SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE AUDITORÍA DE CIBERSEGURIDAD DE LA EMPRESA MUNICIPAL DE TRANSPORTES DE VALÈNCIA, SAU

Exercici 2020

RESUMEN

Por qué realizamos esta auditoría

El artículo 11 de la Ley de Sindicatura de Comptes establece que, en el desarrollo de su función fiscalizadora, la Sindicatura está facultada para verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico-financiera, contable y de gestión. Cada vez un mayor número de aspectos de la gestión pública se realiza con el soporte y apoyo de complejos sistemas y la conectividad por internet se ha convertido en una característica fundamental de dichos sistemas de información. Esta circunstancia ha traído aparejado un gran crecimiento de las amenazas de todo tipo provenientes del ciberespacio, multiplicándose los incidentes de seguridad de los que son víctimas los sistemas de información y comunicaciones de las entidades públicas, con graves repercusiones potenciales, tanto económicas como en la prestación de los servicios públicos. Adicionalmente, en el Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022, se señala la ciberseguridad como una de las áreas de alto riesgo y prioritarias para llevar a cabo la tarea fiscalizadora. Por esta razón se ha realizado una **auditoría de ciberseguridad** de la Empresa Municipal de Transportes de València, SAU, focalizada en las áreas de ingresos por transporte de viajeros, de contabilidad y de tesorería, referida a la situación de los controles durante 2020.

Conclusiones

Hemos constatado un bajo índice de madurez de los controles de ciberseguridad, cuantificado en un 51,5%, siendo el objetivo del 80,0%.

Frente a la multiplicidad de amenazas existentes se requiere mayor concienciación en relación con la ciberseguridad por parte de los órganos superiores de la EMT y más recursos dedicados a la seguridad de la información, ya que la subsanación de las deficiencias que se señalan a lo largo del informe requiere actuaciones e inversiones, tanto en medios materiales como personales.

Es necesario actualizar y reforzar la gobernanza de la seguridad de la información, alineándola con lo establecido en el Esquema Nacional de Seguridad.

En la auditoría hemos observado que la situación de los controles de acceso privilegiado a los sistemas debe ser mejorada, ya que existen graves deficiencias en los controles relacionados con los usuarios administradores de algunos sistemas que proporcionan soporte a procesos críticos de negocio.

Recomendaciones

Además de las deficiencias de control significativas, que deben ser subsanadas con urgencia, como resultado de la auditoría realizada se han efectuado 16 recomendaciones para cuya atención la EMT deberá dedicar los esfuerzos y recursos necesarios.

Respuesta de la entidad

Durante la fase de alegaciones, la Dirección de EMT ha enfatizado en el proceso de mejora del sistema de seguridad de la información emprendido por la entidad durante los dos ejercicios anteriores y en su intención de atender las recomendaciones realizadas.

Tanto durante el transcurso del trabajo de campo de la auditoría como en la fase de alegaciones, la EMT nos ha informado de la adopción de varias iniciativas para subsanar deficiencias observadas, algunas subsanadas y otras pendientes al emitir el informe.

En las valoraciones del nivel de madurez de los controles, hemos tenido en cuenta solo las mejoras ya implantadas y en funcionamiento en el momento de nuestra revisión, existiendo otras iniciativas en marcha para atender buena parte de las recomendaciones que hemos realizado cuyo diseño y eficacia operativa podrán ser evaluadas en un posterior informe de seguimiento.

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.

Informe de auditoría de ciberseguridad de la Empresa Municipal de Transportes de València, SAU

Ejercicio 2020

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

El artículo 6 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, incluye entre sus funciones, además de las referidas al control externo de la gestión económico-financiera del sector público valenciano y de sus cuentas, aquellas que de acuerdo con el ordenamiento jurídico sean convenientes para asegurar adecuadamente el cumplimiento de los principios financieros, de legalidad, de eficacia, de economía y de transparencia, exigibles al sector público, así como la sostenibilidad ambiental y la igualdad de género. Por otra parte, el artículo 11 de la misma Ley establece que en el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico-financiera, contable y de gestión. Cada vez un mayor número de aspectos de la gestión pública se realiza con el soporte y apoyo de complejos sistemas, y la conectividad por internet se ha convertido en una característica fundamental de dichos sistemas de información. Esta circunstancia ha traído aparejado un gran crecimiento de las amenazas de todo tipo provenientes del ciberespacio, multiplicándose los incidentes de seguridad de los que son víctimas los sistemas de información y comunicaciones de las entidades públicas, con graves repercusiones potenciales, tanto económicas como en la prestación de los servicios públicos.

En la guía de auditoría *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa*, del *Manual de fiscalización* de la Sindicatura de Comptes se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas, razón por la que los auditores públicos deben prestar cada vez más atención a dichas cuestiones. En línea con lo anterior, en el Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022 se señala a la ciberseguridad como una de las áreas de alto riesgo y prioritarias para llevar a cabo la tarea fiscalizadora.

Considerando que las empresas públicas locales no son ajenas a la problemática planteada por la ciberseguridad, el Consell de la Sindicatura de Comptes acordó incluir en el programa anual de actuación de 2020 (PAA2020) la realización de una auditoría de ciberseguridad de la Empresa Municipal de Transportes de València, SAU, focalizada en las áreas de ingresos por transporte de viajeros, contabilidad y de tesorería.

El PAA2020 también establece que la Sindicatura realizará una auditoría de las cuentas de 2019 de la EMT, centrada en las áreas de ingresos por transporte de viajeros y de la tesorería, que se publicará en un informe específico.

Consideraciones sobre el fraude experimentado por EMT

Durante el ejercicio 2019 la EMT ha sido víctima de un tipo de estafa conocida como "fraude del CEO"[1] que ha tenido como consecuencia económica la pérdida de una cantidad superior a cuatro millones de euros.

Con objeto de dilucidar las deficiencias de gestión y seguridad que han posibilitado la perpetración de la estafa y depurar las responsabilidades sobre las mismas, se han iniciado durante 2019 y 2020 una comisión de investigación por parte del Consejo de Administración de la EMT, un proceso judicial y una investigación del Tribunal de Cuentas, trabajos actualmente en curso y cuyos resultados se encuentran pendientes de conclusión y/o publicación.

La presente auditoría no tiene como objeto incidir en este fraude y no serán revisados los hechos concretos a través de los que se ha materializado la estafa, que ya están siendo investigados por los organismos competentes y no debemos interferir en las actuaciones judiciales en curso.

No obstante, y en conformidad con el enfoque de riesgos recogido en las normas de auditoría, durante la planificación y ejecución de la auditoría sí han sido tenidas en consideración las circunstancias generales del fraude y hemos incluido en el ámbito de la revisión las áreas de interés relacionadas con los hechos, en particular el área de tesorería, dados los riesgos de posible falta de eficacia de los controles de seguridad de la información en dicha área.

2. RESPONSABILIDADES DE LOS ÓRGANOS DE LA ENTIDAD EN RELACIÓN CON LOS CONTROLES DE CIBERSEGURIDAD

El Pleno del Ayuntamiento de València, órgano que de acuerdo con los Estatutos de la EMT asume las funciones de la Junta General, tiene la responsabilidad de impulsar en la entidad, como empresa sujeta al derecho privado y cuya titularidad es 100% del Ayuntamiento, la implementación de medidas equivalentes al Esquema Nacional de Seguridad (ENS).

---

[1] Según el Centro Criptológico Nacional, "los ataques de *Business Email Compromise* (BEC), habitualmente conocidos como *Fraude al CEO*, son un tipo de ataques en auge en los últimos años, ya que requieren por lo general poco conocimiento técnico e inversión en infraestructura –fundamentalmente el engaño se basa en ingeniería social–, pero pueden llegar a reportar grandes cantidades de dinero a los delincuentes".

"Este tipo de fraude consiste en que un empleado de alto rango o con capacidad para hacer transferencias o acceso a datos de cuentas, recibe un correo, supuestamente de su jefe, ya sea su CEO, presidente o director de la empresa. En este mensaje le pide ayuda para una operación financiera confidencial y urgente. Si el empleado no se diera cuenta de que es un mensaje fraudulento podría responder a su supuesto jefe y caer en el engaño."

Por otra parte, el Consejo de Administración de la EMT es el órgano responsable de que existan unos adecuados controles internos, siendo el **máximo responsable de la seguridad de los sistemas de información y las comunicaciones**. De acuerdo con sus competencias, el Consejo debe garantizar que el funcionamiento de la entidad resulte conforme con las normas aplicables y que los controles internos proporcionen una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplan las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el ENS: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La implicación del Consejo y del director-gerente es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información (SGSI). Ésta deberá materializarse en aspectos tales como[2]:

- Formular y aprobar la política de seguridad de la información (PSI) y difundirla a la totalidad de los miembros de la organización, así como, en su caso, a proveedores y clientes.
- Asignar los roles y responsabilidades en seguridad de la información.
- Proporcionar los recursos necesarios y asegurar que se implantan programas de concienciación, formación y capacitación.
- Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- Autorizar la implementación y operación del SGSI.
- Dirigir las revisiones periódicas de la PSI y velar por la realización de las auditorías internas.

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

La responsabilidad de la Sindicatura de Comptes es concluir sobre la situación de los controles 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

[2] *Guía de Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*.

requerimientos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una evaluación de los controles de ciberseguridad.

Ámbito objetivo

La presente fiscalización está focalizada en la revisión de una serie de controles de seguridad de las tecnologías de la información y las comunicaciones implantados en los sistemas que soportan dos de los procesos de gestión más relevantes, relacionados con sendas áreas que están siendo auditadas por otro equipo de fiscalización de la Sindicatura. Estas áreas son la gestión de tesorería (de muy alto riesgo, tal como han acreditado las circunstancias de los últimos meses y señaladas en el apartado 1 anterior) y los ingresos por transporte de viajeros (actividad principal de la entidad). También hemos incluido dentro de nuestro alcance la contabilidad.

