



SINDICATURA
DE COMPTES



**Informe de auditoría de los controles
básicos de ciberseguridad del
Ayuntamiento de Sant Vicent del
Raspeig
Ejercicio 2020**



INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE SANT VICENT DEL RASPEIG

Ejercicio 2020



RESUMEN

La auditoría realizada por la Sindicatura de Comptes sobre los controles básicos de ciberseguridad del Ayuntamiento de Sant Vicent del Raspeig en el ejercicio 2020 ha concluido que, con carácter general, el grado de cumplimiento existente en la gestión de esta materia es de un 52,8% respecto al nivel establecido como objetivo. Esto implica que, aunque existe cierto nivel de efectividad en los controles analizados, es insuficiente y existen claras posibilidades de mejora.

Por otra parte, la valoración de la auditoría sobre el cumplimiento de los aspectos de legalidad representa un índice del 20,6% respecto al nivel establecido como objetivo, una cifra que el órgano fiscalizador considera excesivamente baja e insatisfactoria ya que existen incumplimientos generalizados de la normativa.

Este trabajo se enmarca dentro de las auditorías realizadas a los controles básicos de ciberseguridad de los municipios con población superior a 50.000 habitantes de la Comunitat Valenciana, incluidas en los programas anuales de actuación de 2019 y 2020 de la Sindicatura. Con sus valoraciones, la Sindicatura verifica si el marco de ciberseguridad aplicado sobre los sistemas de información garantiza un nivel de control adecuado, incluyendo la protección de la información que gestionan los ayuntamientos y la continuidad de los servicios públicos ofrecidos.

En este sentido, la crisis sanitaria y socioeconómica mundial causada por la pandemia de COVID-19 que marca nuestra realidad en el momento de publicar este informe, ha puesto de manifiesto la total dependencia que tiene la gestión pública de los sistemas de información y las comunicaciones (SIC). Esto hace que administraciones públicas y ayuntamientos sean más vulnerables frente a los ciberataques y que, por tanto, mantener un sólido sistema de protección frente a ellos y una adecuada ciberhigiene sea más necesario que nunca.

Con el propósito de mejorar la gestión de la ciberseguridad en el ente auditado, además del informe con los resultados obtenidos en el trabajo, la Sindicatura ha trasladado al Ayuntamiento de Sant Vicent del Raspeig el análisis detallado de las deficiencias identificadas y las recomendaciones orientadas a subsanarlas. La mejora de los controles de ciberseguridad requerirá actuaciones e inversiones, tanto en medios materiales como personales, que tienen que ser adecuadamente planificadas. En este sentido, la Sindicatura de Comptes prevé realizar el seguimiento de las recomendaciones como parte del Programa Anual de Actuación de 2021.



La Sindicatura considera que es necesario que los máximos órganos responsables del Ayuntamiento (Pleno, alcalde y la concejalía responsable de las TIC) tomen conciencia de la necesidad de conseguir los niveles exigidos por la normativa para la protección de los sistemas de información ante la multiplicidad de amenazas existentes, a fin de garantizar la consecución de los objetivos de la entidad, la prestación adecuada de servicios a los ciudadanos y la protección de la información y del resto de los activos de los sistemas de información.

NOTA

Este resumen pretende ayudar a la comprensión de los resultados de nuestro informe y facilitar la labor a los lectores y a los medios de comunicación. Recomendamos su lectura para conocer el verdadero alcance del trabajo realizado.



ÍNDICE	Página
1. Introducción	3
2. Responsabilidades de los órganos municipales en relación con los controles de ciberseguridad	3
3. Responsabilidad de la Sindicatura de Comptes	4
4. Conclusiones	6
5. Situación de los controles	8
6. Recomendaciones y medidas para el cumplimiento de la legalidad	14
APÉNDICE. Metodología aplicada	19
TRÁMITE DE ALEGACIONES	29
APROBACIÓN DEL INFORME	30



1. INTRODUCCIÓN

En virtud de lo dispuesto en el artículo 8.3 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y según lo previsto en el Programa Anual de Actuación de 2020 (PAA2020) se ha efectuado una auditoría sobre la situación en 2020 de los controles básicos de ciberseguridad (CBCS) de los ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes, entre los que se encuentra el Ayuntamiento de Sant Vicent del Raspeig.

La realidad de nuestro entorno cercano y del resto de la sociedad española y mundial en el momento de elaborar este informe es la de una crisis sanitaria y socioeconómica sin precedentes provocada por la epidemia del COVID-19. Entre otras muchas cuestiones, esta crisis ha puesto de manifiesto que gran parte de las Administraciones públicas y ayuntamientos han sido capaces de continuar en marcha confiando en gran medida en el buen funcionamiento y la eficacia de los sistemas de información y las comunicaciones (SIC).

Al mismo tiempo, esta circunstancia ha mostrado con absoluta claridad la total dependencia de los SIC que existe actualmente en la gestión pública, lo que hace que nuestras administraciones sean más vulnerables frente a los ciberataques y que, por tanto, mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos sea más necesario que nunca.

