INFORME 16/2024

AYUNTAMIENTO DE SANTA COLOMA DE GRAMENET
CONTROLES BÁSICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

INFORME 16/2024

AYUNTAMIENTO DE SANTA COLOMA DE GRAMENET
CONTROLES BÁSICOS DE CIBERSEGURIDAD, EJERCICIO 2023

SINDICATURA DE COMPTES DE CATALUNYA

Edición: noviembre 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	Control básico 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 fiscalización de seguridad limitada relativo a los controles básicos de ciberseguridad del Ayuntamiento de Santa Coloma de Gramenet (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 del *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 modo 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 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 30 de mayo 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, 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, 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 realizado, y en el 4, Recomendaciones, 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 ciber-

3. De acuerdo con lo que prevé el artículo 46 de la Ley 18/2010, de 7 de junio, de la Sindicatura de Cuentas, y 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.

seguridad 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 Santa Coloma de Gramenet 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 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 básicos del Ayuntamiento de Santa Coloma de Gramenet son el Pleno, la Comisión de Gobierno, la alcaldesa, los tenientes de alcalde y la Comisión Especial de Cuentas.

En el ejercicio fiscalizado, el Ayuntamiento disponía de los siguientes órganos complementarios: la Comisión Informativa Permanente, las Comisiones Especiales, la Junta de Portavoces, los presidentes de los Grupos Municipales, los consejos y comisiones sectoriales de participación, el Consejo de Entidades Ciudadanas y los concejales de Distrito.

En lo referente a los entes dependientes, en el ejercicio 2023 el Ayuntamiento tenía constituido 1 organismo autónomo y 3 sociedades mercantiles. Estos entes eran los siguientes:

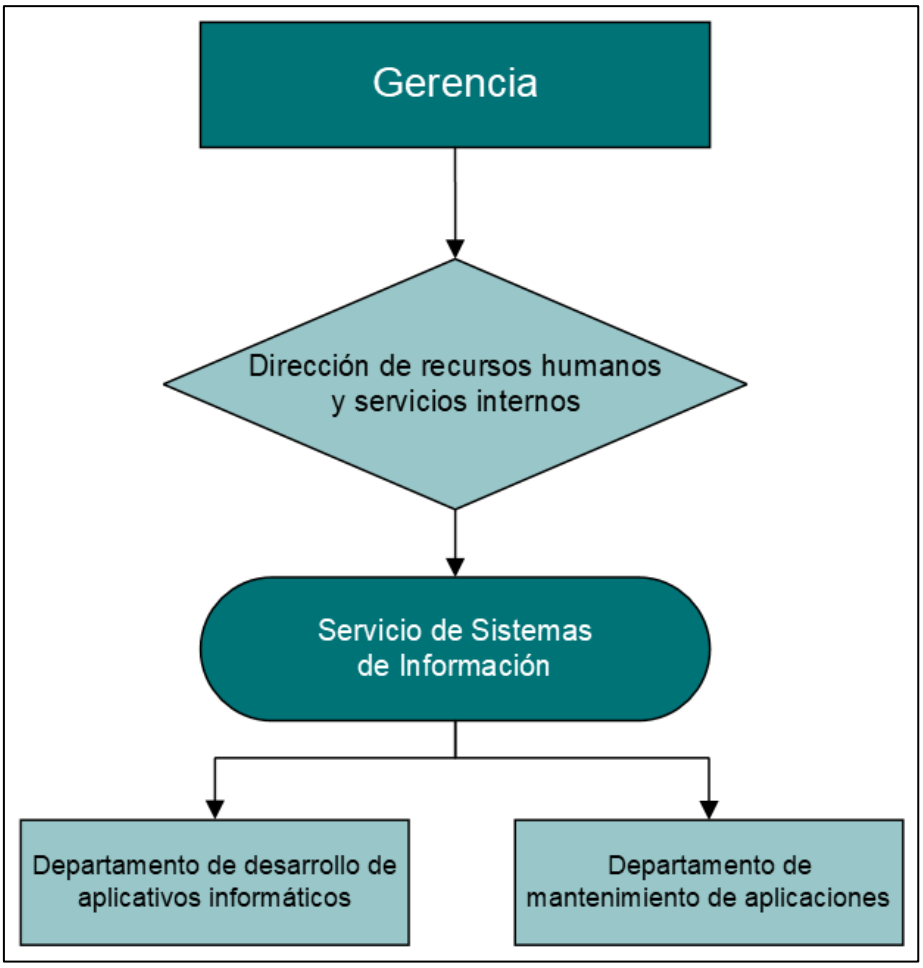
- Patronato de la Música de Santa Coloma de Gramenet
- GRAMEIMPULS, SA
- GRAMEPARK, SA
- BressolGramenet, SA