Dado el elevado riesgo de estas áreas, la auditoría de la ciberseguridad ha consistido en la revisión de dos grupos de controles en estas áreas:

1. Revisión de los **controles básicos de ciberseguridad (CBCS).**

2. Revisión de otros **controles generales de tecnologías de la información relevantes** para la seguridad de las aplicaciones de gestión, adicionales a los CBCS.

Consideramos relevantes al conjunto de controles revisados porque su ausencia o su mal funcionamiento representaría una deficiencia significativa o una debilidad material de control interno y sobre la seguridad de los procesos señalados.

En el apéndice 1 se proporciona un mayor detalle tanto del ámbito objetivo de la auditoría (qué controles se han revisado) como de la metodología utilizada.

Ámbito temporal

En cuanto al ámbito temporal del trabajo, las conclusiones se refieren a la situación de los controles en 2020. La auditoría se inició el 4 de junio de 2020 y el trabajo de campo finalizó el 30 de septiembre de 2020.

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 las guías prácticas de fiscalización *GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad (CBCS)* y *GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica*, y en el resto de las secciones aplicables del *Manual de fiscalización* de la Sindicatura de Comptes. En total se han revisado 53 subcontroles o controles detallados, agrupados en los 15 controles principales que se señalan en el cuadro 1.

La presente auditoría ha sido realizada en coordinación con otro equipo de auditoría de la Sindicatura que está realizando la fiscalización de regularidad, para el que también hemos revisado los controles internos informatizados de las aplicaciones de gestión relacionadas y cuyos resultados se integrarán en el informe que emitan. Para la ejecución del trabajo también se ha contado con la colaboración de expertos externos.

Hemos evaluado la situación de los controles 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 Esquema Nacional de Seguridad.

De acuerdo con dicha metodología, los sistemas de información revisados están clasificados como de categoría de seguridad MEDIA, y el nivel de madurez requerido u objetivo es *N3, proceso definido*[3] y un índice de madurez del 80%.

Confidencialidad

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

4. CONCLUSIONES

Bajo índice de madurez de los controles de ciberseguridad

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el grado de control existente en la gestión de los controles de ciberseguridad señalados en el apartado 3 alcanza un **índice de madurez del 51,5%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles en general se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente.

El índice de madurez real está lejos del objetivo del 80% y del nivel de madurez N3.

Agregando los resultados obtenidos por categorías de controles, según la clasificación de controles incluida en la *GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica*, se obtienen los resultados detallados mostrados en el cuadro 1.

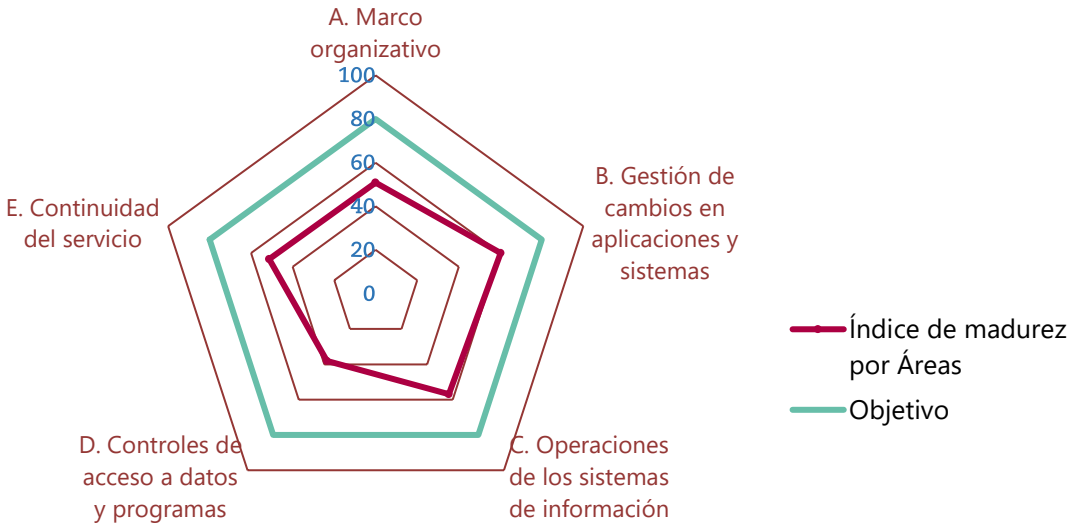
[3] Los niveles de madurez se describen en el cuadro 4 del apéndice 1.

Cuadro 1. Índice de madurez por áreas de los controles de ciberseguridad de la EMT

Áreas	Controles principales		Índice de madurez
A. Marco organizativo	A.1 Cumplimiento de legalidad (CBCS 8)	41,7%	**50,9% (N2)**
	A.3 Formación y concienciación	60,0%	
B. Gestión de cambios en aplicaciones y sistemas	B.3 Gestión de cambios	60,2%	**60,2% (N2)**
C. Operaciones de los sistemas de información	C.1 Inventario de *hardware* (CBCS 1)	63,8%	**56,9% (N2)**
	C.1 Inventario de *software* (CBCS 2)	70,0%	
	C.2 Gestión de vulnerabilidades (CBCS 3)	60,7%	
	C.3 Configuraciones seguras (CBCS 5)	49,5%	
	C.4 Registro de la actividad de los usuarios (CBCS 6)	51,8%	
	C.5 Servicios externos	49,8%	
	C.8 Gestión de incidentes	53,1%	
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	38,6%	**38,1% (N1)**
	D.2 Mecanismos de identificación y autenticación	40,3%	
	D.3 Gestión de derechos de acceso	36,4%	
	D.4 Gestión de usuarios	37,3%	
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	51,3%	**51,3% (N2)**
	General		**51,5% (N2)**

Y de una forma más sintética y gráfica, la situación observada de los controles queda reflejada en el gráfico 1.

Gráfico 1. Índice de madurez, por áreas, de los controles de ciberseguridad de la EMT



Se requiere mayor concienciación y más recursos dedicados a la seguridad de la información

A la vista de los resultados obtenidos en la revisión de los controles de ciberseguridad, consideramos que, **aunque existe cierto nivel de control, hay posibilidades de mejora, por lo que es necesario que tanto el Consejo de Administración como el Pleno del Ayuntamiento de València, en su condición de Junta General de la sociedad, 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 desde los órganos de gobierno a todos los niveles y departamentos de la EMT.

La subsanación de las debilidades de control señaladas y de las deficiencias de los controles de ciberseguridad que se señalan a lo largo del informe requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.

Insuficiente gobernanza de la seguridad de la información

La EMT dispone de una *Política de seguridad de la información* (PSI), que **no ha sido aprobada por el Consejo de Administración**, máximo órgano de dirección de EMT, tal como requieren el ENS y la norma UNE-EN ISO/IEC 27001/27002, ni cumple con todos los requisitos establecidos en ambas normas.

La gestión de la seguridad de los sistemas de información requiere establecer una organización de la seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte y los mecanismos de coordinación y resolución de conflictos, designando un **Comité de Gestión de la Seguridad de la Información**, de forma que la gobernanza de la seguridad de la información esté adecuadamente estructurada.

La PSI que apruebe el Consejo de Administración debe recoger con claridad las responsabilidades sobre la gestión, administración y seguridad de los sistemas descentralizados (aquellos gestionados de manera autónoma por los departamentos), ya que la actual PSI no refleja fielmente las particularidades del modelo organizativo de la entidad. La administración de sistemas de información, que de manera general se realiza por parte del Área de Desarrollo, es asumida en determinados casos por los propios departamentos de la entidad, que administran las aplicaciones específicas que soportan los procesos críticos de sus departamentos. Esta situación no resulta recomendable, ya que dificulta la capacidad operativa del responsable de seguridad como figura que debe velar por la aplicación homogénea de medidas de seguridad en el conjunto de los sistemas de la entidad y su coherencia en un entorno de sistemas administrados por distintos departamentos. Además, existe un elevado riesgo de que los departamentos carezcan de las competencias profesionales requeridas para la administración de sistemas y de que los intereses departamentales no se encuentren alineados con los principios de la seguridad de la información aprobados por la organización.

La situación de los controles de acceso privilegiado debe ser mejorada

Existen graves deficiencias en los controles relacionados con los usuarios administradores de los sistemas, particularmente en aquellos gestionados de manera autónoma por los departamentos correspondientes (identificados más adelante en el informe como "sistemas descentralizados") y que proporcionan soporte a procesos críticos de negocio.

Las carencias detectadas, entre las que destacan una insuficiente aplicación del principio de mínimo privilegio y una deficiente gestión de los registros de actividad de los usuarios administradores, tienen un reducido coste de corrección y un alto impacto en el nivel general de ciberseguridad de la entidad.

Durante el trámite de alegaciones la EMT nos ha informado de la existencia de una propuesta de trabajo para la resolución de estas deficiencias. Hemos verificado la existencia de dicha propuesta y del plan de trabajo, que incluye las modificaciones necesarias en cuanto a la gestión adecuada de derechos de acceso y privilegios administrativos de los usuarios, registros de actividad y aplicación adecuada del principio de mínimo privilegio. Al emitir el presente informe esas acciones estaban en fase de implantación.

Insuficiente grado de adecuación a la normativa de ciberseguridad

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel insatisfactorio de adecuación a la normativa de

ciberseguridad. El Ayuntamiento de València y el Consejo de Administración de la EMT tienen la responsabilidad de impulsar un grado de implementación de medidas equivalentes al Esquema Nacional de Seguridad, en el marco del cumplimiento de la normativa en materia de protección de datos, y deben promover las acciones necesarias para subsanar esa situación.

Otros hallazgos de la auditoría

En el apéndice 2 se señalan los hallazgos de la auditoría que sustentan las conclusiones de este apartado y las recomendaciones que se destacan en el siguiente apartado.

5. RECOMENDACIONES

Además de las deficiencias de control significativas señaladas en el apartado 4 anterior, que deben ser subsanadas con urgencia, como resultado de la auditoría realizada procede efectuar las recomendaciones que se señalan a continuación, para cuya atención la EMT 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 y que contemple las revisiones periódicas de *hardware* y su actualización, incluyendo las fechas de dichas revisiones.