2. RESPONSABILIDADES DE LOS ÓRGANOS MUNICIPALES EN RELACIÓN CON LOS CONTROLES DE CIBERSEGURIDAD

Los órganos municipales (el Pleno, el alcalde, la Junta de Gobierno y la Secretaría General) son los responsables de que existan unos adecuados controles sobre los SIC. De acuerdo con sus competencias deben garantizar que el funcionamiento de la entidad resulta conforme con las normas aplicables y que los controles internos proporcionan una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplen las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad (ENS)¹:

- Confidencialidad, es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- Integridad, es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea

¹ Véase el anexo I del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.



de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.

- Disponibilidad, se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.
- Autenticidad, es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad, es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

La responsabilidad de la Sindicatura de Comptes es concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación sobre su diseño y eficacia operativa, sobre el cumplimiento de la normativa básica relativa a la seguridad de la información y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control. Para ello, hemos llevado a cabo el trabajo de conformidad con los *Principios fundamentales de fiscalización de las instituciones públicas de control externo* y con las normas técnicas de fiscalización aprobadas por el Consell de la Sindicatura recogidas en el *Manual de fiscalización* de la Sindicatura de Comptes. Dichos principios exigen que cumplamos los requerimientos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una evaluación de los CBCS.

Ámbito objetivo

La auditoría se ha centrado en el análisis de la situación de los ocho CBCS:

- 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 remediación 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 normativo



Dada la naturaleza del objeto material a revisar –la gran amplitud, complejidad y diversidad de los sistemas de información de un ente local de tamaño grande-, ha sido necesario delimitar y concretar qué sistemas se iban a analizar. En este sentido, hemos analizado las aplicaciones que soportan dos de los procesos de gestión más relevantes a efectos de la Sindicatura, como son la gestión contable y presupuestaria y la gestión tributaria y recaudatoria. La revisión ha incluido los controles relacionados con:

- las aplicaciones informáticas que los soportan
- las bases de datos subyacentes
- los sistemas operativos instalados en cada uno de los sistemas que integran la aplicación de gestión (ej. servidor web, servidor de aplicación, servidor de base de datos)

Además, por su importancia para el buen funcionamiento de los sistemas de información y la ciberseguridad, hemos analizado también una selección de los siguientes tipos de elementos:

- controlador de dominio
- *software* de virtualización
- equipos de usuario
- elementos de la red de comunicaciones (*router*, *switches*, punto de acceso a red *wifi*, etc.)
- elementos de seguridad (*firewall*, *IPS*, *proxy* de correo, *proxy* de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Metodología

Esta auditoría de los controles básicos de ciberseguridad ha sido realizada por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI), siguiendo la metodología establecida en la guía GPF-OCEX 5313 *Revisión de los controles básicos de ciberseguridad* (integrada en el *Manual de fiscalización* de la Sindicatura de Comptes).

Hemos evaluado la situación de los CBCS utilizando el modelo de nivel de madurez de los procesos, ya que, además de ser un sistema ampliamente aceptado, permite establecer objetivos y realizar comparaciones entre entidades distintas y ver la evolución a lo largo del tiempo. La metodología utilizada está plenamente alineada con lo establecido por el ENS que es de aplicación obligatoria en todos los entes públicos.



En el apéndice se proporciona un mayor detalle de la metodología utilizada.

Confidencialidad

Dado que la información utilizada en la auditoría y los resultados detallados de la misma tienen un carácter sensible y pueden afectar a la seguridad de los sistemas de información, los resultados detallados de cada uno de los controles solo se comunican con carácter confidencial a los responsables del Ayuntamiento para que puedan adoptar las medidas correctoras que consideren precisas. En el presente informe los resultados se muestran de forma sintética.

4. CONCLUSIONES

Como resultado del trabajo realizado cabe concluir que, con carácter general, el grado de control existente en la gestión de los CBCS señalados en el apartado 3, alcanza un índice de madurez del 42,3%, que se corresponde con un nivel de madurez *N1-inicial/ad hoc*; es decir, los procesos de control existen, pero su gestión no está correctamente organizada.

Los sistemas de información revisados están clasificados como de categoría de seguridad *MEDIA*. Así, acorde con esta categoría, el nivel de madurez requerido por el ENS y que también lo aplicamos para los CBCS en esta auditoría es *N3-Proceso definido* y un índice de madurez del 80%.

En consecuencia, el índice de cumplimiento de los CBCS es del 52,8%, que resulta de comparar el indicador de madurez observado con el nivel requerido u objetivo que debe tener el sistema según el ENS.