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

La unidad de Servicio de Sistemas de Información tiene la misión de ofrecer las herramientas informáticas y de comunicaciones necesarias para que los trabajadores del Ayuntam-

iento puedan llevar a cabo sus tareas de modo que se optimicen los recursos económicos y personales a su alcance. 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



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

Los principales servicios que presta la unidad son los siguientes:

- Soporte informático. Asistencia remota y presencial a los usuarios ante las incidencias relacionadas con el *software* y el *hardware* que el Ayuntamiento pone a su alcance para que lleven a cabo sus tareas.

- Desarrollo y mantenimiento de aplicaciones. Análisis, desarrollo e implantación de nuevas aplicaciones. Mantenimiento correctivo y evolutivo de las aplicaciones internas. Seguimiento e implantación de nuevas versiones, y dar cuenta de las incidencias al proveedor de aplicaciones externas.

- Gestión de usuarios. Gestión de alta y baja de cuentas de usuarios, sus perfiles y sus privilegios de acceso, tanto en la aplicación como en los recursos compartidos.

- Mantenimiento de la infraestructura de los sistemas de información y comunicación. Conjunto de trabajos de mantenimiento correctivo y preventivo de los elementos que forman la infraestructura de los sistemas de información y comunicaciones, como por ejemplo la instalación y actualización de nuevas versiones del *software*, micro *software* y ejecución de copias de seguridad, entre otros. Monitorización de sistemas automatizados y aplicaciones y actuaciones en caso de incidencia.

En el ejercicio 2023 el número de plazas asignadas a esta unidad era de 17, ocupadas con 4 funcionarios de carrera, 9 funcionarios interinos y 4 laborales.

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 en 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 calificado de la siguiente forma:

Cuadro 2. Valoración de cada subcontrol

Nivel	Descripción
Control efectivo	• Cubre al 100% el objetivo de control y: o El procedimiento está formalizado (documentado y aprobado) y actualizado. o 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: o Se sigue un procedimiento, aunque puede no estar formalizado o presentar aspectos de mejora (detalle, nivel de actualización, etc.). o 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: o Se sigue un procedimiento, aunque puede no estar formalizado. o El resultado de las pruebas de implementación y eficacia operativa es satisfactorio. • Cubre en líneas generales el objetivo de control, pero: o No se sigue un procedimiento claro. o 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.

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 ese 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. Hay 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 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.

Nivel	Índice	Descripción
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 con 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 a 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, hay que tener 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 ser considerados 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[4] 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 las tareas 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, 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 hace de la gobernanza existente basándose en la implicación

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

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 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 Santa Coloma de Gramenet 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 fiscalización realizada y los indicadores reflejan la situación a 30 de mayo de 2024. El grado de control en la gestión de los CBCS llega a un índice de madurez general del 57,25%, 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 hay 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 y índice de cumplimiento

Control		Índice de madurez (%)	Nivel de madurez*	Índice de cumplimiento (%)
CBCS 1	Inventario y control de dispositivos físicos	60,00	N2	75,00
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	45,00	N1	56,25
CBCS 4	Uso controlado de privilegios administrativos	40,00	N1	50,00
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	30,00	N1	37,50
CBCS 6	Registro de la actividad de los usuarios	70,00	N2	87,50
CBCS 7	Copias de seguridad de datos y sistemas	78,00	N2	97,50
CBCS 8	Cumplimiento de legalidad	60,00	N2	75,00
Índice general		**57,25**	**N2**	**71,56**

