de madurez N3, Proceso definido (véase el apartado 5.1).

2) Gobernanza de la ciberseguridad

Los órganos de gobierno del Ayuntamiento son los principales responsables de la existencia de los controles adecuados sobre los sistemas de la información y de las comunicaciones, y su implicación, compromiso y liderazgo constituyen, probablemente, el factor más importante para la implantación eficaz de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Hay compromiso con la ciberseguridad por parte de los órganos de gobierno del Ayuntamiento y de los gestores y responsables de las áreas revisadas, sin embargo, se han identificado algunas debilidades. Las más significativas son las siguientes (véase el apartado 5.2):

- El rol de responsable de la información y de responsable del servicio recae en la misma persona, la cual no tiene el nivel de responsabilidad adecuada en el Ayuntamiento para desarrollar las funciones.
- El Ayuntamiento no dispone de ningún Plan estratégico TIC o documento equivalente.
- Falta de recursos humanos asignados al Departamento de Informática y TIC.

3) Cumplimiento normativo

Los máximos órganos de dirección del Ayuntamiento tienen la responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales y deben impulsar las medidas necesarias para corregir la situación. La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel de cumplimiento satisfactorio (véase el apartado 5.1.8).

4) Aplicación del Real decreto 311/2022

A la finalización de la redacción de este informe (octubre de 2024) el Ayuntamiento no había acreditado la adecuación al ENS, pero ha iniciado los trámites para aprobar la normativa y los procedimientos que le faltaban para dar cumplimiento al Real decreto 311/2022, aunque estos procedimientos no se encuentran completamente implementados.

En lo referente a los 4 controles adicionales revisados sobre la gestión de los usuarios y los derechos de acceso a los sistemas, requeridos para cumplir con lo previsto en el Real decreto 311/2022, se han observado unos índices de madurez superiores al CBCS 4, Uso controlado de privilegios administrativos, con unos índices de cumplimiento general del 70,31%, aunque no alcanzan el nivel mínimo de seguridad exigido por la falta de procedimientos documentados de las prácticas que habitualmente se llevan a cabo (véase el apartado 5.3).

4. RECOMENDACIONES

A continuación, se incluyen las recomendaciones sobre algunos aspectos que se han puesto de manifiesto durante el trabajo de fiscalización de seguridad limitada de acuerdo con el objeto y alcance del informe descritos en la introducción, que ayudarían al Ayuntamiento a mejorar los niveles de madurez de los controles indicados en el apartado anterior. También se señalan las medidas que deben adoptarse para el cumplimiento de la legalidad.

1. Habría que implementar completamente los manuales y procedimientos aprobados y ponerlos en conocimiento del personal implicado con acciones formativas.

2. Debería elaborarse un plan de mantenimiento del *software* e identificar y actualizar todos los sistemas operativos que están fuera del período de apoyo.

3. Se recomienda elaborar un listado de *software* autorizado y llevar a cabo revisiones periódicas y con una frecuencia mínima en los dispositivos para detectar el *software* no autorizado.

4. Deberían realizarse periódicamente análisis de vulnerabilidades y test de penetraciones.

5. Para un uso racional de los privilegios de administrador, los usuarios con este privilegio deberían disponer adicionalmente de un usuario nominativo sin privilegios para llevar a cabo los trabajos habituales.

6. Se recomienda centralizar los registros de actividades de los usuarios en una única herramienta y realizar revisiones de estos registros.

7. Habría que dedicar más recursos humanos al Departamento de Informática y TIC, teniendo en cuenta la falta de personal especialista en proyectos y en seguridad, y previendo la reposición del personal cercano a la fecha de jubilación.

5. RESULTADOS DE LA FISCALIZACIÓN

En la GPF-OCEX 5311, Ciberseguridad, seguridad de la información y auditoría externa, se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas.

Todas las entidades públicas deben implementar controles sobre la seguridad de la información y las comunicaciones, de acuerdo con las directrices establecidas en el ENS, que es de obligado cumplimiento.

Dado el alcance tan amplio de las medidas previstas en el ENS, su complejidad y la intensa dedicación que requiere una revisión completa de su cumplimiento, el 12 de noviembre de 2018, en la Conferencia de presidentes de los Órganos de Control Externo se aprobó la GPF-OCEX 5313, en la que se definieron 8 CBCS que mantenían la máxima coherencia con los postulados del ENS.