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

2. Elaborar y aprobar un procedimiento para la gestión integral del *software* de la entidad que contemple:

   - 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*.
   - La definición de un plan de mantenimiento de la totalidad del *software* utilizado en la entidad, incluyendo tanto el gestionado por parte de la EMT como el gestionado por parte de terceros.
   - La revisión, identificación y actualización de los sistemas que se encuentran fuera del período de soporte.

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

3. Aprobar un procedimiento de identificación y remediación de vulnerabilidades que formalice y amplíe el proceso actual, que se aplique a la totalidad de sistemas de la entidad 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)

4. Formalizar un único procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad y que incluya:

   - Aplicación del principio de mínimo privilegio en la asignación de permisos a usuarios en todos los sistemas de entidad (esto es especialmente aplicable al departamento financiero).
   - 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 creación y utilización de diferentes cuentas para un mismo usuario con distintos niveles de privilegios administrativos, adecuando la asignación de permisos a los distintos tipos de tareas a realizar.
   - Incluir las cuentas para administración de sistemas utilizadas por los servicios de mantenimiento externos.

5. Activar y gestionar los registros de actividad en todos los sistemas de la entidad, habilitando específicamente aquellos registros que detallan las acciones de los usuarios administradores.

Sobre el control de acceso a datos y programas (D2, D3 y D4)

6. Finalizar y aprobar el procedimiento de control de accesos, actualmente en estado de borrador, incluyendo el detalle necesario sobre la identificación y autenticación de los usuarios, la gestión y provisión de derechos de acceso con el principio del mínimo privilegio y la gestión continuada. Dicho procedimiento debe contemplar

tanto los sistemas centralizados como los descentralizados.

7. Mejorar el proceso de autenticación del sistema que soporta el proceso contable, mediante la configuración adecuada de los mecanismos y herramientas existentes en la plataforma, y aplicar adecuadamente el criterio de mínimo privilegio en la asignación de derechos de acceso a dicho sistema.

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

8. Aprobar 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, 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 CCN[4].

   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.

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

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

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

10. Aprobar formalmente un procedimiento para la gestión de copias de seguridad de datos y sistemas que defina, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, las ubicaciones, los responsables, las pruebas de restauración y los requisitos de protección de las copias. La política de copias de seguridad debe estar basada en las necesidades de disponibilidad y conservación de la información, requisitos que deberán ser especificados por los distintos servicios de la entidad.

[4] 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 corresponde a "guías generales", "guías de entornos Windows" y "guías de otros entornos" respectivamente.

El procedimiento debe contemplar la gestión del servicio prestado por el proveedor externo para la realización de copias, basado en el establecimiento de acuerdos de nivel de servicio entre las partes y la monitorización de indicadores.

Sobre la formación y concienciación (A3)

11. Desarrollar un plan de formación y concienciación en materia de seguridad de la información que implique y motive a los empleados, desde los puestos operativos hasta la alta dirección, teniendo presente los riesgos a los que se exponen los distintos colectivos y adaptando el contenido a cada uno de ellos.

Sobre la gestión de cambios (B3)

12. Aprobar formalmente un procedimiento para la gestión continua de cualquier cambio en aplicaciones y sistemas, tanto en su configuración como en los componentes y arquitectura, que especifique y amplíe las acciones actualmente implantadas, que defina los roles necesarios para asumir las diferentes responsabilidades y que asigne los roles correspondientes al personal competente para ello.

Sobre la gestión de servicios externos (C5)

13. Aprobar formalmente un procedimiento para la gestión continua de los servicios externos contratados por la EMT, que defina tanto los pasos previos a la contratación del servicio como las actividades de gestión durante la prestación del mismo, y que especifique lo siguiente:

    - La definición de las características y requisitos del servicio, los requisitos de seguridad, los acuerdos de nivel de servicio, las responsabilidades de ambas partes y las consecuencias del incumplimiento de los acuerdos establecidos. En definitiva, es el contenido mínimo aconsejable que debe ser incluido en los pliegos de prescripciones técnicas.
    - Las actividades destinadas a medir el cumplimiento de las obligaciones de servicio y los acuerdos de nivel de servicio, así como el personal responsable de realizarlas.

Sobre la gestión de incidentes (C8)

14. Aprobar formalmente un procedimiento para la gestión de eventos e incidentes de seguridad que recoja el plan de actuación tras su detección. El procedimiento debería incluir:

    - la definición de los roles necesarios para asumir las diferentes responsabilidades,
    - la asignación de dichos roles al personal competente,
    - el escalado al responsable de la gestión de los mismos,

- la toma de decisiones urgentes,
- la asignación de recursos para el análisis, respuesta e investigación de los incidentes,
- la comunicación de los mismos a partes interesadas internas y externas,
- la implantación de medidas para evitar incidentes similares y
- la mejora continua del proceso de gestión.

Sobre el cumplimiento de la legalidad (CBCS 8)

15. Implantar las medidas necesarias para que el sistema de gestión de la seguridad de la información de la EMT sea coherente con los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad, o equivalentes. Específicamente, la EMT debe:

    - Actualizar la *Política de Seguridad de la Información* actual, de modo que satisfaga todos los requisitos establecidos en el ENS y/o se adecue a las prácticas de la norma UNE-EN ISO/IEC 27001[5]. Es especial, debe ser aprobada por el Consejo de Administración, conforme al artículo 11 del ENS y las recomendaciones de la norma UNE-EN ISO/IEC 27001.
    - El Consejo de Administración debe designar a los distintos actores en materia de seguridad de la información, en particular al Comité de Seguridad de la Información y al responsable de seguridad, entre otros. La gestión de la seguridad de los sistemas de información exige establecer una organización de la seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte y los mecanismos de coordinación y resolución de conflictos[6].

16. En relación con la protección de datos personales, la EMT debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular, debe:

    - Aplicar la totalidad de medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 RGPD.
    - Planificar y ejecutar las auditorías de cumplimiento en materia de protección de datos.

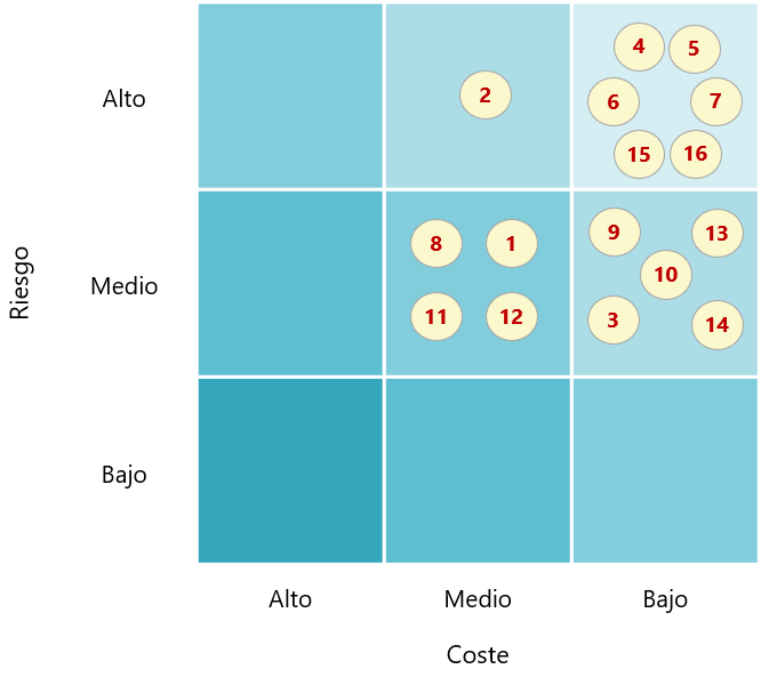
[5] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.*

[6] Véase el artículo 10 del ENS y la *Guía de Seguridad de las TIC CCN-STIC 801 ENS Responsabilidades y funciones.*

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación.

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, hemos comunicado a los responsables de la EMT otras recomendaciones con una relación de riesgo potencial a mitigar y coste de su implantación menos favorable que las anteriores.

Durante la fase de alegaciones la Dirección de EMT ha enfatizado en el proceso de mejora del sistema de seguridad de la información emprendido por la entidad durante los dos ejercicios anteriores y en su intención de atender las recomendaciones realizadas. En las valoraciones del nivel de madurez de los controles hemos tenido en cuenta solo las mejoras ya implantadas y en funcionamiento en el momento de nuestra revisión, existiendo otras iniciativas en marcha, en fase de planificación o de implantación, para atender buena parte de las recomendaciones que hemos realizado, cuyo diseño y eficacia operativa podrán ser evaluadas en un posterior informe de seguimiento.

APÉNDICE 1
Metodología aplicada

Ámbito objetivo

La presente fiscalización está focalizada en la revisión de la ciberseguridad y los controles de tecnologías de la información (TI) de los sistemas que soportan dos de los procesos de gestión más relevantes, como son la gestión de tesorería (de muy alto riesgo, tal como han acreditado las circunstancias de los últimos meses en EMT) y los ingresos por transporte de viajeros (actividad principal de la entidad).

Las aplicaciones identificadas como significativas para la gestión de los procesos de tesorería e ingresos y sobre las que se han revisado los controles relevantes, son las siguientes:

- CTI, para la gestión de los ingresos por transporte de viajeros.
- EXPERT, para la gestión de la contabilidad y tesorería.

Dado el elevado riesgo de estas áreas, el trabajo ha consistido en la revisión de dos grandes bloques:

Revisión de los controles básicos de ciberseguridad (CBCS).

Se ha aplicado la metodología establecida en la *GPF-OCEX 5313, Revisión de los controles básicos de ciberseguridad*, que incluye la revisión de siete controles que han sido debidamente referenciados con el Esquema Nacional de Seguridad, y la verificación del cumplimiento de diversas normas relacionadas con la seguridad de la información.