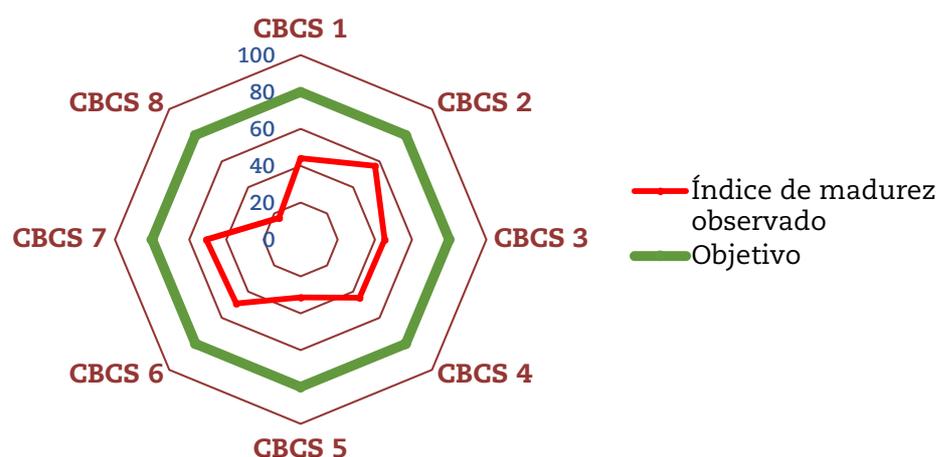
En el cuadro siguiente se muestran de forma detallada los resultados de la evaluación realizada para cada uno de los CBCS.



Cuadro 1. Índice y nivel de madurez de los CBCS del Ayuntamiento

Control	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	44,1%	N1	55,1%
CBCS 2 Inventario y control de <i>software</i> autorizado y no autorizado	56,5%	N2	70,6%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	45,3%	N1	56,6%
CBCS 4 Uso controlado de privilegios administrativos	44,7%	N1	55,9%
CBCS 5 Configuraciones seguras del <i>software</i> y <i>hardware</i>	31,4%	N1	39,2%
CBCS 6 Registro de la actividad de los usuarios	49,0%	N1	61,3%
CBCS 7 Copias de seguridad de datos y sistemas	50,7%	N2	63,3%
CBCS 8 Cumplimiento normativo	16,5%	N1	20,6%
Índice/Nivel global del Ayuntamiento	42,3%	N1	52,8%
Índice/Nivel requerido u objetivo	80,0%	N3	100,0%

Gráfico 1. Índice de madurez de los CBCS



A la vista de los resultados obtenidos en la revisión, se concluye que, aunque existe cierto nivel de efectividad en los controles analizados, existen claras posibilidades de mejora. Por tanto, es necesario que los máximos órganos responsables del Ayuntamiento (Pleno, alcalde y la concejalía responsable de las TIC) tomen conciencia de la necesidad de alcanzar los niveles exigidos por la normativa para la protección de los



sistemas de información frente a la multiplicidad de amenazas existentes, con objeto de garantizar la consecución de los objetivos de la entidad, la adecuada prestación de servicios a los ciudadanos y la protección de la información y del resto de los activos de los sistemas de información. Esta cultura de ciberseguridad se debe trasladar a todos los niveles y departamentos del Ayuntamiento.

La mejora de los controles de ciberseguridad requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.

Además, la revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel de cumplimiento excesivamente bajo e insatisfactorio, ya que existen incumplimientos generalizados de esa normativa. 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 subsanar la situación.

5. SITUACIÓN DE LOS CONTROLES

A continuación, se detallan los principales aspectos surgidos en la revisión de cada uno de los CBCS del Ayuntamiento.

1. Sobre el inventario y control de dispositivos físicos (CBCS 1)

El proceso de inventariado se encuentra respaldado por el uso de una herramienta específica, que gestiona el inventario de la mayor parte de los activos de la entidad, bien mediante agente de red o por detección automática. Se ha evidenciado que el inventario existente se encuentra actualizado para este tipo de elementos. No obstante, dicho proceso no se encuentra establecido en un procedimiento formalmente aprobado.

Para los elementos que por su naturaleza no se encuentran inventariados mediante la herramienta automática, se dispone de herramientas propietarias o de inventarios de gestión manuales, que se mantienen actualizados.

Por otra parte, no se han implantado medidas efectivas que impidan la conexión de dispositivos físicos no autorizados a la red corporativa, lo que representa un riesgo alto.

Existe un nivel de control insuficiente sobre el inventario de dispositivos físicos, y la valoración global del control alcanza un índice de madurez del 44,1%, que se corresponde con un nivel de madurez N1-inicial/ad hoc; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 1 del 55,1%.



2. Sobre el inventario y control de software autorizado (CBCS 2)

En cuanto al control del *software* instalado y autorizado en los equipos, hemos verificado que, aunque existe un proceso definido, no ha sido formalmente aprobado.

El inventario de *software* se mantiene correctamente actualizado de manera automatizada, mediante el uso de la herramienta que también gestiona el inventario de activos físicos y que mantiene relacionados ambos inventarios.

Por otra parte, se ha evidenciado la existencia de un determinado número de equipos con *software* fuera del periodo de soporte del fabricante, hecho que supone un grave riesgo para el sistema de información. La existencia de dichos sistemas obsoletos responde a necesidades operativas, dado que existen determinadas aplicaciones de gestión de servicios municipales que únicamente disponen de compatibilidad con sistemas operativos obsoletos.

Adicionalmente, la entidad cuenta con medidas orientadas a impedir el uso de *software* no autorizado, pero existen determinadas carencias que limitan la efectividad de dichas medidas.