Los 8 CBCS son controles globales formados por 26 subcontroles, detallados en el cuadro 8 del anexo. Si se aplican correctamente los 7 primeros controles hay una importante reducción del riesgo frente a posibles ciberataques.

5.1. CONTROLES BÁSICOS DE CIBERSEGURIDAD

Los procedimientos de esta fiscalización y la ejecución del trabajo de campo siguen el contenido de la GPF-OCEX 5313, y en concreto los cuestionarios y fichas de revisión incluidos en los anexos 2 y 3, respectivamente, de dicha guía.

A continuación, se presentan los hallazgos de la auditoría que sustentan las conclusiones y recomendaciones de este informe, como resultado de la revisión de los 8 CBCS. La información se mostrará manteniendo la máxima confidencialidad posible, dado el carácter sensible de la información revisada y el riesgo que su difusión significaría sobre la seguridad de los sistemas de la información de la entidad. La información totalmente detallada solo se ha facilitado al Ayuntamiento.

5.1.1. Inventario y control de dispositivos físicos (CBCS 1)

El CBCS 1 ayuda a las organizaciones a definir qué deben defender. El inventario de los dispositivos físicos debe ser tan completo como sea posible, y en cualquier caso debe saberse qué hay en la red para que pueda ser defendido y, posteriormente, impedir que dispositivos no autorizados se unan a la red.

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todos los dispositivos de *hardware* en la red, de modo que solo los dispositivos autorizados tengan acceso a ellos.

Situación del control

El Ayuntamiento dispone de una herramienta desarrollada internamente para la gestión del inventario de activos y de una herramienta específica para el mantenimiento del inventario, en la cual se hacen constar los responsables de los activos.

El procedimiento aprobado por el Ayuntamiento no recoge la frecuencia de revisión del inventario de activos ni se indican los responsables de llevar a cabo estas revisiones.

Aunque el Ayuntamiento efectúa determinados controles de acceso en la red se han detectado carencias vinculadas con la efectividad de este control que se han notificado directamente al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo al control de activos físicos, la valoración general alcanza un 65% del índice de madurez, que corresponde a un nivel de madurez N2, Repetible, pero intuitivo; es decir, los procesos siguen una pauta regular cuando distintas personas llevan a cabo determinados procedimientos, pero no hay procedimientos escritos ni actividades formativas.

5.1.2. Inventario y control del *software* autorizado y no autorizado (CBCS 2)

La finalidad del CBCS 2 es asegurar que solo está permitido ejecutar *software* autorizado en los sistemas de la organización y que se impide la ejecución de *software* potencialmente vulnerable.

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todo el *software* en la red, de forma que solo se pueda instalar y ejecutar *software* autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

Situación del control

Se ha analizado la gestión que el Ayuntamiento realiza del inventario del *software* y se ha comprobado que no dispone de ningún listado de *software* autorizado, aunque los usuarios no son administradores locales y por lo tanto no pueden instalar *software*. La misma herramienta que gestiona el mantenimiento del inventario de activos físicos se utiliza para revisar el *software* instalado en los equipos.

En lo referente al *software* con soporte del fabricante, se ha comprobado que no existe un plan de mantenimiento de este *software* de acuerdo con las especificaciones de los fabricantes y se ha detectado *software* que está fuera del soporte del fabricante.

En relación con el control de *software* no autorizado no existe ningún procedimiento aprobado, aunque se aplican guías de instalación y refuerzo de la seguridad de los sistemas. Las carencias detectadas en relación con este *software* se han notificado directamente al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo al control de *software* autorizado y no autorizado, la valoración general alcanza un 60% del índice de madurez, que corresponde a un nivel de madurez N2, Repetible, pero intuitivo; es decir, los procesos siguen una pauta regular cuando distintas personas llevan a cabo determinados procedimientos, pero no hay procedimientos escritos ni actividades formativas.

5.1.3. Proceso continuo de identificación y corrección de vulnerabilidades (CBCS 3)

El CBCS 3 está definido para identificar y, en su caso, eliminar las debilidades técnicas existentes en los sistemas de información de la organización y permite reducir la probabilidad de que los sistemas sean vulnerables.