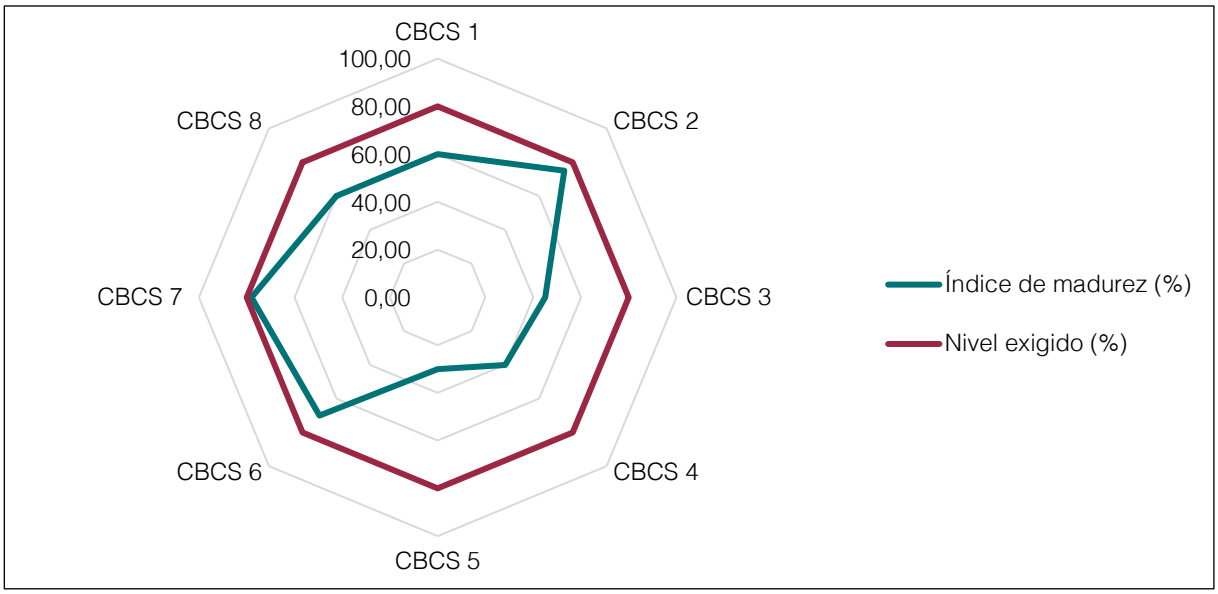
Fuente: Elaboración propia.

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

El índice de cumplimiento general de los CBCS es del 71,56%, que es el resultado de comparar el índice de madurez alcanzado con el nivel requerido del sistema de acuerdo con el ENS, que, 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 requerido por el ENS:

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 7, Copias de seguridad de datos y sistemas, que alcanza un índice de madurez del 78% y de cumplimiento del 97,50%. 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 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, 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 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 un compromiso con la ciberseguridad por parte de los órganos de gobierno del Ayuntamiento y de los gestores y responsables de las áreas revisadas, no obstante, se han identificado carencias relevantes que dificultan la implementación de un sistema efectivo que garantice la ciberresiliencia. Las carencias más significativas son las siguientes (véase el apartado 5.2):

- Los órganos de gobierno no han aprobado la política de seguridad de la información ni tampoco las normas y procedimientos de seguridad que tenían redactadas.

- No se ha creado el Comité de Seguridad de la información ni el Comité de Seguridad Corporativa tal como establece la política de seguridad definida.

- No existen determinados roles clave en la organización, como el responsable de seguridad. De hecho, no han sido nombrados ninguno de los 4 responsables en materia de seguridad que determina el ENS.

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 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 (véase el apartado 5.1.8).

4) Aplicación del Real decreto 311/2022

A la finalización de la redacción de este informe (julio de 2024) el Ayuntamiento no había acreditado la adecuación al ENS y no ha trabajado de forma proactiva en la aprobación de la normativa ni de los procedimientos que le faltaban para dar cumplimiento al Real decreto 311/2022. Tampoco ha designado los 4 responsables que determina el ENS, los cuales permitirían la coordinación efectiva de las áreas y la adopción de medidas de mejora continua. En lo referente a los 2 comités de seguridad, el Ayuntamiento no ha avanzado en su creación.

En cuanto 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 que se deben adoptar para el cumplimiento de la legalidad.

1. Los órganos de gobierno deberían promover la aprobación 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 aprobar los manuales y protocolos existentes y formalizar otros para los procedimientos que todavía no tienen pero que de forma informal y periódica el personal del Ayuntamiento está realizando.

3. 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.

4. 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.

5. Deberían hacerse revisiones periódicas de los registros de actividad e indicar en la documentación del sistema los acontecimientos de seguridad que serán auditados y el tiempo que los responsables los deben retener antes de la eliminación.

6. Para hacer un uso racional de los privilegios de administrador, sería necesario que los usuarios con este privilegio dispusieran adicionalmente de un usuario nominativo sin privilegios para llevar a cabo las tareas habituales.