Existe cierto nivel de control sobre el inventario y el *software* autorizado, pero existen posibilidades de mejora, y su valoración global alcanza un índice de madurez del 56,5%, que se corresponde con un nivel de madurez N2, *repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 2 del 70,6%.

3. Sobre el proceso continuo de identificación y remediación de vulnerabilidades (CBCS 3)

Hemos analizado la gestión de vulnerabilidades realizada por el Ayuntamiento y hemos observado que dichas acciones forman parte de un proceso parcialmente definido que no se encuentra formalmente establecido en un procedimiento aprobado.

La identificación y remediación de vulnerabilidades se realiza, bien de manera manual mediante la búsqueda y resolución para determinados elementos, o bien por parte de terceros mediante contratos de mantenimiento de determinados sistemas. No obstante, no se utilizan herramientas específicas para la identificación de vulnerabilidades ni servicios externos para la realización de pruebas de penetración y *hacking* ético.



Las vulnerabilidades son priorizadas y resueltas mediante un proceso informal que no se encuentra contemplado en el procedimiento existente.

Se ha evidenciado durante el trabajo de auditoría un adecuado nivel de parcheo de los sistemas incluidos en el alcance de la revisión, particularmente para los sistemas basados en el sistema operativo Windows, que son gestionados mediante una herramienta para la centralización de actualizaciones.

Consideramos que existe un nivel de control insuficiente, por lo que se deberán dedicar esfuerzos y recursos para mejorarlo. La valoración global del control alcanza un índice de madurez del 45,3%, que se corresponde con un nivel de madurez N1, *inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 3 del 56,6%.

4. Sobre el uso controlado de privilegios administrativos (CBCS 4)

Hemos analizado la gestión realizada de las cuentas de administración y hemos verificado que no existe un control efectivo, ya que, si bien existen determinadas medidas adecuadas para controlarlas, estas no se encuentran implantadas de manera homogénea en todos los sistemas y no han sido establecidas en un procedimiento formalmente aprobado.

Se ha detectado el uso de cuentas de administración no nominativas en todos los sistemas incluidos en el alcance de la fiscalización, lo que impide la trazabilidad de las acciones.

No se aplica una política de autenticación homogénea en todos los sistemas o la política aplicada no es robusta en todos los casos, dado que únicamente se han establecido requisitos de autenticación en los sistemas Windows y en aquellos que han implementado SSO (*single sign-on*) con el directorio activo. Adicionalmente, el procedimiento de gestión de contraseñas no ha sido formalmente aprobado.

Sí que se dispone de identificadores diferenciados para un mismo usuario, dependiendo del tipo de tarea a desempeñar en el sistema, con objeto de limitar el uso de identificadores con privilegios administrativos en las tareas que no lo requieren.

Existe, por tanto, un nivel de control insuficiente en el uso de privilegios administrativos, por lo que se deberán dedicar esfuerzos y recursos para su mejora. La valoración global del control existente sobre el uso de privilegios administrativos alcanza un índice de madurez del 44,7%, que se corresponde con un nivel de madurez N1,



inicial/*ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 4 del 55,9%.

5. Sobre las configuraciones seguras del software y hardware (CBCS 5)

Hemos analizado las acciones realizadas para el control de la configuración segura en aplicaciones y dispositivos y hemos verificado que no existe un procedimiento para ello.

Se aplican configuraciones de seguridad en determinados sistemas, pero dichas acciones no son suficientes para asegurar la efectividad del control. Se dispone de plantillas para la configuración de determinados dispositivos, pero dichas plantillas no tienen carácter de bastionado ni la configuración segura de estos dispositivos se encuentra formalmente establecida.

Esto significa que existe un deficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deberán dedicar esfuerzos y recursos para su mejora. La valoración global del control alcanza un índice de madurez del 31,4%, que se corresponde con un nivel de madurez N1, *inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 5 del 39,2%.

6. Sobre el registro de la actividad de los usuarios (CBCS 6)

Hemos analizado las acciones del Ayuntamiento para el registro de la actividad de los usuarios en los distintos sistemas y hemos verificado que, aunque se han aplicado ciertas medidas relacionadas con este control, estas no se han establecido en un procedimiento formalmente aprobado.

Hemos verificado que el registro de actividad se encuentra activado en la mayoría de los sistemas, si bien se mantiene la configuración por defecto que define el fabricante.

El Ayuntamiento dispone de dos sistemas para la gestión centralizada de registros de actividad de determinados activos, lo que supone una mejora de la configuración básica por defecto de los *logs* de auditoría. No obstante, estas herramientas no integran todos los sistemas relevantes desde el punto de vista de la ciberseguridad y la revisión de dichos registros de actividad se realiza de forma informal, no procedimentada.

Por tanto, existe un deficiente nivel de control y su valoración alcanza un índice de madurez del 49,0%, que se corresponde con un nivel de madurez N1, *inicial/ad hoc*; es decir, los controles se realizan,



pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 6 del 61,3%.

7. Sobre la copia de seguridad de datos y sistemas (CBCS 7)

El Ayuntamiento realiza diversas acciones para las copias de seguridad de los datos y sistemas. El proceso se encuentra definido e implantado y ha sido recogido en un procedimiento que no ha sido formalmente aprobado y no refleja con exactitud el proceso completo de copia.