Objetivo del control

Disponer de un proceso continuo de revisión que permita obtener información sobre nuevas vulnerabilidades, identificarlas, corregirlas y reducir la ventana de oportunidad de los atacantes.

Situación del control

El Departamento de Informática y TIC está suscrito a diferentes boletines de información para recibir alertas de vulnerabilidades, incluyendo las alertas de la Agencia de Ciberseguridad de Cataluña y las del Centro Criptográfico Nacional.

En el plan de puesta en servicio de los sistemas se prevé que deben hacerse pruebas de vulnerabilidades y test de penetración. De la revisión del procedimiento se ha obtenido evidencia que a pesar de estar previstas no se están llevando a cabo.

En relación con la priorización de vulnerabilidades, se dispone de un procedimiento que recoge la obligación de actualizar los sistemas y que estas actualizaciones deben estar recogidas en la herramienta específica, pero no se han obtenido pruebas de que se esté aplicando. En lo referente al procedimiento de priorización de vulnerabilidades no se refiere al análisis, la priorización ni el momento de aplicación de las actualizaciones.

No existe un procedimiento formalizado de seguimiento de vulnerabilidades, pero se ha comprobado que cuando se recibe una alerta relacionada con alguna vulnerabilidad se aplican los parches de modo inmediato.

Al recibir alertas de vulnerabilidades por parte de los fabricantes se ha comprobado que se instalan los parches, pero no se dispone de ningún procedimiento de instalación de estos parches en los dispositivos.

De las evidencias obtenidas en la revisión de este control, relativo al proceso continuo de identificación y corrección de vulnerabilidades, la valoración general alcanza un 45% del índice de madurez, que corresponde a un nivel de madurez N1, Inicial / *ad hoc*; es decir, los procesos existen, pero no se gestionan o su gestión no está correctamente organizada.

5.1.4. Uso controlado de privilegios administrativos (CBCS 4)

El CBCS 4 garantiza que los privilegios de administración de sistemas estén asignados únicamente a los empleados que los necesitan, según las funciones que ejercen, y que la entidad pueda atribuir las acciones administrativas a usuarios individuales.

Objetivo del control

Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en ordenadores, redes y aplicaciones.

Situación del control

De acuerdo con el procedimiento aprobado el personal del departamento de informática debería ser el único con privilegio de administración, pero se ha observado que hay usuarios que no son del departamento que tienen permisos de administrador local y en algunas aplicaciones también se ha detectado la existencia de usuarios con permisos de administración.

El Ayuntamiento no dispone de inventario de los usuarios con privilegio de administración, y estos usuarios no disponen de identificadores únicos en función de las diferentes funciones que hayan de llevar a cabo en el sistema.

Las contraseñas por defecto se cambian antes de la entrada en producción de un sistema, pero en la configuración de los servidores no se ha observado que haya un procedimiento que avise de la necesidad de retirar las cuentas de administración estándares ni del cambio de contraseñas por defecto.

El dominio del sistema está configurado para forzar que los usuarios utilicen contraseñas robustas, pero se han detectado aspectos a mejorar en la gestión de la autenticación de los usuarios con privilegios de administradores que se han notificado directamente al Ayuntamiento.

El Ayuntamiento no dispone de una política o normativa documentada que indique que hay que registrar la actividad de los usuarios en el sistema. Aunque el control está activado en los servidores y bases de datos, no se realizan de forma periódica revisiones en los registros de actividad.

De las evidencias obtenidas en la revisión de este control, relativo al uso controlado de privilegios administrativos, la valoración general alcanza un 38% del índice de madurez, que corresponde a un nivel de madurez N1, Inicial / *ad hoc;* es decir, los procesos existen, pero no se gestionan o su gestión no está correctamente organizada.

5.1.5. Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores (CBCS 5)

El CBCS 5 asegura que la entidad haya reforzado las configuraciones predeterminadas de los fabricantes del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, que están orientadas a facilitar el uso y no necesariamente a garantizar la seguridad. Es importante que se reconfiguren los sistemas de acuerdo con los estándares de seguridad.

Objetivo del control

Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso riguroso de gestión de cambios y configuraciones, para evitar que los atacantes exploten servicios y configuraciones vulnerables.

