INFORME 9/2024

AYUNTAMIENTO DE MATARÓ
CONTROLES BÁSICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

INFORME 9/2024

AYUNTAMIENTO DE MATARÓ
CONTROLES BÁSICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

Edición: septiembre de 2024

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	Controles básicos de ciberseguridad
ENS	Esquema Nacional de Seguridad
GPF-OCEX	Guía práctica de fiscalización de los órganos de control externo

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 Mataró (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 relacionan 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: Elaboración propia.

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, la disponibilidad, la autenticidad, la 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 la consideración por parte del auditor de si el control, individualmente o en combinación con otros controles, es capaz de prever de modo eficaz, o 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 eficazmente.

Dada la naturaleza del objeto material a revisar, ha sido necesario delimitar y concretar qué sistemas debían analizarse. Se han revisado las aplicaciones que sustentan los procesos de gestión contable y presupuestaria y la gestión tributaria y recaudatoria, así como 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, que 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

En cuanto al ámbito temporal del trabajo, las conclusiones se refieren a la situación a 31 de diciembre de 2023, 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, se ha ampliado el trabajo efectuado con la valoración de la gobernanza que desempeñan 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. 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 realizado, 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.

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.

3. De acuerdo con lo que prevé 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 expertos externos y profesionales especializados para cubrir este déficit de conocimientos.

1.2. ENTE FISCALIZADO

1.2.1. Actividades y organización

El municipio de Mataró 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 todas las 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 del Ayuntamiento de Mataró son el Pleno, el alcalde, los tenientes de alcalde, la Junta de Gobierno Local y los concejales de regidorías delegadas.

Como órganos complementarios, en el ejercicio fiscalizado, disponía de los siguientes: las comisiones informativas, la Comisión Especial de Cuentas, la Comisión Especial de Organización, los grupos municipales, los portavoces y la Junta de Portavoces.

En lo referente a los entes dependientes, en el ejercicio 2023 el Ayuntamiento tenía constituidas 2 entidades públicas empresariales locales, 2 sociedades mercantiles y 3 fundaciones; además, tenía adscritos 3 consorcios.

Estos entes eran los siguientes:

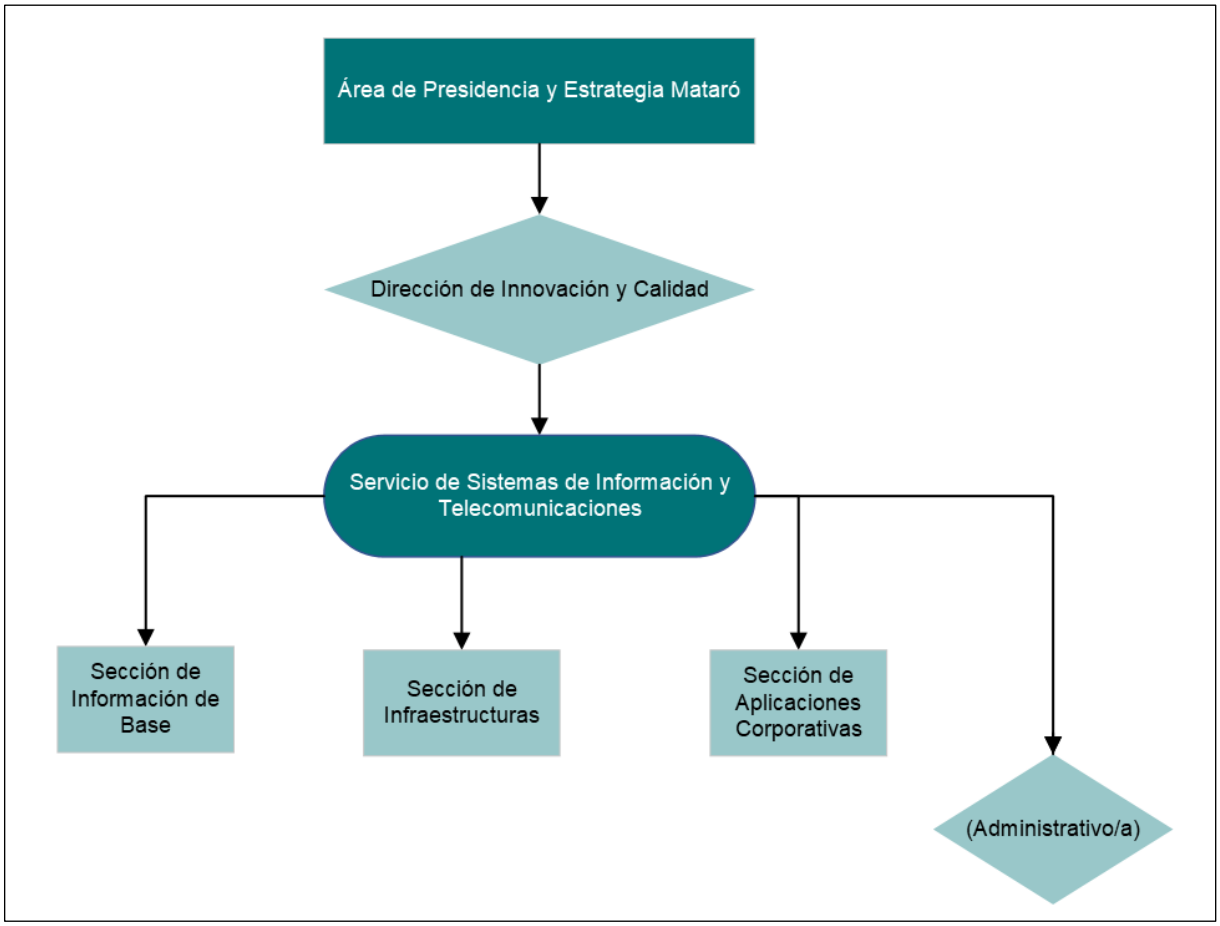
- Mataró Audiovisual[4]
- Parc Tecnocampus Mataró[4]
- Aigües de Mataró, SA
- Promocions Urbanístiques de Mataró, SA
- Fundació Privada Hospital Sant Jaume i Santa Magdalena de Mataró
- Fundació Tecnocampus Mataró-Maresme
- Fundació Unió de Cooperadors de Mataró pel Foment de l'Economía Social i la Rehabilitació Urbana
- Consorcio para el Tratamiento de Residuos Sólidos Urbanos de El Maresme
- Consorcio Transversal Red de Actividades Culturales (CTXAC)
- Consorcio Museo de Arte Contemporáneo de Mataró

4. Entidad pública empresarial local.

b) Organización de la unidad de Servicio de Sistemas de Información y Telecomunicaciones

Desde la unidad de Servicio de Sistemas de Información y Telecomunicaciones se define, planifica y ejecuta la estrategia tecnológica. Esta unidad organizativa depende de la Dirección de Innovación y Calidad, adscrita al Área de Presidencia y Estrategia Mataró. La dependencia y la organización básica de la unidad se muestra en el siguiente gráfico:

Gráfico 1. Organigrama funcional de la unidad de Servicio de Sistemas de Información y Telecomunicaciones



Fuente: Elaboración propia.

Los principales objetivos estratégicos de la unidad de Servicio de Sistemas de Información y telecomunicaciones son:

- Desarrollar y mantener herramientas tecnológicas que den apoyo a la ejecución y la gestión de los procesos de la institución implementando metodologías y mejores prácticas de la ingeniería de *software*.

- Garantizar la existencia de una información cartográfica y alfanumérica veraz, fiable, contrastada y actualizada del término municipal para la gestión y planificación de este territorio y su población.

- Implementar y gestionar una plataforma tecnológica que sea fiable, íntegra y altamente disponible, que admita los procesos del Ayuntamiento, mejorando así el cumplimiento de los funcionarios en sus respectivas actividades.

- Gestionar los sistemas de información y comunicación modernos y con el grado de eficiencia adecuado para dar respuesta a los objetivos estratégicos.

En el ejercicio 2023 el número de plazas asignadas a esta unidad era de 16, ocupadas con 14 funcionarios de carrera, 1 funcionario interino y 1 persona contratada mediante un plan de empleo.