7. Habría que dedicar esfuerzos a corregir, en un tiempo razonable, las no conformidades e incidencias detectadas en la auditoría de protección de datos.

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 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 ante 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 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 ha diseñado y redactado un procedimiento para la recepción, inventario, configuración y asignación de equipos personales a los usuarios, pero no ha sido aprobado por los órganos responsables. Asimismo, también ha definido el procedimiento de asignación de equipos y el modelo que hay que formalizar para controlar la entrega de activos.

Se ha comprobado que el Ayuntamiento ha desarrollado un *software* propio que le permite inventariar y controlar los activos físicos, pero la herramienta no permite la actualización automática ni continua del inventario.

No se ha obtenido evidencia de que los cambios de ubicación de un activo se hayan recogido en el inventario y el Ayuntamiento no efectúa revisiones periódicas para mantener actualizado este inventario.

El control de activos físicos no autorizados que lleva a cabo el Ayuntamiento ha puesto de manifiesto una serie de debilidades 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 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.

5.1.2. 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 del control del *software* y se ha comprobado que dispone de un procedimiento documentado para solicitar la instalación de *software*, pero no ha sido aprobado.

Aunque no se permite que los usuarios puedan instalar *software* sin pedir autorización, y que el Ayuntamiento dispone de una lista de aplicaciones restringidas, el control es insuficiente, ya que no se dispone de un inventario de *software*, el listado de aplicaciones restringidas no está actualizado y no se lleva a cabo periódicamente un control del *software* no autorizado.

En cuanto al *software* con soporte del fabricante, se ha observado que no existe un plan de mantenimiento de este *software* de acuerdo con las especificaciones de los fabricantes. El departamento de informática controla la fecha de finalización de soporte de los fabricantes y define planes de migración para este *software*, pero durante la fiscalización se ha puesto de manifiesto que existen servidores con sistemas operativos que están fuera del soporte del fabricante.

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

La unidad de Servicio de Sistemas de Información es la encargada de identificar vulnerabilidades, y para determinadas tareas de soporte y actualización de los sistemas ha contratado los servicios en una empresa externa.

El Ayuntamiento dispone de sistemas de prevención de intrusiones, pero no realiza escaneos de vulnerabilidad ni test de intrusión de forma periódica. Tampoco realiza auditorías de código fuente de los desarrollos internos de *software*.

Para identificar vulnerabilidades no dispone de ninguna herramienta concreta, pero utiliza diferentes medios, como por ejemplo la suscripción a comunicaciones de fabricantes o de organismos de referencia: el Centro Criptográfico Nacional, entre otros.

En lo referente a los procedimientos, el Ayuntamiento tiene 2 de documentados. Por un lado el de notificación y gestión de incidencias y por el otro la actualización e instalación de parches en los servidores.

Se ha puesto de manifiesto que en algunas ocasiones las acciones efectuadas no se correspondían con las previsiones definidas en los manuales. Sin embargo, a pesar de las carencias en la definición de algunos procedimientos se ha podido comprobar que el Ayuntamiento dispone de herramientas para gestionar e instalar parches y actualizaciones de seguridad.

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% de 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.

5.1.4. 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

La gestión de la asignación de privilegios de administración en los sistemas revisados varía según el sistema. En general, el Ayuntamiento ha hecho un uso restringido de los usuarios con permisos de administración y dispone de una herramienta específica para registrar estos usuarios por sistemas.

Se ha verificado que no existe un procedimiento formal para el alta y la baja en los sistemas ni consta aprobado el procedimiento que regula el inventario de usuarios administradores. En cuanto a la asignación de identificadores únicos en función del rol, no existe homogeneidad. Por un lado, se ha detectado el uso de cuentas no nominativas compartidas y por otro, usuarios nominativos con privilegios de administrador.

El Ayuntamiento no dispone de una política que defina específicamente los mecanismos de autenticación de las cuentas de administración de los sistemas antes de ponerlos en explotación o una vez puestos en producción. Además, no hay ningún procedimiento de fortificación o refuerzo de la seguridad de los sistemas antes de ponerlos en funcionamiento y las contraseñas no cumplen todas las reglas básicas de seguridad.

Los registros de actividad del directorio activo son almacenados y revisados, aunque se ha constatado que en ciertos programas no se monitorizan los registros de actividad, lo que ha sido comunicado al Ayuntamiento por los canales establecidos.