Los procesos establecidos para la realización de copias, así como el conjunto de soluciones tecnológicas implantadas, son adecuados y eficaces. Asimismo, las medidas implantadas para la protección de las copias pueden considerarse efectivas.

Sin embargo, no se realizan pruebas de recuperación planificadas de forma sistemática y el resultado de los trabajos de copia es revisado mediante un proceso manual que no se encuentra completamente definido y gestionado.

Esto significa que existe cierto nivel de control sobre las copias de seguridad de datos y sistemas, pero existen posibilidades de mejora. La valoración global del control alcanza un índice de madurez del 50,7%, que se corresponde con un nivel de madurez N2, *repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 7 del 63,3%.

8. Sobre el cumplimiento de la legalidad (CBCS 8)

El Ayuntamiento ha incurrido en un nivel elevado de incumplimientos legales, alguno de ellos graves, por lo que la valoración global sobre el cumplimiento de los aspectos de legalidad que hemos verificado es que el Ayuntamiento alcanza un índice de madurez del 16,5%. Esto se corresponde con un nivel de madurez N1, que indica que existen incumplimientos significativos generalizados de la normativa. Esto representa un índice de cumplimiento del CBCS 8 del 20,6%.

En relación con el ENS

Se dispone de una Política de Seguridad que, si bien precisa adecuadamente objetivos y misión de la entidad, marco legal y normativo, definición de roles y funciones, estructura organizativa y el proceso de aprobación y revisión de la misma, no ha sido aprobada por el órgano superior competente.



Del mismo modo, se ha desarrollado la normativa asociada a la Política de Seguridad, pero dicha normativa no ha sido formalmente aprobada

Se ha cumplimentado y remitido el Informe del Estado de la Seguridad (Informe INES).

Adicionalmente:

- No se ha elaborado una declaración de aplicabilidad ni adoptado las medidas de seguridad allí descritas.
- No se realizan las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010.
- No se han publicado en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes previstos en el ENS.

En materia de protección de datos personales

Se ha nombrado un delegado de protección de datos (DPD) de acuerdo con lo previsto en el artículo 37.1.a del RGPD, pero no se ha comunicado a la Agencia de Protección de Datos.

Adicionalmente:

- No se ha realizado un análisis de riesgos sobre sus tratamientos de datos personales ni, en su caso, las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.
- No se ha hecho público el registro de actividades de tratamiento, conforme al artículo 31.2 de la Ley Orgánica 3/2018.
- No se han aplicado las medidas organizativas y técnicas necesarias para proteger los datos personales, requeridas por el artículo 24.1 del RGPD.
- No se han ejecutado auditorías de cumplimiento en materia de protección de datos de las previstas en el artículo 32.1 del RGPD.

En relación con la Ley de factura electrónica

No se han llevado a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.

6. RECOMENDACIONES Y MEDIDAS PARA EL CUMPLIMIENTO DE LA LEGALIDAD

Como resultado de la auditoría realizada procede efectuar las recomendaciones que se señalan a continuación, para cuya atención el Ayuntamiento deberá dedicar los esfuerzos y recursos necesarios. También se señalan las medidas para el cumplimiento de la legalidad que deben adoptarse.

Sobre el inventario y control de dispositivos físicos (CBCS 1)

- 1) Aprobar formalmente un procedimiento para la gestión del inventario y el control de activos físicos que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo las fechas de dichas revisiones.
- 2) Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.

Sobre el inventario y control de software autorizado (CBCS 2)

- 3) Elaborar y aprobar formalmente un procedimiento para la gestión integral del *software* de la entidad que incluya:
 - La autorización de las instalaciones, la elaboración de listas de *software* autorizado (listas blancas), la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas del *software* instalado.
 - La definición de un plan de mantenimiento de la totalidad del *software* utilizado en el Ayuntamiento.
- 4) Identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte.

Sobre el proceso continuo de identificación y remediación de vulnerabilidades (CBCS 3)

- 5) Documentar los controles actualmente existentes, completarlos y aprobar formalmente unos procedimientos, de manera que incluyan las acciones actualmente implantadas y que considere, como mínimo, los siguientes aspectos:
 - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y las acciones actualmente establecidas de seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad.



- La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

- 6) Completar y aprobar formalmente el procedimiento existente de gestión unificada de usuarios con privilegios de administración, estableciendo las directrices para todos los sistemas de la entidad y que incluya:
 - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos.
 - Cuando existan razones de índole técnico que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas.
 - La utilización, para cada administrador de sistemas de la entidad, de diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (gestión del dominio y servidores, administración de equipos de usuario o tareas ofimáticas no administrativas).
 - La política de autenticación a aplicar a este tipo de cuentas.

Sobre las configuraciones seguras del software y hardware (CBCS 5)

- 7) Aprobar formalmente e implantar un procedimiento de configuración segura o bastionado de los sistemas, que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN².

Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.

² Las guías STIC (seguridad de las tecnologías de la información y de las comunicaciones) están estructuradas en series. Las series a las que hace referencia la recomendación corresponden a “guías generales”, “guías de entornos Windows” y “guías de otros entornos” respectivamente.