Los ocho CBCS establecidos en la GPF-OCEX 5313 son los siguientes:

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

La revisión ha incluido los controles relacionados con los sistemas identificados como significativos para la gestión de los procesos de tesorería e ingresos:

- las aplicaciones informáticas que soportan la gestión de los ingresos por transporte de viajeros, la contabilidad y la tesorería.
- las bases de datos subyacentes

- los sistemas operativos instalados en cada uno de los sistemas que integran la aplicación de gestión (por ejemplo, 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, se han analizado los siguientes tipos de elementos:

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

Revisión de otros controles generales de TI relevantes para las aplicaciones de gestión de los procesos de tesorería e ingresos.

Dado que hemos calificado el riesgo de auditoría de estas áreas como ALTO, hemos considerado necesario ampliar los CBCS con otra serie de siete CGTI adicionales, del total de controles detallados en la *GPF-OCEX 5330, Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica*. Dichos controles adicionales los consideramos relevantes porque su ausencia o su mal funcionamiento representa una deficiencia significativa o una debilidad material de control interno sobre las aplicaciones de gestión de los procesos de tesorería e ingresos, que están siendo auditados por otro equipo de auditoría (y nuestros resultados les serán de utilidad).

Los siete controles, adicionales a los CBCS, identificados como relevantes para los objetivos de esta auditoría, son los siguientes:

- Formación y concienciación (A.3.3)
- Gestión de cambios (B.3)
- Servicios externos (C.5)
- Gestión de incidentes (C.8)
- Mecanismos de identificación y autenticación (D.2)
- Gestión de derechos de acceso (D.3)
- Gestión de usuarios (D.4)

Aplicabilidad del Esquema Nacional de Seguridad (ENS)

En el CBCS 8 se ha revisado el cumplimiento con determinados aspectos que se consideran relevantes de la normativa básica en materia de seguridad de los sistemas y de la información.

Es conveniente aclarar que, dado que el ente auditado es una sociedad mercantil, la obligación sobre el cumplimiento normativo debe ser matizada por los motivos que exponemos a continuación:

- La EMT es una entidad de derecho privado cuyo capital es íntegramente público, ya que pertenece en su totalidad al Ayuntamiento de València.

- El ámbito subjetivo de aplicación del Real Decreto 3/2010, de 8 de enero (modificado por el Real Decreto 951/2015), por el que se aprueba el Esquema Nacional de Seguridad, se encuentra determinado por las leyes 39/2015 y 40/2015. Del análisis de dichas leyes se desprende que "*El Real Decreto 3/2010 será de aplicación a las entidades de derecho privado vinculadas o dependientes de la Administración de las Entidades Locales en las materias en que les sea de aplicación la normativa presupuestaria, contable, de control financiero, de control de eficacia y contratación, de acuerdo a lo dispuesto por la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, así como en el ejercicio de las funciones públicas que les hayan sido atribuidas estatutariamente, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta.*"[7]

  A la vista de los artículos 3 y 24 de los estatutos sociales de la EMT, aprobados el 31 de mayo de 2013, **consideramos que el RD 3/2010, de 8 de enero (ENS) no es de aplicación directa en la entidad**, dado que la EMT no está sujeta a las disposiciones de la Ley 7/1985, de 2 de abril Reguladora de las Bases del Régimen Local, y las funciones públicas que le han sido atribuidas estatutariamente no se rigen por las previsiones de la Ley 39/2015, de 1 de octubre.

- La disposición adicional primera "Medidas de seguridad en el ámbito del sector público" de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dispone lo siguiente en su punto 2: "*Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como* ***impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado***."

[7] Así se encuentra recogido en la *guía CCN-STIC-830 Ámbito de Aplicación del Esquema Nacional de Seguridad*, del Centro Criptológico Nacional.

Considerando que la EMT en su Registro de Actividades del Tratamiento incluye un total de 28 tratamientos de datos personales relativos a 13 de los 14 procesos de negocio identificados por la empresa, podemos inferir que el cumplimiento de la disposición adicional primera, y por consiguiente **el deber de impulsar la implementación de medidas equivalentes al ENS, es de aplicación a la totalidad de materias, procesos y sistemas de la EMT**.

- La Sindicatura considera que la implementación de las medidas de seguridad recogidas en el ENS constituye un requisito fundamental del control interno de las entidades públicas, dado que su implementación supone de facto la implantación efectiva de un Sistema de Gestión de la Seguridad de la Información (SGSI) equivalente al impulsado por la norma UNE-EN ISO/IEC 27001.

Por las razones expuestas, la adecuación al ENS ha sido incluida en el presente trabajo como parte fundamental para la valoración del nivel de madurez del control interno, así como el cumplimiento del deber de impulsar un grado de implementación de medidas equivalentes al ENS en la EMT por parte de los órganos superiores de la EMT.

Las GPF-OCEX 5313, GPF-OCEX 5330 y el Esquema Nacional de Seguridad

La presente auditoría está basada en las Guías prácticas de fiscalización ***GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad*** y ***GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica*****,** aprobadas por la Conferencia de Presidentes de los Órganos de Control Externo (OCEX) el 12/11/2018, que forman 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 esas guías.

El contenido de ambas guías, 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.

Los controles generales de TI incluyen los CBCS y abarcan, de manera general, la totalidad de los requisitos contemplados en el ENS. Los controles generales de TI se clasifican de la siguiente manera:

Cuadro 2. Los controles generales de tecnologías de la información y el ENS

Controles Generales de TI		Medidas de seguridad del ENS
A. Marco organizativo	**A.1 Cumplimiento de legalidad (CBCS 8)**	org.1
	A.2 Estrategia de seguridad	org.2
	A.3 Organización y personal de TI	
	A.4 Marco normativo y procedimental de seguridad	mp.per
B. Gestión de cambios en aplicaciones y sistemas	B.1 Adquisición de aplicaciones y sistemas	
	B.2 Desarrollo de aplicaciones	mp.sw.1 y 2
	B.3 Gestión de cambios	op.exp.5
C. Operaciones de los sistemas de información	**C.1 Inventario de hardware (CBCS 1)**	op.exp.1
	C.1 Inventario de software (CBCS 2)	op.exp.1 y 2
	C.2 Gestión de vulnerabilidades (CBCS 3)	op.exp.3 y 4
	C.3 Configuraciones seguras (CBCS 5)	op.exp.2 y 3
	C.4 Registro de la actividad de los usuarios (CBCS 6)	op.exp.8 y 10
	C.5 Servicios externos	op.ext.1 y 2
	C.6 Protección frente a malware	op.exp.6
	C.7 Protección de las instalaciones e infraestructuras	mp.if
	C.8 - Gestión de incidentes	op.exp.7 y 9
	C.9 Monitorización	
D. Controles de acceso a datos y programas	**D.1 Uso controlado de privilegios administrativos (CBCS 4)**	op.acc.4
	D.2 Mecanismos de identificación y autenticación	op.acc.1 y 5
	D.3 Gestión de derechos de acceso	op.acc.4
	D.4 Gestión de usuarios	op.acc
	D.5 Protección de las redes y comunicaciones	mp.com
E. Continuidad del servicio	**E.1 Copias de seguridad de datos y sistemas (CBCS 7)**	mp.info.9
	E.2 Plan de continuidad	op.cont.2 y 3
	E.3 Alta disponibilidad	mp.if.9

La auditoría de las 15 áreas señaladas en negrita en el cuadro anterior ha incluido la revisión de 53 subcontroles o controles detallados.

Criterios de auditoría: los controles básicos de ciberseguridad, los controles generales de TI y sus subcontroles

Los CBCS y los controles generales de TI son controles globales formados por varios subcontroles detallados. Todas nuestras comprobaciones tienen por finalidad contrastar su situación real en la entidad con las buenas prácticas recogidas en las GPF-OCEX 5313 y

5330, en las que se especifica con el máximo detalle los aspectos comprobados en cada control.

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

Evaluación de los resultados del trabajo

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

Subcontroles

Los CBCS y los controles generales de TI 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 3. Evaluación de los subcontroles

Evaluación	Descripción
Control efectivo	Cubre al 100% con el objetivo de control y: - 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: - 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: - Se sigue un procedimiento, aunque éste 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: - 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 controles

Para determinar la situación global de cada control de ciberseguridad hemos utilizado el modelo de nivel de madurez de los procesos de control de acuerdo con lo establecido en las *GPF-OCEX 5313 y GPF-OCEX 5330*, que a su vez están basadas en la *Guía de seguridad CCN-STIC 804* del CCN, usando una escala, según se resume en el siguiente cuadro.

Cuadro 4. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El control no está siendo aplicado en este momento.
N1 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 tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.*
N2 Repetible, pero intuitivo	50	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas. 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. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.*
N3 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 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).* *El éxito es algo más que buena suerte: se merece.* *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 sí se gestiona en el nivel 3.*
N4 Gestionado y medible	90	La dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere. *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.* *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.*

Nivel	Índice	Descripción
N5 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, utilizándose como indicadores en la gestión de la mejora de los procesos.* *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.*

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 control 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.

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.

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 éstos 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 son[8]:

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 considerados a los efectos del ENS 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%.

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 y controles generales de TI, ya que permiten llevar a cabo tanto un resumen del estado de las medidas de seguridad de los entes auditados a los efectos del ENS, como de los CBCS y controles generales:

- El índice de madurez sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de controles de ciberseguridad.

- 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.

Fechas de la auditoría

Los trabajos de auditoría se iniciaron en junio de 2020 y finalizaron en noviembre de 2020. Consideramos como fin del trabajo de campo la fecha en la que los hallazgos de la auditoría, las conclusiones y el borrador previo del informe son discutidos con los responsables de la entidad auditada, de acuerdo con lo establecido en nuestro Manual de

[8] 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.

fiscalización, ya que hasta entonces es admitida cualquier evidencia adicional disponible. Por tanto, el informe con carácter general refleja la situación en ese momento, ya que es frecuente que, desde que se inicia el trabajo de campo, determinadas deficiencias observadas y señaladas a los gestores sean subsanadas y consideradas de esta forma en las conclusiones y en los indicadores.