Situación del control

El Ayuntamiento aplica a los dispositivos maquetas de seguridad antes de su entrada en producción, pero no están basadas en guías de fortificación de seguridad reconocidas, como por ejemplo las del Centro Criptográfico Nacional. Estas maquetas solo se aplican a los equipos de usuarios, pero no a los servidores.

La configuración de los equipos y el *software*, una vez puestos en producción, solo puede ser alterada por los miembros del departamento de informática, pero no hay ningún procedimiento que defina la frecuencia y los motivos por los cuales hay que modificar la configuración inicial.

En cuanto a la gestión de la configuración que lleva a cabo el Ayuntamiento se han encontrado otros aspectos a reforzar que se han notificado directamente al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo a las configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, la valoración general alcanza un 35% del índice de madurez, que corresponde a un nivel de madurez N1, Inicial / *ad hoc*; es decir, los procesos existen, pero no se gestionan o su gestión no está correctamente organizada.

5.1.6. Registro de la actividad de los usuarios (CBCS 6)

El CBCS 6 está definido para establecer si todos los sistemas y aplicaciones tienen habilitadas las trazas de auditoría, incluidas las respuestas a las preguntas *desde dónde*, *quién*, *qué* y *cuándo*, y si tienen definidas acciones de alerta. Un ataque al sistema podría pasar desapercibido de modo indefinido y con daños irreversibles si no hay un registro de auditoría.

Objetivo del control

Recoger, gestionar y analizar registros de acontecimientos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Situación del control

No disponen de una política o normativa documentada que indique qué actividades deben registrarse. Todo y así, el registro de actividad de los usuarios está habilitado por los servidores, las bases de datos y el dominio activo, y recoge las acciones tanto de los usuarios generales como de los usuarios administradores.

Únicamente los usuarios administradores pueden acceder al registro de actividades y no se ha podido comprobar cuál es el período de conservación de estos registros. El Ayuntamiento no utiliza ninguna herramienta o sistema automático que recoja todos los registros ni que correlacione los acontecimientos.

Se han detectado algunos aspectos a reforzar respecto al registro de actividades de los usuarios que se han notificado directamente al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo al registro de la actividad de los usuarios, la valoración general alcanza un 30% del índice de madurez, que corresponde a un nivel de madurez N1, Inicial / *ad hoc*; es decir, los procesos existen, pero no se gestionan o su gestión no está correctamente organizada.

5.1.7. Copias de seguridad de datos y sistemas (CBCS 7)

El CBCS 7 determina si la organización tiene una capacidad fiable de recuperación de datos, cuando se descubren atacantes de los sistemas, ya que a menudo estos atacantes cambian significativamente las configuraciones y el *software*, y puede ser extremadamente difícil eliminar todos los aspectos de su presencia en los sistemas.

Objetivo del control

Utilizar procesos y herramientas para hacer la copia de seguridad de la información crítica con una metodología probada que permita recuperar la información en un tiempo oportuno.

Situación del control

El procedimiento de las copias de seguridad está definido y es adecuado. Se realizan copias de seguridad que permiten recuperar datos perdidos y estas copias de seguridad abarcan las aplicaciones, los datos de configuración, los servicios y los registros.

La frecuencia con la que se deben realizar las pruebas de recuperación de las copias de seguridad está recogida en el procedimiento aprobado, pero estas pruebas solo se realizan bajo petición de los usuarios.

Las copias de seguridad tienen la misma seguridad que los datos originales en cuanto a integridad, confidencialidad, autenticidad y trazabilidad, aunque se han detectado aspectos a reforzar relacionados con la protección de las copias de seguridad que se han notificado directamente al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo a las copias de seguridad de datos y sistemas, la valoración general alcanza un 70% del índice de madurez, que corresponde a un nivel de madurez N2, Repetible, pero intuitivo; es decir, los procesos siguen una pauta regular cuando distintas personas llevan a cabo determinados procedimientos, pero no hay procedimientos escritos ni actividades formativas.

5.1.8. Cumplimiento de legalidad (CBCS 8)

La normativa que afecta directamente a los sistemas de la información es amplia y variada. Con el CBCS 8 se revisa el cumplimiento de los principales aspectos normativos relacionados con la seguridad de la información.

Objetivo del control

Asegurar el cumplimiento de la normativa básica en materia de seguridad de la información.