Sobre el registro de la actividad de los usuarios (CBCS 6)

- 8) Aprobar formalmente un procedimiento para el tratamiento de logs de auditoría de actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los logs. Para la revisión de logs es aconsejable su centralización en sistemas dedicados a tal efecto.

Sobre la copia de seguridad de datos y sistemas (CBCS 7)

- 9) Completar y aprobar formalmente el procedimiento para la gestión de copias de seguridad de datos y sistemas, especificando, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración y los requisitos de protección de las copias.

Sobre el cumplimiento de la legalidad (CBCS 8)

- 10) Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe:
 - Aprobar por parte del órgano superior competente la Política de Seguridad (PS) desarrollada.
 - Realizar la designación de las personas para los roles definidos en la PS y constitución de los órganos allí descritos.
 - Elaborar una declaración de aplicabilidad y adoptar las medidas de seguridad allí descritas.
 - Realizar las auditorías previstas en el artículo 34 del Real Decreto 3/2010.
 - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes.
- 11) En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe:
 - Comunicar a la Agencia de Protección de Datos el nombramiento del DPD.
 - Publicar y hacer accesible por medios electrónicos el registro de actividades del tratamiento.



- Realizar un análisis de riesgos sobre sus tratamientos de datos personales y, en su caso las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.
- Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 RGPD.
- Planificar y ejecutar auditorías sobre protección de datos.

12) Llevar a cabo la auditoría del registro de facturas exigida por la Ley 25/2013, de 27 de diciembre.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación. No se incluyen las medidas a implantar 10 a 12 por ser exigencias legales.

Gráfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones



Además de las recomendaciones anteriores, junto con el detalle al máximo nivel de las deficiencias de seguridad observadas, se ha



comunicado a los responsables del Ayuntamiento otras recomendaciones con una relación de riesgo potencial a mitigar y coste de su implantación menos favorable que las anteriores.



APÉNDICE. Metodología aplicada

1. La GPF-OCEX 5313 y el Esquema Nacional de Seguridad

La presente auditoría está basada en la Guía práctica de fiscalización de los OCEX GPF-OCEX 5313 *Revisión de los controles básicos de ciberseguridad* aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12/11/2018, que forma parte del *Manual de fiscalización* de la Sindicatura de Comptes y que puede consultarse en nuestra web. Para mayor detalle sobre la metodología utilizada nos remitimos a esa guía.

El contenido de la GPF-OCEX 5313, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, es coherente con los postulados del ENS, que es de obligado cumplimiento para todos los entes públicos. Esta alineación facilita la realización de las auditorías de ciberseguridad por parte de la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que verifica la Sindicatura están exigidos por el ENS.

No obstante, dada la amplitud del ENS, que está formado por 75 medidas de seguridad, para su inclusión en los CBCS se seleccionó una serie limitada de controles. Para seleccionar los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS³), que prioriza y clasifica los controles según su importancia para hacer frente a las ciberamenazas.

Los 20 controles de seguridad críticos del CIS son un conjunto conciso y priorizado de acciones de ciberdefensa, orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. La versión 7 de los controles CIS clasifica los seis primeros controles como básicos y son los que se han utilizado como referencia en la GPF-OCEX 5313 para establecer los controles básicos de ciberseguridad (CBCS) de los OCEX. A ellos se añadió el relativo a las copias de seguridad de datos y sistemas -por su importancia para la recuperación frente a un desastre o ataque exitoso y por tanto para garantizar una razonable ciber-resiliencia- y un octavo CBCS relacionado con el cumplimiento normativo, por su importancia en una administración pública.

³ Center for Internet Security, <www.cisecurity.org>.



Los ocho controles básicos de ciberseguridad debidamente referenciados con el ENS son:

Cuadro 2. Los CBCS y el ENS

Control	Medida de seguridad del ENS
CBCS 1 Inventario y control de dispositivos físicos	op.exp.1
CBCS 2 Inventario y control de <i>software</i> autorizado y no autorizado	op.exp.1 op.exp.2
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2 op.exp.4
CBCS 4 Uso controlado de privilegios administrativos	op.acc.4 op.acc.5
CBCS 5 Configuraciones seguras del <i>software</i> y <i>hardware</i> , dispositivos móviles, portátiles, equipos de sobremesa y servidores	op.exp.2 op.exp.3
CBCS 6 Registro de la actividad de los usuarios	op.exp.8 op.exp.10
CBCS 7 Copias de seguridad de datos y sistemas	mp.info.9
CBCS 8 Cumplimiento de la legalidad	ENS RGPD/LOPD Ley 25/2013

2. Criterios de auditoría: los controles básicos de ciberseguridad y sus subcontroles

Los CBCS son controles globales formados por varios subcontroles detallados que se muestran en la siguiente tabla. Todas nuestras comprobaciones tienen por finalidad contrastar su situación real en la entidad con las buenas prácticas recogidas en la GPF-OCEX 5313, que se resumen en el siguiente cuadro.

Los aspectos que se comprueban en cada CBCS se especifican con el máximo detalle en la GPF-OCEX 5313.