Finalmente, el informe es sometido al procedimiento contradictorio de manera formal mediante el trámite de alegaciones.

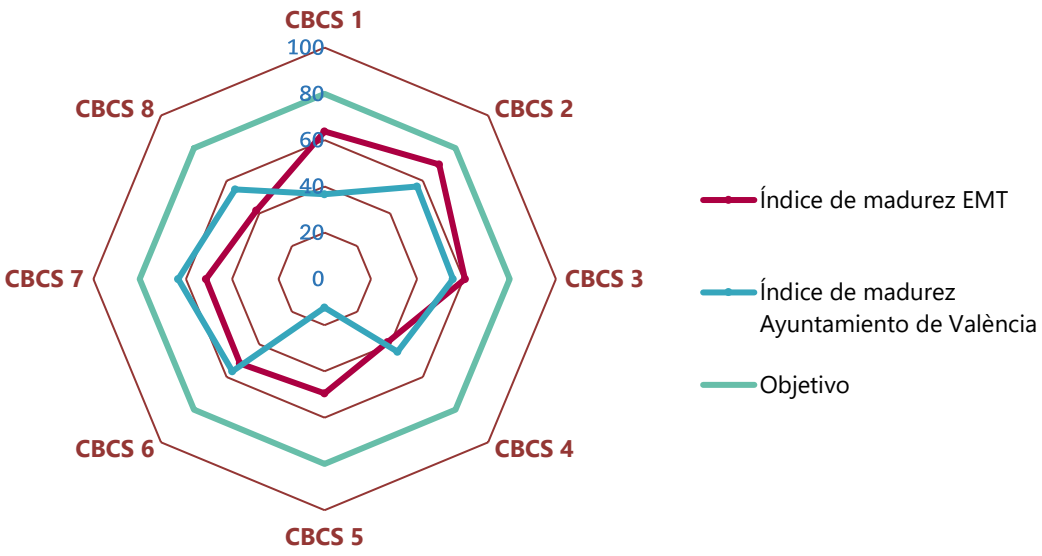
APÉNDICE 2
Situación observada de los controles

A continuación, se señalan los principales aspectos surgidos en la revisión de los controles de ciberseguridad de la EMT. 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 de la EMT para que puedan adoptar las medidas correctoras que consideren precisas. En este apéndice los resultados se muestran de forma sintética.

1. Situación comparativa de los CBCS

Para realizar un análisis comparativo en términos homogéneos de la situación de los controles de ciberseguridad de la EMT con su entidad matriz, hemos considerado el subconjunto de los CBCS, del total de controles de seguridad que hemos revisado en la presente auditoría, que coinciden con los que revisamos en el Ayuntamiento de València, cuyo informe[9] fue publicado en marzo de 2020. El siguiente gráfico 3 presenta los resultados comparados obtenidos en la revisión de los CBCS en ambas entidades.

Gráfico 3. Comparativa del Índice de madurez de los controles básicos de ciberseguridad de la EMT y del Ayuntamiento de València



El índice medio de madurez de los CBCS ha sido del 53,4% en la EMT y del 47,5% en el Ayuntamiento de València; en ambos casos la situación de los controles de ciberseguridad es claramente mejorable y no puede considerarse que los sistemas de información estén debidamente protegidos.

[9] Ver Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València. Ejercicio 2019.

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

Hemos verificado que la EMT realiza acciones para el inventario y control de activos físicos de la entidad, garantizando un control efectivo sobre ellos. La responsabilidad del inventariado de dispositivos se encuentra establecida en el Área de Desarrollo, con el soporte de un proveedor externo. No obstante, el proceso no ha sido detallado en un procedimiento formalmente aprobado.

La EMT dispone de un inventario de gestión automatizada para la administración de los activos, que incluye todos los elementos *hardware* propiedad de la entidad: servidores, equipos de usuarios, dispositivos de red, teléfonos móviles, monitores, impresoras, etc. Sin embargo, los dispositivos de red se introducen en el inventario de forma manual, no automatizada.

Las máquinas virtuales no se incluyen en dicho inventario ni tampoco se encuentran inventariadas por ningún otro sistema. Dicha carencia puede limitar la posterior aplicación de otros controles de seguridad relevantes sobre los dispositivos no controlados.

Por otra parte, si bien no se dispone de un sistema que impida la conexión de dispositivos físicos no autorizados a la red, sí se dispone de diferentes controles compensatorios robustos que detectan, impiden o limitan la actividad de los dispositivos físicos no autorizados en el sistema de información.

En síntesis, existe cierto nivel de control sobre el inventario de dispositivos físicos y la valoración global del control alcanza un índice de madurez del 63,8%, 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.

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

Hemos analizado la gestión que realiza la EMT sobre el inventario y control de *software* y hemos verificado que, aunque la responsabilidad del inventariado de *software* se encuentra establecido en la Política de Seguridad vigente mediante el requisito de mantener un inventario de activos, el proceso implantado no ha sido detallado en un procedimiento formalmente aprobado.

La EMT dispone de un inventario de gestión automatizada para la administración de los activos, entre los que se incluye el *software* gestionado por el Área de Desarrollo. El inventario incluye, entre otra información, el *software* instalado en los dispositivos de la entidad, la versión, el número de licencias disponibles y número de licencias instaladas.

Por otra parte, se ha evidenciado la existencia de un reducido número de equipos con sistemas operativos fuera del periodo de soporte del fabricante, así como servidores y equipos de usuario, hecho que supone un riesgo para los sistemas de información.

La gestión del licenciamiento y el mantenimiento de aplicaciones se realiza mediante un proceso adecuado, pero no formalizado.

La entidad cuenta con medidas orientadas a impedir el uso de *software* no autorizado que pueden considerarse completamente efectivas, además de disponer de un proceso de autorización para la instalación y uso de nuevo *software*.

Consideramos que existe cierto nivel de control sobre el inventario y el *software* autorizado, pero hay posibilidades de mejora. La valoración global del control alcanza un índice de madurez del 70,0%, 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.

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

Hemos analizado la gestión de vulnerabilidades realizada por la EMT y hemos observado que se realizan diferentes acciones con el objeto de identificar y remediar vulnerabilidades. A pesar de que dichas acciones se han implantado de manera efectiva en todos los sistemas, no han sido formalmente documentadas y aprobadas.

La identificación de vulnerabilidades se realiza sobre todos los sistemas que hemos revisado, mediante la realización de ejercicios de *hacking* ético por parte de terceros gracias a contratos de mantenimiento, a través de herramientas que permiten la identificación automática de vulnerabilidades y mediante suscripción a listas de difusión de fabricantes y organismos de referencia.

El proceso de priorización y resolución, aunque parcialmente efectivo, se gestiona de manera informal, debido a que no se encuentra recogido en un procedimiento, ni se utilizan herramientas específicas de priorización de vulnerabilidades o herramienta de *workflow*.

Sobre la aplicación de parches y actualizaciones de seguridad, estos se aplican de modo sistemático sobre aquellos sistemas adquiridos a proveedores y cuya actualización se establece en los contratos de mantenimiento con terceros. Se dispone de herramientas que permiten la gestión centralizada de actualizaciones y parches de seguridad de los sistemas Windows y de los elementos de la electrónica de red.

Consideramos que existe cierto nivel de control, pero hay posibilidades de mejora. La valoración global del control alcanza un índice de madurez del 60,7%, 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.

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

Hemos analizado las acciones que realiza la EMT para el control de las cuentas de administración y hemos verificado que no existe un control efectivo y fiable.

La gestión de la asignación de privilegios administrativos en los sistemas revisados se realiza con distinto grado de efectividad dependiendo del sistema y de manera independiente para cada uno de ellos, dado que no ha sido formalmente aprobado ni implantado un procedimiento que establezca las políticas comunes de gestión de privilegios administrativos para el conjunto de sistemas de la EMT. La gestión de privilegios administrativos se realiza por parte del Área de Desarrollo, excepto para determinadas aplicaciones de los sistemas descentralizados, que son directamente administrados por los responsables de los departamentos afectados y que soportan procesos críticos de la entidad,

Se ha detectado el uso de cuentas no nominativas compartidas en algunos de los sistemas revisados, lo que dificulta la trazabilidad de las acciones en caso de incidentes. Dicha deficiencia se encuentra parcialmente compensada por un adecuado inventariado y control en el uso de las cuentas.

Se han identificado como deficiencias graves de control la inadecuada aplicación del principio de mínimo privilegio en aplicaciones descentralizadas que soportan procesos críticos de negocio, la configuración incorrecta de las cuentas de administración de los servicios de mantenimiento externos de determinados sistemas revisados y un insuficiente control en la definición y gestión de los mecanismos de autenticación utilizados por los sistemas.

Únicamente se hace una correcta aplicación del uso dedicado de cuentas de administración en sistemas gestionados por el Área de Desarrollo.

El registro de la actividad de los usuarios administradores tampoco se encuentra correctamente configurado en los sistemas descentralizados, lo que representa una grave deficiencia de control que dificulta la gestión en caso de incidente de seguridad. Para el resto de los sistemas revisados, gestionados por el área de Desarrollo, si bien no existe un proceso sistemático para realizar una configuración específica y homogénea de los registros de actividad de los administradores, estos registros se encuentran activados y son almacenados y gestionados.

Consideramos que existe un deficiente nivel de control sobre las cuentas de usuarios administradores, por lo que se deberán dedicar esfuerzos y recursos para mejorarlo. La valoración global de este control alcanza un índice de madurez del 38,6%, 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.

6. Sobre el control de acceso a datos y programas (D2, D3, D4)

Hemos analizado las acciones de la organización para el control de los accesos de las cuentas de usuario sobre los sistemas que soportan los procesos de contabilidad e ingresos y hemos verificado que no existe un control totalmente efectivo.

La responsabilidad de la gestión de usuarios, sus privilegios y el control de los accesos a los sistemas, se encuentra parcialmente establecida en la Política de Seguridad aprobada. No obstante, esta no ha sido desarrollada en un procedimiento que detalle las acciones necesarias.