Situación del control

a) Cumplimiento del ENS

El Ayuntamiento dispone de una política de seguridad escrita y aprobada en febrero de 2024, ha formalizado un documento con la declaración de aplicabilidad, y ha enviado los datos necesarios para el Informe del estado de la seguridad (Informe INES). Por otro lado, no se ha hecho la auditoría de certificación del ENS.

b) Cumplimiento de la Ley orgánica de protección de datos y del Reglamento general de protección de datos

En relación con las obligaciones relativas a la Protección de Datos, la designación del delegado de protección de datos recae en una empresa privada y se dispone del registro de actividad de tratamiento actualizado a diciembre de 2023.

No se dispone de un análisis de riesgos de los tratamientos de datos ni tampoco se ha realizado ninguna auditoría en materia de protección de datos personales.

c) Cumplimiento de legalidad del registro de facturas

De acuerdo con la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público, los órganos de control interno deben elaborar anualmente una auditoría de sistemas para verificar que los correspondientes registros contables de facturas cumplen con las condiciones de funcionamiento previstas en la Ley y en su normativa de desarrollo.

El Ayuntamiento realiza esta auditoría, pero bienalmente, y no anualmente. La última auditoría realizada por el Ayuntamiento es del ejercicio 2021 y se ha comprobado que recoge lo mínimo establecido en la Guía para las auditorías de los registros contables de facturas elaborada por la Intervención General de la Administración del Estado.

Índice de madurez

De las evidencias obtenidas en la revisión de este control, relativo al cumplimiento de legalidad, la valoración general alcanza un 68% del índice de madurez, que corresponde a un nivel de madurez N2, Repetible, pero intuitivo; es decir, los procesos siguen una pauta regular

cuando distintas personas llevan a cabo determinados procedimientos, pero no hay procedimientos escritos ni actividades formativas.

5.2. GOBERNANZA DE LA CIBERSEGURIDAD

La gobernanza es el proceso de establecer y mantener un marco de referencia, y prestar apoyo a la estructura y a los procesos de gestión. Existe un liderazgo efectivo, procesos sólidos y estrategias de acuerdo con los objetivos de la organización.

La responsabilidad sobre este proceso es de alta dirección, que, en el caso de las entidades locales, corresponde a su presidente y a la Junta de Gobierno. Ellos son los responsables de garantizar que el funcionamiento de la organización es conforme a las normas aplicables y que existen unos controles adecuados sobre los sistemas de información y las comunicaciones. La responsabilidad de la ejecución de las actividades establecidas por la alta dirección corresponde a los gestores, que conforman la dirección ejecutiva del ente.

Los órganos superiores han mostrado un compromiso e implicación reciente con la ciberseguridad que implica una mejora en la gobernanza de ciberseguridad, pero con carencias y con medidas y procesos de seguridad pendientes de aplicar. Durante el trabajo de fiscalización se han puesto de manifiesto las siguientes debilidades:

- El rol de responsable de la información y de responsable del servicio recae en la misma persona, la cual no tiene el nivel de responsabilidad adecuado en el Ayuntamiento para desarrollar las funciones, que debería tener un perfil directivo y/o ejecutivo.

- El responsable de la seguridad (del ENS) debe ser el secretario del Comité de Seguridad, pero en el caso del Ayuntamiento el secretario del comité es la misma persona designada como responsable de la información y responsable del servicio.

- El Ayuntamiento no dispone de un plan estratégico TIC o documento equivalente.

- Falta personal de sistemas para llevar a cabo con garantías todo lo relativo al mantenimiento del sistema y la ciberseguridad.

- No hay ningún plan de formación en el ámbito de la ciberseguridad.

No obstante, se han identificado algunos aspectos positivos:

- El Ayuntamiento dispone tanto de la política de seguridad de la información como de una serie de normativa y procedimientos de seguridad. Estos documentos han sido aprobados durante el transcurso de los trabajos de fiscalización.

- El Ayuntamiento ha realizado un análisis de los riesgos referente al año 2024 para garantizar la seguridad de la información y ha aprobado un procedimiento de elaboración, actualización y gestión de los análisis de riesgos y de impacto.

5.3. APLICACIÓN DEL REAL DECRETO 311/2022

El Real decreto 3/2010, de 8 de enero, reguló el ENS y determinó la política de seguridad que debía aplicarse en la utilización de medios electrónicos. El 5 de mayo de 2022 entró en vigor el Real decreto 311/2022, que derogaba el anterior y que actualizó el marco normativo y lo adecuó al contexto estratégico existente para garantizar la seguridad en la administración digital.