En cuanto a los índices o niveles objetivo que deben alcanzarse en cada CBCS y subcontrol, véase el apartado 4 siguiente.

Cuadro 3. Los CBCS y sus subcontroles

Control	Objetivo de control	Subcontrol	
CBCS 1 Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos <i>hardware</i> en la red, de forma 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 de dispositivos físicos no autorizados.
CBCS 2 Inventario y control de <i>software</i> autorizado	Gestionar activamente todo el <i>software</i> en los sistemas, de forma que solo se pueda instalar y ejecutar <i>software</i> autorizado.	CBCS 2-1: Inventario de SW autorizado	La entidad dispone de un inventario de SW completo, actualizado y detallado.
		CBCS 2-2: SW soportado por el fabricante	El SW 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 SW no autorizado	La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas 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 estas son identificadas en tiempo oportuno.
		CBCS 3-2: Priorización	Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al 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 forma que se garantiza que estas son resueltas en el tiempo previsto en el procedimiento.
		CBCS 3-4: Parcheo	La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.
CBCS 4 Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y 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 su correcto control.
		CBCS 4-2: Cambio de contraseñas por defecto	Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema.
		CBCS 4-3: Uso dedicado de cuentas de administración	Las cuentas de administración solo se realizan para las tareas que son 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 mediante dichas cuentas.
		CBCS 4-5: Auditoría y control	El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.

Control	Objetivo de control	Subcontrol	
CBCS 5 Configuraciones seguras del <i>software</i> y <i>hardware</i> de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer, implantar y gestionar la configuración de seguridad de los dispositivos móviles, portátiles, servidores y de sobremesa, mediante un proceso de control de cambios y gestión de la configuración riguroso, con el objetivo de prevenir ataques mediante 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 SW
		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 (vuelta a la configuración segura) en un periodo 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 eventos 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: Retención y protección	Los logs se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis. Durante dicho periodo, el control de acceso garantiza que no se producen accesos no autorizados.
		CBCS 6-3: Centralización y revisión de logs	Los logs de todos los sistemas son revisados periódicamente para detectar anomalías y posibles riesgos de seguridad del sistema. Se dispone de mecanismos para la centralización de los logs de auditoría, de forma que se facilite su revisión.
		CBCS 6-4: Monitorización y correlación	La entidad dispone de un SIEM (<i>security information and event management</i>) o una herramienta de analítica de logs para realizar correlación y análisis de logs.
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: Realización de copias de seguridad	La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.
		CBCS 7-2: Realización de pruebas de recuperación	Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando 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, mediante 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 con los requisitos legales y reglamentarios que le son de aplicación.	CBCS 8-1: Cumplimiento del ENS	La entidad cumple con los requerimientos establecidos en el ENS.
		CBCS 8-2: Cumplimiento de la LOPD/RGPD	La entidad cumple con los requerimientos establecidos en la LOPD/RGPD
		CBCS 8-3: Cumplimiento de la Ley 25/2013	La entidad cumple con los requerimientos establecidos en la Ley 25/2013, de 27 de diciembre.



3. Confianza en las auditorías del ENS

Dado que los CBCS están alineados con el ENS, cuando su revisión se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del Real Decreto 3/2010 por el que se aprueba el ENS, la revisión podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría y determinadas comprobaciones podrán darse por cumplidas.

Para depositar confianza en dichas auditorías externas de seguridad, deberán cumplir con los requisitos legalmente establecidos como son, entre otros, que las entidades certificadoras estén acreditadas y constar en la sección “Entidades de certificación acreditadas” de la página web del CCN (es necesario acreditarlas si se pretende certificar el cumplimiento del ENS). Cuando se haya depositado confianza en estas auditorías se señalará expresamente en el informe.

4. Evaluación de los resultados del trabajo

Los resultados del trabajo se analizan y evalúan a dos niveles: subcontroles y CBCS.

Subcontroles

Los CBCS son controles globales compuestos por varios controles detallados o subcontroles (tal como puede verse en el apartado 2 anterior), de los que hemos revisado su diseño y eficacia operativa.

El trabajo de auditoría consiste básicamente en evaluar cada subcontrol en función de los resultados de las pruebas realizadas y las evidencias obtenidas, o bien de la información proporcionada en el informe de auditoría del ENS, si existe y si confiamos en él. Cada subcontrol se evalúa según la escala mostrada en el siguiente cuadro:



Cuadro 4. Evaluación de los subcontroles

Evaluación	Descripción
Control efectivo	Cubre al 100% con el objetivo de control y: <ul style="list-style-type: none"> - El procedimiento está formalizado (documentado y aprobado) y actualizado - El resultado de las pruebas realizadas para verificar su 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: <ul style="list-style-type: none"> - Se sigue un procedimiento formalizado, aunque puede presentar aspectos de mejora (detalle, nivel de actualización, nivel de aprobación, etc.). - Las pruebas realizadas para verificar la implementación son satisfactorias. - Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.
Control poco efectivo	Cubre de forma muy limitada el objetivo de control y: <ul style="list-style-type: none"> - Se sigue un procedimiento, aunque este puede no estar formalizado. - El resultado de las pruebas de implementación y de eficacia no es satisfactorio. Cubre en líneas generales el objetivo de control, pero: <ul style="list-style-type: none"> - 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 están generalizados).
Control no efectivo o no implantado	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).