De las evidencias obtenidas en la revisión de este control, relativo al uso controlado de privilegios administrativos, la valoración general alcanza un 40% 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 asegura que la entidad haya reforzado las configuraciones predeterminadas de los fabricantes de *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, que están orientadas a facilitar su 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 realiza algunas acciones para fortificar o reforzar la seguridad de los sistemas de los activos antes de su puesta en marcha, pero no dispone de un procedimiento documentado de guías de fortificación ni utiliza plantilles de configuración de seguridad en todos los sistemas. Tampoco realiza pruebas de seguridad de los sistemas antes de pasar a producción para comprobar que cumplen los criterios en materia de seguridad.

Aunque los usuarios no pueden modificar la seguridad de los sistemas, se han encontrado debilidades en los controles que realiza el Ayuntamiento en relación con la detección de cambios no autorizados o erróneos de la configuración para poder corregirlos en un oportuno período de tiempo.

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 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.

5.1.6. 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 *des de dónde*, *quién*, *qué* y *cuándo*, y si tienen definidas acciones de alerta. Un ataque al sistema podría pasar desapercibido de forma indefinida 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

De la revisión de las actividades efectuadas por el Ayuntamiento para el registro de la actividad de los usuarios se ha constatado que no existe un procedimiento formalmente aprobado y que el Ayuntamiento no dispone de un plan que garantice la capacidad de almacenamiento teniendo en cuenta el volumen y la política de conservación. Se registra la actividad del directorio activo, del sistema de ficheros, del antivirus y de algunas aplicaciones.

En cuanto al almacenamiento, se ha constatado que los acontecimientos del directorio activo, antivirus y cortafuegos se envían a una herramienta externa de administración de eventos e información, que los correlaciona. Esta herramienta es gestionada por un centro de operaciones de seguridad contratado a una empresa externa.

A pesar de los registros de actividades que realiza el Ayuntamiento, no hay un servidor que centralice los registros generados por los diferentes sistemas.

Un programa específico se encarga de la auditoría de la actividad de los usuarios, pero monitoriza únicamente el directorio activo y el sistema de ficheros, y almacena los registros en una base de datos del *software*. La herramienta de administración de eventos e información de seguridad realiza revisiones automatizadas de los registros, pero estas revisiones no son generales en todos los sistemas.

De las evidencias obtenidas en la revisión de este control, relativo al registro de la actividad de los usuarios, 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.

5.1.7. 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, pero no ha sido aprobado formalmente. Para realizar las copias, el Ayuntamiento utiliza una aplicación específica y se hacen, tanto en disco como en cinta.

Se ha comprobado que el contenido de las copias es el definido en el procedimiento escrito y abarca el directorio activo, las bases de datos SQL, los servidores críticos y el repositorio de ficheros.

En cuanto a las pruebas de restauración, aunque se realizan a partir de las copias de seguridad, no existe un calendario definido para realizarlas y no queda documentado cuando se han efectuado. Se ha comprobado que solo se documenta, mediante una hoja de cálculo, cuando se realizan recuperaciones a solicitud de algún usuario.

Estas copias de seguridad tienen la misma seguridad que los datos originales, tanto en lo referente al acceso como al almacenamiento y el transporte. Solo los administradores del sistema pueden acceder al sistema de copias de seguridad y al sistema de ficheros de las copias. Además, se realizan copias de seguridad que no son accesibles a través de la red.

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 78% 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

Desde 2014, el Ayuntamiento dispone de un documento con la política de seguridad, sin embargo, este documento no está aprobado ni actualizado.

Por otro lado, el Ayuntamiento ha hecho una auditoría de cumplimiento del ENS para los sistemas de categoría media y alta, pero no ha llevado a cabo el proceso de adecuación ni ha habido la certificación del ENS. A pesar de ello, ha formalizado la declaración de aplicabilidad del ENS, aunque esta declaración no está actualizada.

El Ayuntamiento no ha formalizado ni ha 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 el año 2019, el Ayuntamiento adscribió, de modo provisional, a un funcionario como delegado de protección de datos. A la fecha de finalización del trabajo (30 de mayo de 2024) no se había provisto el puesto de trabajo por el procedimiento reglamentariamente establecido. Este nombramiento provisional se notificó a la Autoridad Catalana de Protección de Datos.

No se dispone de un análisis de riesgos de los tratamientos de datos, y el registro de actividades de tratamiento no está actualizado ni debidamente aprobado. Por otro lado, en el año 2023 se hizo una auditoría en materia de protección de datos personales con un resultado de 4 no conformidades.

c) Cumplimiento de legalidad del registro de facturas

El Ayuntamiento dispone de la auditoría de sistemas del registro contable de facturas del ejercicio 2022, de acuerdo con la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas del sector público, que los órganos de control interno deben elaborar anualmente.