De acuerdo con los objetivos y el alcance descritos en el apartado 1.1, una vez revisados los 8 controles básicos se ha ampliado la valoración efectuada de la situación del Ayuntamiento con una selección adicional de controles revisados y la revisión de las acciones efectuadas.

Este análisis ha tenido 2 vertientes: la primera ha sido la evaluación de una selección de controles adicionales relacionados con la gestión de los usuarios y los derechos de acceso a los sistemas, y la segunda, la revisión de las acciones llevadas a cabo por el Ayuntamiento entre la finalización del trabajo de campo y la redacción del informe para alcanzar el cumplimiento del Real decreto 311/2022.

En la GPF-OCEX 5330, Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica, se prevén 24 controles generales, clasificados en 5 categorías, alineados con los requerimientos previstos por el ENS. De estos 24 controles, 7[6] se refieren a los controles básicos analizados y valorados en los apartados anteriores.

Para ampliar la valoración efectuada de los 8 controles básicos, la Sindicatura ha incluido la revisión de 4 controles adicionales clasificados en la categoría de Controles de acceso a datos y programas, por considerarlos los más relevantes de entre los controles generales que faltaba revisar. En el siguiente cuadro se incluyen todos los controles de la categoría seleccionada.

6. Los CBCS 1 y 2 están incluidos en el mismo control general C1, Inventario de *hardware* y *software*, de la GPF-OCEX 5330.

Cuadro 6. Controles de acceso a datos y programas

D.1: Uso de controles de privilegios administrativos (CBCS 4) *
D.2: Mecanismo de identificación y autenticación
D.3: Gestión de derechos de acceso
D.4: Gestión de usuarios
D.5: Protección de redes y comunicaciones

Fuente: GPF-OCEX 5330.
* Analizado en el apartado 5.1.4.

La ejecución del trabajo de valoración de estos 4 controles sigue el contenido de la GPF-OCEX 5330, y en concreto los cuestionarios incluidos en el anexo 3 de la guía.

Los índices de cada control adicional revisado se detallan en el siguiente cuadro:

Cuadro 7. Índice de madurez y de cumplimiento de los controles ampliados

Control	Índice de madurez	Nivel de madurez (a)	Índice de cumplimiento
D.2: Mecanismo de identificación y autenticación	55,00	N2	68.75
D.3: Gestión de derechos de acceso	55,00	N2	68.75
D.4: Gestión de usuarios	55,00	N2	68.75
D.5: Protección de redes y comunicaciones	60,00	N2	75,00
Índice general (b)	**56,25**	N2	**70,31**

Fuente: Elaboración propia.
Notas:
(a) Existen 6 niveles de madurez que se identifican y se definen en el cuadro 3.
(b) El CBCS 4 tiene un índice de madurez y de cumplimiento del 38% y del 47,50%, respectivamente, que no se ha tenido en cuenta en la valoración de estos controles adicionales.

En lo referente al resultado de la revisión de los controles y subcontroles seleccionados, destaca la protección de redes y comunicación, con un índice de cumplimiento del 75%. El resto de los controles alcanza el mismo índice de cumplimiento, que es del 68,75%.

El índice de cumplimiento general de estos 4 controles se sitúa ligeramente por encima del 70% y es superior al del CBCS 4, Uso controlado de privilegios administrativos, que es del 47,50%. Esto significa que tiene unas prácticas de seguridad implantadas que se llevan a cabo puntualmente, y alguna de forma periódica, pero que no han sido documentadas o están documentadas, pero no se aplican completamente.

En cuanto a los trabajos llevados a cabo por el Ayuntamiento para dar cumplimiento al Real decreto 311/2022, a la fecha de redacción de este informe (octubre de 2024) no se había acreditado la adecuación al ENS, pero hay que destacar las siguientes acciones:

- El Ayuntamiento ha iniciado contactos con empresas especializadas en sistemas y seguridad para realizar una auditoría de la infraestructura TIC.

- El Ayuntamiento ha solicitado el servicio gratuito de Localret de inventario y evaluación de la infraestructura TIC.