Nivel de madurez de los CBCS

Para determinar la situación global de cada control básico de ciberseguridad hemos utilizado el modelo de nivel de madurez de los procesos de control de acuerdo con lo establecido en la GPF-OCEX 5313, que a su vez está basada en la *Guía de seguridad CCN-STIC 804* del Centro Criptológico Nacional, usando una escala, según se resume en el siguiente cuadro.



Cuadro 5. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El CBCS no está siendo aplicado en este momento.
N1 Inicial / ad hoc	10	<p>El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado.</p> <p>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 tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.</p>
N2 Repetible, pero intuitivo	50	<p>Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas. No hay procedimientos escritos ni actividades formativas.</p> <p>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. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.</p>
N3 Proceso definido	80	<p>Los procesos están estandarizados, documentados y comunicados con acciones formativas.</p> <p>Se dispone de un catálogo de procesos que se mantiene actualizado. Estos garantizan la consistencia 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 la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).</p> <p>El éxito es algo más que buena suerte: se merece.</p> <p>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.</p>
N4 Gestionado y medible	90	<p>La dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere.</p> <p>Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La dirección es capaz de establecer objetivos cualitativos y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.</p> <p>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 era solamente cualitativa.</p>

Nivel	Índice	Descripción
N5 Optimizado	100	<p>Se siguen buenas prácticas en un ciclo de mejora continua.</p> <p><i>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, utilizándose como indicadores en la gestión de la mejora de los procesos.</i></p> <p><i>En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.</i></p>

La evaluación que realizamos sobre el nivel de madurez no se ha basado únicamente en los procesos teóricos o en los procedimientos aprobados, sino también en la verificación de su aplicación práctica.

Para evaluar el nivel de madurez de cada CBCS se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control del CBCS.

Este modelo proporciona una base sólida para formarse una idea general de la situación en la entidad revisada en relación con los controles de ciberseguridad y el cumplimiento de la legalidad en esta materia. También permite comparar resultados entre distintos entes y entre distintos periodos.

5. Nivel de madurez mínimo requerido en función de la categoría de los sistemas de información auditados

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:

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Cumplir sus obligaciones diarias de servicio.
- d) Respetar la legalidad vigente.
- e) Respetar los derechos de las personas.

La categoría de un sistema será de aplicación a todos los sistemas empleados para la prestación de los servicios de la administración electrónica y soporte del procedimiento administrativo general de un ente.



A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se deben tener en cuenta las cinco dimensiones de la seguridad:

Confidencialidad Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Integridad Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.

Disponibilidad Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.

Autenticidad Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Trazabilidad Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO.

Teniendo en cuenta lo anterior, se definen tres categorías de sistemas de información:

- a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
- c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La categoría de un sistema de información, en materia de seguridad, modula el equilibrio entre la importancia de la información que maneja, de los servicios que presta y el esfuerzo de seguridad requerido, en función de los



riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

De acuerdo con la categoría de cada sistema, los niveles mínimos de exigencia o de madurez requeridos son⁴:

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%)

Los sistemas auditados en el presente informe están clasificados como de categoría MEDIA.

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

6. Indicadores globales

A efectos del ENS, la guía CCN-STIC-824 contempla una serie de indicadores agregados capaces de aportar información resumida sobre el estado de la seguridad en los organismos públicos. Dichos indicadores han sido adaptados para su aplicación a los CBCS ya que permiten llevar a cabo tanto un resumen del estado de las medidas de seguridad de cada ayuntamiento a los efectos del ENS, como de los CBCS:

- El índice de madurez sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de CBCS.
- El índice de cumplimiento analiza igualmente el nivel de madurez alcanzado, pero en relación a la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema. Es decir, compara el índice de madurez con el nivel mínimo exigido para dicha categoría en el ENS, que en la presente auditoría es N3 (80%) para todos los casos.

⁴ Informe nacional del estado de seguridad de los sistemas de las tecnologías de la información y la comunicación, de 2018, apartado 3.1. En los diferentes perfiles se evalúan los controles mediante un nivel de exigencia, también conocido como nivel de madurez, y se fija el nivel mínimo de exigencia requerido.



TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, el borrador previo del Informe de auditoría se discutió con los técnicos responsables del área de sistemas de información del Ayuntamiento de Sant Vicent del Raspeig para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

Posteriormente, en cumplimiento del artículo 16 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, y del artículo 55.1.c) del Reglamento de Régimen Interior de la Sindicatura de Comptes, así como del acuerdo del Consell de esta Institución por el que tuvo conocimiento del borrador del Informe de auditoría correspondiente al ejercicio 2020, el mismo se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Transcurrido dicho plazo no se han recibido alegaciones.



APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, y del artículo 55.1.h) de su Reglamento de Régimen Interior y del Programa Anual de Actuación de 2020 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 18 de junio de 2020, aprobó este informe de auditoría.