Del contenido de esta auditoría se ha evidenciado que no se ha revisado la gestión de la seguridad en aspectos relacionados con la confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad de los datos y los servicios de gestión de acuerdo con lo establecido por la Guía para las auditorías de los registros contables de facturas elaborada por la Intervención General de la Administración del Estado.

d) Índice de madurez

De las evidencias obtenidas en la revisión de este control, relativo al cumplimiento de legalidad, 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.

5.2. GOBERNANZA DE LA CIBERSEGURIDAD

La gobernanza[5] 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, es el presidente y la Junta de Gobierno. Ellos son los responsables de garantizar que el funcionamiento de la organización está 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 del ente.

Durante el trabajo de fiscalización se ha evidenciado una implicación y un compromiso con la ciberseguridad insuficientes por parte de los órganos de gobierno, y que, como consecuencia de ello, el Ayuntamiento no tiene establecida una adecuada gobernanza de la ciberseguridad. Las principales debilidades observadas son las siguientes:

- El Ayuntamiento dispone de la política de seguridad de la información redactada y de las normas y los procedimientos de seguridad, pero ninguno de ellos ha sido aprobado por los órganos de gobierno.

- No se ha designado el responsable de la información, el servicio, la seguridad de la información y el sistema que exige el ENS.

5. Definición de acuerdo con el apartado 1 de la GPF-OCEX 5314, Gobernanza de la ciberseguridad y su auditoría.

- No se ha creado el Comité de Seguridad de la Información ni el Comité de Seguridad Corporativa tal como establece la política de seguridad definida.

- El Ayuntamiento no dispone de un Plan Estratégico TIC o documento equivalente, ni tampoco ha hecho un análisis sobre los riesgos que afectan a los sistemas de información.

- Existen determinados incumplimientos normativos, detallados en el apartado 5.1.8.

No obstante, se han identificado algunos aspectos positivos:

- Se ha verificado el incremento de las inversiones previstas para el ejercicio 2024, que permitirán desarrollar proyectos e implantar sistemas que tendrán un potencial impacto positivo en el nivel de seguridad de la organización.

- El Ayuntamiento ha promovido entre el personal la concienciación de los riesgos existentes en ciberseguridad, mediante cursos de formación.

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 (julio de 2024) 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, porque los ha considerado los más relevantes de los controles generales que faltaba revisar. En el siguiente cuadro se incluyen todos los controles de la categoría seleccionada:

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 (a)	Índice de cumplimiento
D.2: Mecanismo de identificación y autenticación	58,00	N2	72,50
D.3: Gestión de derechos de acceso	62,00	N2	77,50
D.4: Gestión de usuarios	59,00	N2	73,75
D.5: Protección de redes y comunicaciones	59,00	N2	73,75
Índice general (b)	**59,50**	N2	**74,38**

Fuente: Elaboración propia.

Notas:

(a) Hay 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 40% y del 50%, respectivamente, que no se ha tenido en cuenta en la valoración de estos controles adicionales.

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

En lo referente al resultado de la revisión de los controles y subcontroles seleccionados, destaca la gestión de derechos de acceso, con un índice de cumplimiento del 77,50%, aunque los 4 controles tienen índices de cumplimiento muy similares.

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, a la fecha de redacción de este informe (julio 2024) no se había acreditado la adecuación al ENS. Cabe destacar que de modo proactivo no se está aprobando la política de seguridad, no se están aprobando los procedimientos, no se están creando los comités ni se están nombrando los responsables que determina el ENS, que permitirían la coordinación efectiva de las áreas y la adopción de medidas de mejora continua.

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 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, si se difundiera, podría llegar a afectar seriamente a 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 su uso y 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 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 correcto control.
			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 tareas 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 efectua 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 Santa Coloma de Gramenet el 17 de septiembre de 2024 para cumplir el trámite de alegaciones.

Una vez transcurrido el plazo establecido no se ha recibido ningún escrito de alegaciones del Ayuntamiento de Santa Coloma de Gramenet.

APROBACIÓN DEL INFORME

Certifico que en Barcelona, el 22 de octubre 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 16/2024, relativo al Ayuntamiento de Santa Coloma de Gramenet: 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