6. RESPONSABILIDADES

6.1. DE LA DIRECCIÓN DE LA ENTIDAD

Los órganos de gobierno del Ayuntamiento son los responsables de que haya unos controles adecuados sobre los sistemas de información y las comunicaciones. De acuerdo con sus competencias, deben garantizar que el funcionamiento de la entidad sea conforme a las normas aplicables y que los controles internos proporcionen una garantía razonable de que la información, los servicios y los sistemas de información que les apoyan cumplan las 5 dimensiones de seguridad de la información que establece el ENS: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

6.2. DE LA SINDICATURA

Los objetivos, el alcance y la metodología utilizada en el trabajo de fiscalización de la Sindicatura, de acuerdo con lo que se expone en el apartado 1.1 y en el apartado 2, son obtener una seguridad limitada sobre la situación de los controles básicos de ciberseguridad revisados.

Los procedimientos realizados en una auditoría de seguridad limitada son reducidos en comparación con los que se requieren para obtener una seguridad razonable, pero se espera que el nivel de seguridad sea, de acuerdo con el juicio profesional del auditor, significativo para los destinatarios del informe. La seguridad limitada no garantiza que una fiscalización realizada de acuerdo con los principios fundamentales de fiscalización de los órganos de control externo y las normas internacionales de auditoría adaptadas al sector público detecte siempre un incumplimiento cuando existe.

El detalle de los resultados de la fiscalización contiene información de carácter reservado que, de difundirse, podría llegar a afectar seriamente la seguridad de los sistemas de información de la entidad. Por este motivo, se ha proporcionado a los responsables correspondientes el contenido detallado de cada uno de los controles revisados, con carácter confidencial y por canales cifrados, para que se puedan adoptar las medidas correctoras oportunas. El Ayuntamiento deberá determinar el uso y la publicidad que estime pertinentes, de acuerdo con la valoración de esta confidencialidad. En consecuencia, los resultados del trabajo realizado y las conclusiones que constan en este informe se presentan de forma sintética.

7. ANEXO: LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD Y SUS SUBCONTROLES

Cuadro 8. Los controles básicos de ciberseguridad y sus subcontroles

Control		Objetivo del control	Subcontroles
CBCS 1	Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos de *hardware* en la red, de modo que solo los dispositivos autorizados tengan acceso a la red.	CBCS 1-1: Inventario de activos físicos autorizados La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.
			CBCS 1-2: Control de activos físicos no autorizados La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso a dispositivos físicos no autorizados.
CBCS 2	Inventario y control de *software* autorizado	Gestionar activamente todo el *software* en los sistemas, de modo que solo se pueda instalar y ejecutar *software* autorizado.	CBCS 2-1: Inventario de *software* autorizado La entidad dispone de un inventario de *software* completo, actualizado y detallado.
			CBCS 2-2: *Software* con soporte del fabricante El *software* utilizado por la entidad tiene soporte del fabricante. En caso contrario, se marca en el inventario como fuera de soporte.
			CBCS 2-3: Control de *software* no autorizado La entidad dispone de mecanismos que impiden la instalación y la ejecución de *software* no autorizado.
CBCS 3	Proceso continuo de identificación y solución de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, solucionarlas y reducir la ventana de oportunidad a los atacantes.	CBCS 3-1: Identificación de vulnerabilidades Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que se identifican en tiempo oportuno.
			CBCS 3-2: Priorización de vulnerabilidades Las vulnerabilidades identificadas se analizan y priorizan para resolverlas según el riesgo que suponen para la seguridad del sistema.
			CBCS 3-3: Resolución de vulnerabilidades Se realiza un seguimiento de la corrección de las vulnerabilidades identificadas, de modo que se garantiza que se resuelven en el tiempo previsto en el procedimiento.
			CBCS 3-4: Parches La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.