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 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 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).

Nivel	Descripción
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.

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 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.

Nivel	Índice	Descripción
4 – Gestionado y medible	90	La Dirección controla y mide el seguimiento de los procedimientos y adopta medidas correctoras cuando conviene. 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. 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: la confidencialidad, la integridad, la disponibilidad, la autenticidad y la 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:

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

Categoría del sistema	Nivel mínimo de exigencia/madurez requerido
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 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%.

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

Los principales elementos de una buena gobernanza de la ciberseguridad se incluyen, de forma implícita, 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 realiza de la gobernanza existente basándose en la implicación de los órganos superiores y analizada a partir de los siguientes aspectos:

- La existencia de políticas de seguridad de la información aprobadas por el titular del órgano superior 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 este 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 que dispone 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 Mataró 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 la ciberseguridad.

1) Índice de madurez general

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%.

La fiscalización realizada y los indicadores reflejan la situación a 31 de diciembre de 2023. El grado de control en la gestión de los CBCS llega a un índice de madurez general del 53,11%, 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:

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

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

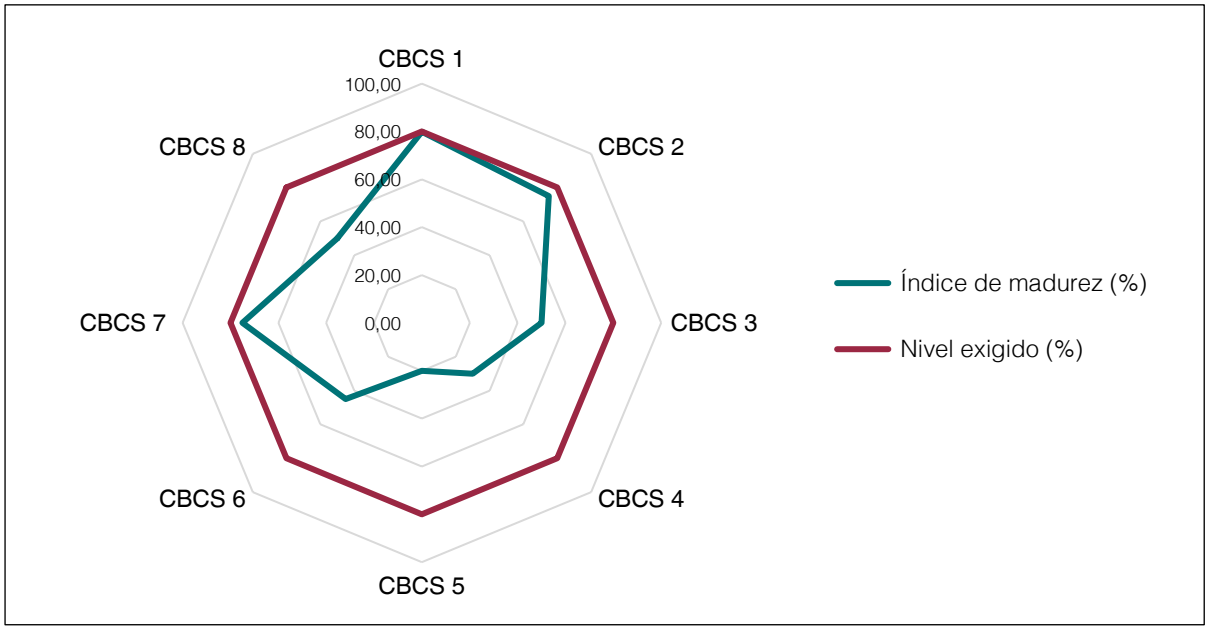
Control		Índice de madurez (%)	Nivel de madurez	Índice de cumplimiento (%)
CBCS 1	Inventario y control de dispositivos físicos	79,90	N2	99,88
CBCS 2	Inventario y control de *software* autorizado y no autorizado	75,00	N2	93,75
CBCS 3	Proceso continuo de identificación y corrección de vulnerabilidades	50,00	N2	62,50
CBCS 4	Uso controlado de privilegios administrativos	30,00	N1	37,50
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	20,00	N1	25,00
CBCS 6	Registro de la actividad de los usuarios	45,00	N2	56,25
CBCS 7	Copias de seguridad de datos y sistemas	75,00	N2	93,75
CBCS 8	Cumplimiento de legalidad	50,00	N2	62,50
Índice general		**53,11**	**N2**	**66,39**

Fuente: Elaboración propia.