Los mecanismos utilizados para la identificación y autenticación de usuarios pueden considerarse efectivos o parcialmente efectivos en ambos sistemas. No obstante, se han identificado claras oportunidades de mejora con un coste de implantación reducido, particularmente en el proceso de autenticación de la aplicación contable. El proceso de identificación y autenticación de la aplicación de ingresos ha sido recientemente rediseñado permitiendo *Single Sign-On* con el Directorio Activo, proporcionando mayores niveles de automatización para el usuario y compensando parcialmente algunas de las carencias y oportunidades de mejora identificadas.

La gestión de usuarios es adecuada o parcialmente adecuada en ambos sistemas. Hemos verificado que en la aplicación contable únicamente se encuentran habilitadas las cuentas de aquellos usuarios que por sus funciones deben hacer uso de la herramienta y que ha sido implantado un proceso de gestión de usuarios de manera informal pero efectiva.

En el caso del sistema que soporta los ingresos, hemos identificado que no existe un proceso de gestión y revisión de usuarios locales al sistema, hecho que supone una deficiencia de control significativa. No obstante, la implantación de *Single Sign-On* con el Directorio Activo y de medidas de limitación de acceso en la electrónica de seguridad red, compensan parcial o totalmente los riesgos derivados de la deficiencia detectada.

La gestión de derechos de acceso no alcanza los niveles de control adecuados, particularmente para la aplicación contable. Hemos evidenciado que en dicho sistema no se ha aplicado adecuadamente el criterio de mínimo privilegio en el ejercicio de provisión de derechos de acceso a los usuarios, siendo esta una deficiencia de control que consideramos significativa. Hemos evidenciado que se encuentra en curso una modificación de los perfiles de determinados usuarios para adecuar sus privilegios a los requerimientos de sus puestos de trabajo. Durante la fase de alegaciones, se nos ha informado de la existencia de una propuesta y plan de trabajo para hacer extensiva esta modificación a todos los usuarios del sistema. Hemos verificado la documentación que soporta la existencia de dicho plan de trabajo y que esta iniciativa se encuentra en fase de implantación al emitir el presente informe.

En el caso de la aplicación de ingresos, únicamente dispone de limitados mecanismos para la adecuación de los derechos de acceso a los puestos de trabajo de los usuarios. No obstante, hemos verificado que, en la medida de las capacidades del sistema, sí se ha

realizado una correcta aplicación del criterio de mínima funcionalidad en la gestión de derechos de acceso a los usuarios.

En síntesis, existe un deficiente nivel de control sobre el acceso de los usuarios a datos y programas y la valoración global del control alcanza un índice de madurez del 38,0%, 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.

7. 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 verificado que no existe un procedimiento formalmente aprobado a tal efecto. La entidad realiza acciones para aplicar una configuración de seguridad en determinados sistemas, pero dichas acciones no son suficientes para asegurar la efectividad del control.

Aunque se ha evidenciado que se dispone de plantillas para la configuración de determinados dispositivos, dichas plantillas no tienen carácter de bastionado ni la seguridad por defecto es el objeto de las mismas.

La entidad dispone de un entorno de preproducción utilizado en el proceso de gestión de cambios y para la realización de pruebas de seguridad en determinados sistemas.

Sobre la monitorización de las configuraciones existentes, se ha establecido un control parcialmente efectivo sobre los equipos de usuario de la entidad mediante el uso combinado de dos de las herramientas de seguridad implantadas.

Existe, por tanto, un insuficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deberán dedicar esfuerzos y recursos para mejorarla. La valoración global del control alcanza un índice de madurez del 49,5%, 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.

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

Hemos analizado los procedimientos aplicados por la EMT para el registro de la actividad de los usuarios en los distintos sistemas y hemos verificado que, aunque se dispone de ciertos controles relacionados con este procedimiento, estos no han sido formalizados y aprobados.

Hemos verificado que el registro de actividad se encuentra activado en la mayor parte de los sistemas revisados, aunque se mantiene la configuración por defecto que define el fabricante.

No obstante, hemos detectado un sistema descentralizado en el que, si bien se dispone de funcionalidades que permiten la activación y almacenamiento de registros de actividad, estas no se encuentran habilitadas. Dicha carencia supone una deficiencia grave

de control, dado que impide la trazabilidad de las acciones de los usuarios y particularmente de aquellos que disponen de privilegios administrativos sobre el sistema.

La EMT dispone de diversos 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 se integran en 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.

Adicionalmente, se dispone de un sistema de seguridad específico que, aunque no puede ser considerado un SIEM[10] por sus especificaciones técnicas y funcionales, sí dispone de capacidades avanzadas de correlación de eventos e inteligencia artificial que le permiten la detección de vulneraciones de seguridad en base al análisis de los datos disponibles.

La valoración de este control alcanza un índice de madurez del 51,8%, 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.

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

La EMT realiza diversas acciones para el control de las copias de seguridad de los datos y sistemas. Sin embargo, los controles implantados no se consideran suficientes para estimar que el proceso resulte completamente efectivo y, adicionalmente, este no se encuentra recogido en un procedimiento documentado y formalmente aprobado.

El control de copias de seguridad se encuentra completamente delegado en un proveedor externo. La solución implantada dispone de las características técnicas adecuadas para un proceso de realización de copias de seguridad acorde con las necesidades de la organización. No obstante, hemos verificado que el pliego de prescripciones técnicas no detalla los requisitos de seguridad ni especifica todos los aspectos necesarios para asegurar la correcta provisión del servicio. Del mismo modo, la supervisión por parte de la EMT del proveedor externo y de los servicios recibidos no resulta adecuada, dado que no se realiza un seguimiento de los niveles de servicio mediante indicadores acordados.

Las políticas de copias de seguridad aplicadas a los sistemas ubicados en el Centro de Procesamiento de Datos (CPD) de la EMT han sido desarrolladas por el proveedor externo sin la realización de un análisis previo que identifique las necesidades de los diferentes servicios, situación que puede resultar en la aplicación de un conjunto de políticas de copia que no satisfaga completamente las necesidades de la organización.

[10] Sistema de gestión de información y eventos de seguridad.

Se ha confirmado que no se realizan de forma sistemática pruebas de recuperación planificadas, si bien hemos confirmado que se han llevado a cabo recuperaciones satisfactorias en aquellas ocasiones que se ha requerido.

Con respecto a la protección de las copias de seguridad, hemos verificado que incluye distintos mecanismos efectivos destinados para ello, pero puede resultar recomendable la aplicación de medidas adicionales para aumentar la protección frente a determinados riesgos a los que se encuentran expuestos los sistemas de información, que han sido comunicados a los responsables de la EMT.

La valoración global del control alcanza un índice de madurez del 51,3%, 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.

10. Sobre la formación y concienciación (A3)

Hemos analizado el proceso que sigue la EMT respecto a la formación y concienciación del personal en materia de seguridad de la información y hemos verificado que, aunque se aplican medidas relacionadas con este aspecto, estas no han sido formalmente establecidas mediante un procedimiento documentado y aprobado, ni se incluye la obligación de llevar a cabo este tipo de acciones en la *PSI*.

Las acciones de la EMT relativas a la concienciación en seguridad de la información consisten principalmente en el envío de píldoras informativas (comunicaciones informativas breves) a partir de publicaciones y alertas emitidas desde grupos de interés como INCIBE, CCN-CERT y organizaciones de seguridad reconocidas. Dichos envíos se realizan de manera periódica en un proceso organizado y de manera reactiva ante determinados anuncios y alertas de interés para la organización.

La EMT se encuentra en fase de planificación de un proyecto de formación y concienciación en materia de seguridad de la información, en el que está previsto involucrar de manera práctica a todos los empleados de la entidad. En base a los resultados obtenidos en una primera fase de identificación de vulnerabilidades y deficiencias de carácter humano en las distintas áreas de la organización, se extenderán las actividades de formación en función de las necesidades y carencias identificadas. Dicho proyecto es gestionado de manera conjunta por el Área de Desarrollo y la de Recursos Humanos.

La valoración global de este control alcanza un índice de madurez del 60,0%, 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.

11. Sobre la gestión de cambios (B3)

Hemos analizado las acciones respecto al proceso de gestión de cambios que sigue la EMT y hemos verificado que, a pesar de no disponer de un procedimiento documentado y aprobado formalmente para tal efecto, el control resulta efectivo.

Se ha evidenciado que tanto los cambios requeridos y ejecutados por la propia entidad, como los cambios solicitados por la EMT y ejecutados por proveedores, se registran y gestionan mediante herramientas automatizadas.

Todos los cambios siguen el proceso de registro, evaluación, aprobación, planificación y ejecución, en un proceso de gestión que puede considerarse adecuadamente diseñado y ejecutado.

Para los cambios que así lo requieren, la gestión del cambio incluye una fase de realización de pruebas en entornos de preproducción, entornos que disponen de las mismas medidas de seguridad que los sistemas productivos y en los que se realiza la anonimización de los datos en caso de ser necesario

Al analizar los cambios incluidos en el muestreo, hemos podido observar que, a lo largo del ciclo de vida de los mismos, intervienen diferentes usuarios con distintas responsabilidades, a pesar de que no hayan definido responsables y/o constituido órganos de gestión de manera formal. Del mismo modo, durante la evaluación del cambio se tiene en cuenta la aprobación por parte del solicitante y su implicación en materia de seguridad de la información.

Consideramos que existe cierto nivel de control sobre la gestión de cambios, pero hay posibilidades de mejora. La valoración global de este control alcanza un índice de madurez del 60,2%, 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.

12. Sobre la gestión de servicios externos (C5)

Hemos analizado las acciones realizadas para la gestión de los servicios externos y hemos verificado que no existe un procedimiento formalmente aprobado. La entidad realiza acciones que implican la aplicación de medidas destinadas a tal efecto, pero dichas acciones no son suficientes para asegurar la efectividad del control.