Control		Objetivo del control	Subcontroles
CBCS 4	Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y la configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	CBCS 4-1: Inventario y control de cuentas de administración Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita el control correcto.
			CBCS 4-2: Cambio de contraseñas por defecto Las contraseñas por defecto de las cuentas que no se utilizan o bien las que son estándar se cambian antes de la entrada en producción del sistema.
			CBCS 4-3: Uso exclusivo de cuentas de administración Las cuentas de administración solo se utilizan para las tareas estrictamente necesarias.
			CBCS 4-4: Mecanismos de autenticación Las cuentas de administración están sujetas a robustos mecanismos de autenticación, que impiden el acceso no autorizado por medio de estas cuentas.
			CBCS 4-5: Auditoría y control del uso de las cuentas con privilegios de administración El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer, implantar y gestionar la configuración de seguridad, por medio de un proceso riguroso de control de cambios y gestión de la configuración, con el objetivo de prevenir ataques por medio de la explotación de servicios y configuraciones vulnerables.	CBCS 5-1: Configuración segura La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y *software*.
			CBCS 5-2: Gestión de la configuración La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (retorno a la configuración segura) en un período de tiempo oportuno.
CBCS 6	Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)	Recoger, gestionar y analizar *logs* de incidencias que pueden ayudar a detectar, entender o recuperarse de un ataque.	CBCS 6-1: Activación de *logs* de auditoría El *log* de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ciberataques.
			CBCS 6-2: Almacenamiento de *logs*: conservación y protección Los *logs* se conservan durante el tiempo indicado en la política de retención, de modo que están disponibles para su consulta y análisis. Durante este período, el control de acceso garantiza que no se producen accesos no autorizados.

Control		Objetivo del control	Subcontroles
			CBCS 6-3: Centralización y revisión de los registros de la actividad de los usuarios Los *logs* de todos los sistemas se revisan periódicamente para detectar anomalías y posibles riesgos de seguridad del sistema. Se dispone de mecanismos para la centralización de los *logs* de auditoría, de modo que se facilita su revisión.
			CBCS 6-4: Monitorización y correlación La entidad dispone de un SIEM (sistema de gestión de incidencias e información de seguridad) o una herramienta de analítica de *logs* para la correlación y el análisis.
CBCS 7	Copia de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	CBCS 7-1: Copia de seguridad de datos y sistemas La entidad realiza periódicamente copias de seguridad automáticas de todos los datos y configuraciones del sistema.
			CBCS 7-2: Pruebas de recuperación Se verifica la integridad de las copias de seguridad realizadas de forma periódica y se lleva a cabo un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.
			CBCS 7-3: Protección de las copias de seguridad Las copias de seguridad se protegen adecuadamente por medio de controles de seguridad física o cifrado mientras están almacenadas o bien son transmitidas a través de la red.
CBCS 8	Cumplimiento de legalidad	La entidad cumple los requisitos legales y reglamentarios que le son aplicables.	CBCS 8-1: Cumplimiento del ENS La entidad cumple los requisitos establecidos en el ENS.
			CBCS 8-2: Cumplimiento de la Ley orgánica de protección de datos y del Reglamento general de protección de datos La entidad cumple los requisitos establecidos en la Ley orgánica de protección de datos y en el Reglamento general de protección de datos
			CBCS 8-3: Cumplimiento de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas. La entidad cumple los requisitos establecidos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas.

Fuente: Elaboración propia.

8. TRÁMITE DE ALEGACIONES

De acuerdo con la normativa vigente, el proyecto de informe de fiscalización fue enviado al Ayuntamiento de Badalona el 19 de noviembre de 2024 para cumplir el trámite de alegaciones.

Transcurrido el plazo establecido no se ha recibido ningún escrito de alegaciones del Ayuntamiento de Badalona.

APROBACIÓN DEL INFORME

Certifico que en Barcelona, el 17 de diciembre de 2024, reunido el Pleno de la Sindicatura de Cuentas, presidido por el síndico mayor, Miquel Salazar Canalda, con la asistencia de los síndicos Anna Tarrach Colls, Manel Rodríguez Tió, Llum Rodríguez Rodríguez, Maria Àngels Cabasés Piqué, Ferran Roquer Padrosa y Josep Viñas Xifra, y de la secretaria general de la Sindicatura, Marta Junquera Bernal, actuando como ponente el síndico Manel Rodríguez Tió, previa deliberación se acuerda aprobar el informe de fiscalización 25/2024, relativo al Ayuntamiento de Badalona, controles básicos de ciberseguridad, ejercicio 2023.

Y, para que así conste y surta los efectos que correspondan, firmo esta certificación, con el visto bueno del síndico mayor.

[Firma digital de Marta Junquera Bernal]

La secretaria general

Visto bueno,

[Firma digital de Miquel Salazar Canalda]

El síndico mayor