El índice de cumplimiento general de los CBCS es del 66,39%, 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.

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 llega a un índice de madurez del 80%, pero hay 3 con índices muy cercanos. El mejor resultado corresponde al CBCS 1, Inventario y control de dispositivos físicos, que alcanza un índice de madurez del 79,90% y de cumplimiento del 99,88%. La peor situación es la del CBCS 5, Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, con un índice de madurez del 20% y de cumplimiento del 25%.

En el caso del CBCS 4, Uso controlado de privilegios administrativos, y el CBCS 5, Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, el nivel de madurez alcanzado es el nivel 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 superiores 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.

Se ha podido verificar la existencia de esta implicación y compromiso con la ciberseguridad por parte de los órganos superiores del Ayuntamiento y de los gestores y responsables de las áreas revisadas. Sin embargo, se han identificado carencias que dificultan la implementación de un sistema completamente efectivo que garantice la ciberresiliencia. Las carencias más significativas son las siguientes (véase el apartado 5.2.):

- La política de seguridad de la información no está completa ni actualizada.
- No se han formalizado ni aprobado todas las normas y los procedimientos de seguridad necesarios.
- Existe dependencia jerárquica entre el responsable de seguridad y el responsable del sistema.
- En el año 2017 se creó el Comité de Seguridad en Protección de Datos, para que hiciese las funciones del Comité de Seguridad de la Información, pero no se ha reunido nunca.

3) Cumplimiento normativo

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel de cumplimiento insatisfactorio. Los máximos órganos de di-

rección 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 (véase el apartado 5.1.8).

4) Aplicación del Real decreto 311/2022

El Ayuntamiento está trabajando en la adaptación al Esquema Nacional de Seguridad promoviendo una serie de acciones e impulsando la aprobación de la normativa que le faltaba. A la finalización de la redacción de este informe (junio de 2024) el Ayuntamiento no había acreditado la adecuación al ENS.

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 índices de cumplimiento por encima del 70%, 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 para el cumplimiento de la legalidad que hay que adoptar.

1. Los órganos de gobierno deberían promover la revisión y actualización de la normativa de seguridad existente e incentivar actuaciones que fomenten la cultura en materia de ciberseguridad con una dirección estratégica y coordinada.

2. Habría que formalizar en manuales y protocolos todos los procedimientos que de forma informal y periódica está llevando a cabo el personal del Ayuntamiento.

3. Dado que el Ayuntamiento dispone de 2 inventarios para el control de los dispositivos físicos, uno con la información de los equipos servidores y de los dispositivos de red y el otro con la de los equipos de usuarios, se recomienda unificarlos en una única herramienta para facilitar el control y la gestión.

4. La unidad responsable de sistemas de la información debería elaborar un plan de mantenimiento del *software* e identificar y actualizar todos los sistemas operativos que están fuera del período de soporte.

5. Habría que 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.

6. Elaborar y aprobar un procedimiento unificado de gestión de usuarios con privilegios de administración que defina las directrices para todos los sistemas de la entidad.

7. Deberían hacerse revisiones periódicas de los registros de actividad y centralizar los registros de todos los sistemas en una sola herramienta.

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 que prevé 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 controles básicos de ciberseguridad 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 estos controles se aplican correctamente implican una reducción alrededor del 85% del riesgo ante los ciberataques.

5.1. PROCEDIMIENTOS DE FISCALIZACIÓN Y EJECUCIÓN DEL TRABAJO

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 el anexo 2 y 3, respectivamente, de la citada guía.

Como resultado de la revisión de los 8 CBCS, a continuación se presentan los hallazgos de la auditoría que sustentan las conclusiones y recomendaciones de este informe. 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 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.