Se ha evidenciado que en los pliegos de contratación de servicios se incluyen cláusulas donde se especifican las características y requisitos del servicio, los acuerdos de nivel de servicio, las responsabilidades de ambas partes, las consecuencias del incumplimiento de los acuerdos y, sumado a ello, los requisitos de confidencialidad y de cumplimiento de la normativa existente en materia de protección de datos personales. No obstante, hemos verificado que en determinados pliegos existe un insuficiente nivel de detalle y no se incluyen los contenidos mínimos imprescindibles, hecho que impide asegurar la provisión de un nivel de servicio que satisfaga las necesidades de la organización.

Por otra parte, para los proveedores que así lo requieren, no se incluye la obligación de que los servicios prestados por los mismos sean conformes al Esquema Nacional de Seguridad y que, además, dispongan de las certificaciones de seguridad correspondientes.

Asimismo, la EMT no ha establecido formalmente un sistema rutinario para medir el cumplimiento de las obligaciones y niveles de servicio por parte de los proveedores que se encuentre basado en los acuerdos formalmente dispuestos y en la medición de dichos niveles de servicio mediante indicadores establecidos.

En conclusión, existe un nivel de control insuficiente sobre los servicios externos y la valoración global del control alcanza un índice de madurez del 49,8%, 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.

13. Sobre la gestión de incidentes (C8)

Hemos analizado las acciones respecto al proceso de gestión de incidentes que sigue la EMT y hemos verificado que, a pesar de no disponer de un procedimiento documentado y aprobado formalmente para tal efecto, se han implantado medidas y se llevan a cabo actuaciones con las que el control resulta parcialmente efectivo, tanto en la detección de eventos como en su gestión y comunicación.

La EMT dispone de diferentes herramientas destinadas a la detección y gestión de eventos e incidentes de seguridad, así como un servicio externo de seguridad gestionada prestado por el Centro de Operaciones de Seguridad (SOC) de un proveedor, proporcionando de manera conjunta un adecuado nivel de control para la detección de eventos.

Como norma general, el responsable del Negociado de Sistemas y Aplicaciones, con el apoyo del equipo de soporte técnico, es el encargado de gestionar los eventos e incidentes ordinarios de seguridad informática.

Para los incidentes que se consideran relevantes, bien por su impacto o bien por requerir actuaciones con carácter de urgencia, se ha constituido un equipo de crisis compuesto por responsables de diferentes Negociados para la toma de decisiones. Aunque dicho comité ha sido utilizado de manera efectiva en determinadas ocasiones, su organización y funcionamiento no se encuentran establecidas en un procedimiento, formal o informal.

Se ha incluido en el proceso de actuación de respuesta al incidente un análisis de la causa raíz, del que se obtiene un informe que incluye tanto los hallazgos identificados durante el análisis como una propuesta de actuaciones y medidas técnicas para evitar futuros ataques similares. Este informe, elaborado para determinados incidentes, se transmite al responsable del sistema afectado y al Director gerente.

Sin embargo, no se lleva a cabo un análisis destinado a la optimización del proceso de gestión de incidentes, así como tampoco se identifican todas las partes interesadas con objeto de comunicarles los hechos acontecidos.

La valoración global de este control alcanza un índice de madurez del 53,1%, 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.

14. Sobre el cumplimiento normativo (CBCS 8)

La entidad no alcanza un satisfactorio nivel de adecuación a la normativa legal, por lo que la valoración global sobre el cumplimiento de los aspectos de legalidad que hemos verificado es que la EMT alcanza un índice de madurez del 41,7%. Esto se corresponde con un nivel de madurez *N1*, que indica que existe una falta de observación generalizada de la normativa.

En relación con el ENS

La EMT no ha realizado acciones específicamente orientadas a alcanzar un grado de implementación de medidas de seguridad equivalentes a los requisitos del Esquema Nacional de Seguridad. No obstante, se encuentra en fase de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la aplicación de la serie UNE-ES ISO/IEC 27000, que contiene las mejores prácticas recomendadas en Seguridad de la información y que resulta en gran medida equivalente al ENS.

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

Aunque no se ha realizado la auditoría del cumplimiento del ENS, sí se han realizado diferentes análisis referidos a la UNE-EN ISO/IEC 27002.

La EMT ha elaborado una *Política de Seguridad de la Información (PSI)*, aprobada por el director del Área de Desarrollo en diciembre de 2018. El contenido de dicha política se adecua parcialmente a los requisitos establecidos por el ENS. Sin embargo:

- La *Política de Seguridad* de la Información debe ser aprobada por el Consejo de Administración, máximo órgano de dirección de EMT, tal como requieren el ENS y la norma UNE-EN ISO/IEC 27001, y no cumple con todos los requisitos establecidos en ambas normas.

- No se han constituido órganos de gobierno de la seguridad que instrumentalicen las responsabilidades respecto a la seguridad de la información, como el Comité de Seguridad de la Información. Ni se ha establecido una organización interna de la seguridad equivalente que establezca un marco de gestión de la seguridad.

- Debe respetarse la segregación de funciones que se establece en el artículo 10 del ENS.

- Existen deficiencias formales en la designación de las personas para los roles definidos en la *Política de Seguridad* de la Información.

  La *PSI* atribuye las funciones de **responsable de seguridad** a dos cargos directivos de la entidad, el responsable de sistemas y la responsable de recursos humanos. Estos cargos no han sido adecuadamente referenciados en el documento, dado que no existen como tales en el organigrama de la organización.

  La asignación de funciones y responsabilidades que asume cada uno de los cargos que conforman el rol no se encuentra detallada y diferenciada en el documento y no se ha producido una aceptación formal por parte las personas sobre las que recae la responsabilidad.

  En esta materia deberían seguirse los criterios establecidos en la *Guía de Seguridad de las TIC CCN-STIC 801 ENS Responsabilidades y funciones*.

Estas carencias limitan el reconocimiento por parte de la organización de las funciones del responsable de seguridad y merman su capacidad operativa, lo que representa un factor de riesgo importante, particularmente en un entorno de sistemas descentralizados en el que el responsable debe velar por la aplicación homogénea de medidas de seguridad en la totalidad de los sistemas de la entidad.

En materia de protección de datos personales

El 1 de junio de 2018 se nombró a la delegada de protección de datos (DPD) de acuerdo con lo previsto en el artículo 37.1 a) del RGPD.

Se ha elaborado el registro de actividades de tratamiento de la información requerida por el RGPD y que incluye el detalle necesario.

Se ha realizado un análisis de riesgos sobre sus tratamientos de datos personales y las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.

Actualmente la entidad se encuentra inmersa en un proyecto de adecuación a esta normativa. En el marco de ejecución del proyecto se dispone de un plan de acción que recoge el seguimiento de las actividades desarrolladas y por desarrollar, partiendo en un análisis diferencial y del análisis de riesgos realizado.

Sin embargo:

- No se ha realizado ninguna auditoría específica en materia de protección de datos.
- El registro de actividades del tratamiento no ha sido publicado ni es accesible por medios electrónicos.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

DPD: Delegado de protección de datos

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de Seguridad de la Información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de Gestión de Seguridad de la Información

SIC: Sistemas de información y comunicaciones

SIEM: Sistema de gestión de información y eventos de seguridad

Ciberamenazas: Eventos con origen en internet que pueden desencadenar un incidente en la organización y producir daños materiales, pérdidas inmateriales en sus activos o la interrupción de un servicio.

Ciberseguridad: Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, así como de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Normas de seguridad: Uniforman el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio y describirán: a) el uso correcto de equipos, servicios e instalaciones, b) lo que se considerará uso indebido y c) la responsabilidad del personal con respecto al cumplimiento o violación de estas normas. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones; como regla general, estará disponible en la intranet corporativa de la entidad a través de una dirección URL. La normativa de seguridad de cada entidad trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y

del desarrollo normativo de la política de seguridad de la entidad en cuestión, en segunda instancia.

Política de seguridad de la información: es un documento de alto nivel que define lo que significa "seguridad de la información" en una organización de acuerdo con el artículo 11 del Real Decreto 3/2010 y articula la gestión continuada de la seguridad. Debe ser aprobada por la junta de gobierno de un ayuntamiento o el consejo de administración de una sociedad. Debe estar accesible para todos los miembros de la organización y redactada de forma sencilla, precisa y comprensible. Conviene que sea breve, y que deje los detalles técnicos para otros documentos más precisos que ayuden a llevar a cabo lo propuesto: normas de seguridad y procedimientos de seguridad.

Procedimientos de seguridad: Abordan tareas concretas, indicando lo que hay que hacer, paso a paso. Detallan de forma clara y precisa: a) cómo llevar a cabo las tareas habituales, b) quién debe hacer cada tarea y c) cómo identificar y reportar comportamientos anómalos.

Sistema de Gestión de Seguridad de la Información: Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos.

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 fiscalización se discutió con los responsables de la Empresa Municipal de Transportes de València, SAU 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 fiscalización correspondiente al ejercicio 2020, el mismo se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Dentro del plazo concedido, la entidad ha formulado las alegaciones que ha considerado pertinentes.

En relación con el contenido de las alegaciones y su tratamiento, es preciso señalar lo siguiente:

1) Todas las alegaciones han sido analizadas detenidamente.

2) Las alegaciones admitidas se han incorporado al contenido del Informe.

El texto de las alegaciones formuladas, así como el informe motivado que se ha emitido sobre las mismas, que han servido de antecedente para su estimación o desestimación por esta Sindicatura, se incorporan en los anexos I y II.

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 15 de enero de 2021, aprobó este informe de fiscalización.