Situación del control

El Ayuntamiento dispone de 2 inventarios de dispositivos físicos. En el primero constan los equipos, servidores, dispositivos de red, etc., mediante una herramienta específica, y en el otro, los equipos de usuario, que se gestionan con una base de datos interna desde el Servicio de Sistemas de Información y Telecomunicaciones.

Se ha comprobado que los 2 inventarios se encuentran completos y cumplen los requerimientos del control, pero no se han formalizado por escrito los procedimientos para dar de alta o baja de estos inventarios los activos.

La red está segmentada en diferentes VLAN[6] que solo permiten los puertos y servicios estrictamente necesarios para la organización. Se ha constatado que se dispone de un *software* para controlar los activos conectados a la organización, y este *software* se revisa periódicamente para detectar en la red equipos no autorizados y su ubicación. Sin embargo, se han detectado algunas carencias que se han comunicado al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo al control de activos físicos, la valoración general alcanza un 79,90% 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 existen procedimientos escritos ni actividades formativas.

6. Red de área local virtual (VLAN por sus siglas en inglés: Virtual LAN). Es una tecnología de redes que permite crear redes lógicas independientes en la misma red física.

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 modo 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 realiza el Ayuntamiento del inventario y control del *software* y se ha verificado que el procedimiento para que los trabajadores del Ayuntamiento soliciten la instalación del *software* no está documentada.

Sin perjuicio de que se revisa el *software* con la misma herramienta que se utiliza para el inventario de *hardware*, el recurso se considera insuficiente ya que el Ayuntamiento no dispone de un listado de *software* autorizado ni lleva a cabo periódicamente un control del *software* no permitido.

En cuanto al *software* con soporte del fabricante, el Ayuntamiento dispone de sistemas operativos sin este soporte y, además, no existe ningún plan de mantenimiento de este *software*.

También se ha comprobado que, aunque el Ayuntamiento no dispone de herramientas específicas para controlar e impedir la instalación de *software* no autorizado, los usuarios no son administradores locales y por lo tanto no tienen la capacidad de instalar *software*.

De las evidencias obtenidas en la revisión de este control, relativo al control del *software* autorizado y no autorizado, la valoración general alcanza un 75% 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 Ayuntamiento utiliza diferentes medios para identificar vulnerabilidades, como la suscripción a comunicaciones de fabricantes o de organismos de referencia, como puede ser el Centro Criptográfico Nacional, entre otros.

La priorización de la resolución de las vulnerabilidades y los defectos de seguridad identificados se hace mediante un procedimiento informal basado en la gestión de riesgos, y este procedimiento no consta formalmente documentado.

Se ha observado que el Ayuntamiento dispone de herramientas para gestionar e instalar parches y actualizaciones de seguridad, aunque el procedimiento a seguir para la instalación de parches no está debidamente formalizado.

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 50% 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 existen procedimientos escritos ni actividades formativas.

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

Todas las cuentas de administración están registradas en un programa al cual solo tienen acceso los técnicos de la sección de infraestructuras y el jefe de servicio.

Solo dispone de privilegios administrativos el personal de sistemas, con un único usuario de administración para todos los miembros del servicio. El resto del personal del Ayuntamiento no dispone de privilegios y todos tienen un identificador único.

En relación con los mecanismos de autenticación, las contraseñas cumplen las reglas básicas de seguridad, pero se ha comprobado que existen ciertas carencias en estos mecanismos.

Las contraseñas por defecto de las cuentas que no se utilizan o bien las que son estándar se eliminan o se renombran antes de la puesta en funcionamiento de un sistema, pero sin que se cumplan todos los requisitos necesarios de fortificación.

El control del uso de las cuentas de administración que realiza el Ayuntamiento ha puesto de manifiesto una serie de debilidades que ya se han notificado al Ayuntamiento.

De las evidencias obtenidas en la revisión de este control, relativo al uso controlado de privilegios administrativos, 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 organizada correctamente.

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

El CBCS 5 controla si las configuraciones predeterminadas de los fabricantes están orientadas a facilitar el uso y no necesariamente 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 lleva a cabo algunas acciones para fortificar o reforzar la seguridad de los sistemas antes de su puesta en marcha, pero no dispone de un procedimiento documentado para hacerlo. Las acciones no son suficientes ni tan completas como deberían ser.

También se han encontrado debilidades en los controles del Ayuntamiento en relación con la detección de cambios no autorizados o erróneos de la configuración para poder corregirlos en un período de tiempo oportuno.

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 20% 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 bien organizada.

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

El CBCS 6 controla si todos los sistemas y aplicaciones tienen habilitadas las trazas de auditoría, incluidas las respuestas a las preguntas des de dónde, quién, qué y cuándo, y si tienen definidas acciones de alerta. En el supuesto de un ataque al sistema, este podría pasar desapercibido de forma indefinida y con daños irreversibles si no existiese 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

El Ayuntamiento dispone de varios sistemas para gestionar los registros de actividad. En cuanto al almacenamiento de *logs* se ha observado un control bastante efectivo. Sin embargo, no se ha formalizado documentalmente qué acontecimientos de seguridad deben ser auditados y con qué periodicidad, el tiempo de retención antes de eliminarlos ni el personal autorizado a acceder a ellos.

De las evidencias obtenidas en la revisión de este control, relativo al registro de la actividad de los usuarios, la valoración general alcanza un 45% 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.

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

El CBCS 7 controla 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 no está documentado formalmente, pero se ha comprobado que desde el Servicio de Sistemas de Información y Telecomunicaciones se hacen copias de seguridad de todos los sistemas críticos, carpetas compartidas y datos sensibles, con los requisitos necesarios para permitir recuperar los datos perdidos.

Estas copias de seguridad tienen la misma seguridad que los datos originales, aunque no se crean copias de seguridad fuera de línea ni se utiliza criptografía para el cifrado de la información.

No existe un calendario definido para la realización de pruebas de restauración a partir de las copias de seguridad y únicamente se hacen restauraciones por necesidad.

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 75% 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 existen 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 de la información, aprobada por decreto de Alcaldía en el año 2019, en la cual se nombraron los principales responsables de la gestión y la seguridad informática. Esta política, sin embargo, no cumple todos los requisitos exigidos por el ENS.

Por otro lado, a la finalización del trabajo (31 de diciembre de 2023) el Ayuntamiento no había hecho la auditoría de cumplimiento del ENS para los sistemas de categoría media y alta, no había formalizado la declaración de aplicabilidad del ENS, ni había formalizado ni enviado los datos necesarios para el informe del estado de la seguridad (Informe INES).

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

En 2021, el Ayuntamiento designó a una funcionaria de carrera como delegada de protección de datos, de manera provisional y en forma de encargo de funciones, y en la fecha de finalización del trabajo no se había provisto el puesto de trabajo por el procedimiento establecido reglamentariamente.

No se dispone de un análisis de riesgos de los tratamientos de datos ni se ha llevado a cabo la auditoría de protección de datos.

c) Cumplimiento de la legalidad del registro de facturas

Se han auditado los sistemas del registro contable de facturas del ejercicio 2022, y se ha observado que cumplen los criterios exigidos por la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas del sector público.

Índice de madurez

De las evidencias obtenidas en la revisión de este control, relativo al cumplimiento de legalidad, la valoración general alcanza un 50% 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 existen 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. Exige 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 existan 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.

Los órganos superiores tienen una implicación y un compromiso con la ciberseguridad que ha quedado evidente durante el trabajo de fiscalización y que implica que se haga una valoración positiva de la gobernanza de ciberseguridad.

A pesar de este compromiso por parte de los responsables, en la fiscalización se han puesto de manifiesto las siguientes debilidades:

- En 2019, el Ayuntamiento aprobó la política de seguridad, pero esta política no ha sido revisada ni actualizada.
- Hay una falta de actividad efectiva y continuada del Comité de Seguridad.
- Existen determinados incumplimientos normativos, detallados en el apartado 5.1.8.

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[7] 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.

7. El 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 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	Índice de cumplimiento
D.2: Mecanismo de identificación y autenticación	56,00	N2	70,00
D.3: Gestión de derechos de acceso	63,30	N2	79,10
D.4: Gestión de usuarios	60,00	N2	75,00
D.5: Protección de redes y comunicaciones	76,00	N2	95,00
Índice general*	**63,80**	**N2**	**79,80**

Fuente: Elaboración propia.
* El CBCS 4 tiene un índice de madurez y de cumplimiento del 30% y del 37,5%, 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 principalmente la protección de las redes y comunicaciones, con un índice de cumplimiento del 95%, seguido de la gestión de derechos de acceso, con un 79,10%.

En conjunto, los subcontroles que integran los aspectos analizados denotan que el Ayuntamiento tiene índices de cumplimiento por encima del 70%, que significa que tiene unas prácticas de seguridad implantadas que se llevan a cabo puntualmente, y alguna de forma periódica, pero no han sido documentadas.

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

- Los órganos de gobierno han promovido la adecuación de la política de seguridad de la información a la normativa. También han impulsado la aprobación de la normativa de seguridad que faltaba aprobar.

- Los diferentes responsables analizaban los posibles riesgos e iban definiendo los procedimientos que se había puesto de manifiesto que faltaba analizar.

- El Ayuntamiento ha contratado una empresa consultora que colabora en la obtención del certificado ISO 27001, relativo a la seguridad y privacidad de la información.

6. RESPONSABILIDADES

6.1. DE LA DIRECCIÓN DE LA ENTIDAD

Los órganos superiores 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 dan soporte 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 CBCS 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 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 se 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 los trabajos estrictamente necesarias.
			CBCS 4-4: Mecanismos de autenticación Las cuentas de administración están sujetas a mecanismos de autenticación robustos, 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 la 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 Mataró el 17 de junio de 2024 para cumplir el trámite de alegaciones.

8.1. ALEGACIONES RECIBIDAS

El escrito de alegaciones presentado por el Ayuntamiento de Mataró, firmado electrónicamente el 2 de julio de 2024, se reproduce a continuación.[8] Los anexos a los que hacen referencia las alegaciones quedan depositados en los archivos de la Sindicatura.

Ajuntament de Mataró

Ayuntamiento de Mataró
La Riera, 48
www.mataro.cat

CARTA

SR. MANEL RODRIGUEZ TIÓ
SÍNDICO
SINDICATURA DE CUENTAS DE CATALUÑA

Apreciado señor:

Visto el informe de fiscalización núm. 28/2023-E que nos ha hecho llegar, con nuestro número de registro de entrada E-08121-2024-042620 de 17 de junio de 2024, correspondiente al Ayuntamiento de Mataró sobre controles básicos de ciberseguridad, ejercicio 2023, revisado por el Pleno de la Sindicatura de Cuentas de Cataluña, para que le presentemos las alegaciones pertinentes hasta el 2 de julio de 2024, le informamos y adjuntamos las correspondientes alegaciones previas a la espera de la emisión del informe definitivo.

Alegación primera

En el apartado "3. CONCLUSIONES" subapartado "2) Gobernanza de la ciberseguridad" donde se dice:

> *"En el año 2017 se creó el Comité de Seguridad en Protección de Datos, para que hiciese las funciones del Comité de Seguridad de la Información, pero no se ha reunido nunca"*

8. El escrito original estaba redactado en catalán. Aquí figura traducido al castellano.

El Ayuntamiento de Mataró informa que el *Comité de Seguridad en Protección de Datos* se reunió el día 18 de julio de 2017 con el siguiente orden del día:

"Estimados y estimadas,

Les convoco a la reunión del Comité de Seguridad el próximo día 18/7/2017 a las 16h en la sala de los leones con el siguiente

Orden del día:

1. Aprobación del acta 1/2017 de fecha 26/5/2017.
2. Conclusiones auditoría 2016.
3. Plan de acción.
4. Informar de las reuniones del Comité Técnico.
5. Ruegos y preguntas.

Mataró, 24 de mayo de 2017

Juan Carlos Jerez
Presidente del Comité de Seguridad"

* Se adjunta el acta de la reunión en archivo 01_Reunions_Comite_seguretat.zip

Sin embargo, el Comité Técnico de Seguridad se ha reunido 15 veces entre 2018 y 2022.

* Se adjuntan las actas en el archivo 02_Reunions_Comite_tecnic_seguretat.zip

Alegación segunda

En el apartado "3. CONCLUSIONES" subapartado "2) Gobernanza de la ciberseguridad" donde se dice:

La política de seguridad de la información no está completa ni actualizada.

No se han formalizado ni aprobado todas las normas y los procedimientos de seguridad necesarios.

El Ayuntamiento de Mataró informa que la actual política de seguridad se publicó por decreto de Alcaldía 3985 el día 22 de mayo de 2019, de acuerdo con Real decreto 951/2015, de 23 de octubre, de modificación del RD 3/2010, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica y que esta política da cumplimiento a dicho RD.

El Ayuntamiento de Mataró informa que con posterioridad, el día 5 de mayo de 2022 se publicó el "Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad", que modifica dicho Esquema Nacional de Seguridad y que actualmente el Ayuntamiento de Mataró está realizando la revisión de la política de seguridad para incorporar los requerimientos de la nueva norma, tal y como queda patente por la contratación del servicio de asesoramiento, consultoría, asistencia técnica y jurídica en materia de protección de datos y de la implementación del Esquema Nacional de Seguridad del Ayuntamiento de Mataró.

https://contractaciopublica.cat/ca/detalle-publicacio/a8a06444-e755-41da-aed5-7bcf0f457580/300059942

En el marco de este contrato, el Ayuntamiento de Mataró con el soporte de la empresa adjudicataria ha iniciado los trabajos a fin de elaborar toda la documentación para dar cumplimiento a los requisitos formales del Real decreto 311/2022.

Hoy en día, la Política de Seguridad ha sido actualizada y se ha elaborado la Normativa de Seguridad, que se encuentran en fase de revisión interna a la espera de su aprobación formal y comunicación al conjunto de la organización.

Alegación tercera

En el apartado "5.1.2 Inventario y control de *software* autorizado y no autorizado (CBCS 2)", donde se dice:

> *Sin perjuicio de que se revisa el* software *con la misma herramienta que se utiliza para el inventario de* hardware*, el recurso se considera insuficiente ya que el Ayuntamiento no dispone de un listado de* software *autorizado ni lleva a cabo periódicamente un control del* software *no permitido.*

El Ayuntamiento de Mataró informa que dispone de un documento "3SPA-Programari_corporatiu_per_ordenadors_personals", donde se especifica "Configuración de software corporativo de los ordenadores personales del Ayuntamiento de Mataró"

> * Se adjunta documento donde se muestra el inventario de *software* autorizado.

Alegación cuarta

En el apartado "5.1.2 Inventario y control de *software* autorizado y no autorizado (CBCS 2)", donde dice:

> *También se ha comprobado que, aunque el Ayuntamiento no dispone de herramientas específicas para controlar e impedir la instalación de* software *no autorizado, los usuarios no son administradores locales y por lo tanto no tienen la capacidad de instalar* software.

El Ayuntamiento de Mataró considera que haber restringido la capacidad de instalar *software* es un mecanismo suficientemente robusto que evita la necesidad de instalar un *software* específico para evitar instalaciones de *software* no autorizado.

Esperamos recibir en breve su conformidad y le saludamos atentamente.

Mataró, en la fecha de la firma electrónica

8.2. TRATAMIENTO DE LAS ALEGACIONES

Las alegaciones formuladas han sido analizadas y valoradas por la Sindicatura de Cuentas.

El texto del proyecto de informe no se ha alterado porque se entiende que las alegaciones enviadas son explicaciones que confirman la situación descrita inicialmente o porque no se comparten los juicios que en ellas se exponen.

APROBACIÓN DEL INFORME

Certifico que en Barcelona, el 16 de julio 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 9/2024, relativo al Ayuntamiento de Mataró, 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