ANEXO I

Alegaciones presentadas

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

C/ Sant Vicent, 4 - 46002
Tel. +34 96 386 93 00
Fax +34 96 386 96 53
sindicom@gva.es
www.sindicom.gva.es

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202003535	FECHA DE ENTRADA 21/12/2020 14:59
ÁREA Fiscalización - Documentación	PROCEDIMIENTO PAA2020/29 Empresa Municipal de Transportes de València, SAU. Auditoría de ciberseguridad
DATOS DEL PRESENTADOR Nombre: ANTONIO MARTINEZ GARCIA DE DIOS NIF / CIF: E-mail: Entidad: EMPRESA MUNICIPAL DE TRANSPORTES, S.A.	
FIRMA DIGITAL DE92E6DC48F4BE16CFE83D0BBE06D83C068E1DFB	
DOCUMENTOS ENVIADOS Fichero1: 53094129D_20201221_20201221_Alegaciones_informe_ciberseguridad_sign.pdf Fichero2: 53094129D_20201221_1b Renovacion de software -plan y presupuesto-.pdf Fichero3: 53094129D_20201221_1c Renovacion de software -plan y presupuesto-.pdf Fichero4: 53094129D_20201221_2 EMT_Actualizacion grado cumplimiento_1 seguridad y RGPD.pdf Fichero5: 53094129D_20201221_3a Proyecto Concienciacion y formacion.pdf Fichero6: 53094129D_20201221_3b Proyecto concienciacion y formacion.pdf	

Pl. Correo Viejo, 5 - 46001 València
Tel.: 96 315 85 00 - Fax 96 392 49 98 - www.emtvalencia.es

EMT VALÈNCIA

INFORME DE LA EMPRESA A LA AUDITORIA DE CIBERSEGURIDAD DEL EJERCICIO 2020 DE LA SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA.

Habiendo realizado la sindicatura de comptes de la Comunitat Valenciana durante los meses de junio a septiembre de 2020 una auditoría de ciberseguridad de los sistemas de EMT València en el presente ejercicio, la entidad, mediante el presente escrito de alegaciones y actuaciones relevantes, formula las precisiones que considera oportunas respecto de este informe provisional de conclusiones emitido por la sindicatura.

A) ALEGACIONES

Apartado 4 del informe de sindicatura: Conclusiones.

1. Bajo índice de madurez de los controles de ciberseguridad.

Al respecto de esta conclusión, añadir que, como se indica en apartado de hitos y se ha podido constatar durante la realización de la auditoría de la sindicatura , el trabajo y las inversiones necesarias para la adecuación al ENS, se ha realizado en pocos años, consiguiendo en ese corto periodo de tiempo un cambio muy significativo del estado de madurez, desde una madurez muy baja N1 hasta el nivel actual (similar o superior al de los resultados de los 15 ayuntamientos de municipios de mayor población de la comunidad valenciana).

Esta evolución también se constata en las revisiones realizadas por la consultora independiente EY y de las que se ha dejado constancia durante la auditoría, ya que su estudio inicial se inicia durante el año 2018 y se revisa a finales de 2019 y principios de 2020 (pasando de un índice de madurez de 1,20, medido según la escala de la norma ISO 27002 donde 1 es el nivel más bajo y 5 el más alto, hasta 2,46 y siendo que el nivel necesario para EMT debe ser superior a 3).

Adicionalmente, destacar que la peor puntuación obtenida se corresponde con el área D " Controles de acceso a datos y programas" y que, en todo caso, los peores resultados se dan en sistemas descentralizados (software o sistemas propietarios no gestionados directamente por la entidad sino por terceras empresas), siendo el resultado de estos mismos controles para los sistemas centralizados de EMT muy superior, tanto a nivel de cuentas, roles y accesos de usuarios como de privilegios y gestión de cuentas de administradores de sistemas).

Por último, indicar, que sobre esos sistemas descentralizados ya se está trabajando con los proveedores durante el año 2020 para conseguir un nivel de madurez adecuado que se pueda constatar en las siguientes revisiones.

2. Se requiere mayor concienciación y más recursos dedicados a la seguridad de la información

Aun cuando se coincide con esta conclusión y con que el compromiso debe ser global en la organización, indicar que entre el 2015 y el 2020 la inversión en materia de seguridad y sistemas ha sido de 2.139.485,14 euros. De esa cifra, el 90% de las partidas se han configurado o licitado desde el año 2018.
El detalle de todas estas inversiones y su efecto sobre el incremento del nivel de madurez y seguridad de la entidad se puede apreciar en el presente informe, en el apartado de hitos de los últimos años.

3. Insuficiente gobernanza de la seguridad de la información

El ENS no especifica que órgano o puesto directivo en concreto tiene la potestad para aprobar la política de seguridad y el nombramiento de los distintos roles o configuración del comité de seguridad. Por tanto, la rotunda afirmación del informe de la sindicatura de comptes en este punto de sus conclusiones en que determina que debe ser el Consejo de Administración el que apruebe la Política de Seguridad de la Información de la compañía, causa a EMT cierta inseguridad, ya que no cita norma legal alguna para amparar tal conclusión. En el caso de la política de seguridad actual de EMT, ha sido redactada según los estándares de la norma ISO 27000 por el director de negociado de sistemas y aprobada por el director del área de desenvolupament, estando además publicada en el portal del empleado y siendo, por tanto, accesible a todas las personas trabajadoras de EMT València
En cualquier caso, EMT cuenta con una política de seguridad en vigor, como se aprecia en la auditoría, que se completará con las propuestas indicadas en la misma. También especifica esta política que el cargo de responsable de seguridad recae en el director del negociado de sistemas, aun cuando la voluntad de la empresa es contratar a un especialista en seguridad y redes que pueda asumir formalmente el cargo y encargarse con mayor detalle del control y la evolución de las políticas de seguridad. Este proceso de contratación se ha iniciado ya durante el año 2020, con un primer proceso de promoción interna, que se ha considerado desierto al no haber recibido solicitudes y continuará externamente en las próximas semanas tras el visto bueno del Ayuntamiento de València a los pliegos del proceso de contratación.
Por último, puntualizar que EMT tiene un procedimiento no escrito pero replicable por el cual, en el caso de posibles incidentes de seguridad se conforma un comité de crisis formado por, al menos, la dirección gerencia y adjunta a gerencia de EMT, la dirección jurídica, la dirección del área de desenvolupament y sistemas y la dirección de comunicación. Tanto en la denuncia presentada como en las distintas declaraciones en actos legales y en la comisión de investigación interna, existen pruebas de la creación de este comité en el caso un incidente que supuestamente podría haber afectado a la seguridad de EMT durante el mes de septiembre del año 2019 de manera inmediata a su descubrimiento.

4. La situación de los controles de acceso privilegiado debe ser mejorada

Tal y como ya se alegaba en la primera recomendación y deja de manifiesto de manera clara esta conclusión, las principales debilidades encontradas se centran en software descentralizado propiedad de proveedores externos y no gestionado directamente por el equipo de sistemas de EMT.
En el caso de los sistemas centralizados y gestionados por el equipo de sistemas, el nivel de madurez es bueno y ha mejorado notablemente en los últimos años gracias a las inversiones y evoluciones realizadas. En este grupo se encuentran las aplicaciones y bases de datos propias que gestionan la recaudación de ingresos y ventas, control de validaciones, indicadores de oferta y demanda, regulación y gestión de la flota, etc. Es decir, los sistemas críticos para la entidad.
Las debilidades encontradas en los sistemas descentralizados serán subsanadas en el corto plazo junto a los proveedores propietarios. Existe ya una propuesta de trabajo compartida y presupuestos para la realización del correspondiente informe de motivación de inversión y su puesta en marcha.

5. Insuficiente grado de adecuación a la normativa de ciberseguridad
Entendemos que la primera parte de esta conclusión redunda en el resultado de las anteriores ya alegadas.
Sin embargo, en cuanto a la adecuación al RGPD de la entidad, se ha de considerar que tras la auditoría de 2018 en esta materia durante el año 2019 y 2020 se han completado los siguientes hitos necesarios legalmente:

1. Actualización interna de procesos y formularios a las nuevas necesidades RGPD.

2. Control y actualización de inventario.

3. Creación del puesto de Delegada de Protección de Datos y gestión a través de herramienta trazable y segura de todas las peticiones y validaciones.

4. Creación del Comité RGPD (una persona responsable por área o equipo) para el seguimiento de estado, incidencias o nuevas medidas.

Sobre este aspecto también existen pruebas formales de los controles realizados por la consultora independiente EY, contratada para el proceso de adecuación al reglamento, de los cuales se ha dejado constancia en la presente auditoría.
Por otro lado, el objeto y la dedicación, controles u obtención de pruebas de la presente auditoría no ha sido la revisión de todos los aspectos del Reglamento General de Protección de Datos, por lo que entendemos que no se puede concluir que no hay una suficiente adecuación sin haberlo realizado en profundidad.

Apartado 5 del informe de sindicatura: Recomendaciones.

Pl. Correo Viejo, 5 - 46001 València
Tel.: 96 315 85 00 - Fax 96 392 49 98 - www.emtvalencia.es

1. Sobre el inventario y control de dispositivos físicos
EMT actualmente está trabajando en un SGSI completo que incluye un protocolo para este aspecto concreto de control.
En todo caso, actualmente EMT tiene el sistema contratado y configurado, un antígena que detecta de forma autónoma y combate amenazas cibernéticas emergentes en toda la empresa protegiendo de la misma forma redes corporativas, entornos virtuales y en la nube, IoT (Internet de las cosas) y sistemas de control, capaz de monitorizar toda la actividad de la red y los dispositivos conectados, navegación y estado o vulnerabilidades.
De esa forma, la red de dispositivos físicos se encuentra perfectamente monitorizada y se detectan posibles amenazas en tiempo real.

2. Sobre el inventario y control de software autorizado.
En todos los dispositivos de usuario de EMT existen privilegios de administrador que impiden la ejecución de software (sea o no autorizado) por parte de las personas usuarias. En caso de necesitar su ejecución, la necesidad debería ser reportada al equipo de soporte por escrito a través de la herramienta de ticketing y sólo se aprobaría tras la supervisión del responsable de sistemas. Adicionalmente controlamos el software instalado en los dispositivos mediante .
Durante el año 2020, la empresa ha contratado licencias de equipos de usuario y servidores de , un sistema de protección IA de última generación y residente en la nube con tecnología de protección para endpoints y, que, además cuenta con un módulo, , que revisa los programas y aplicaciones instalados detectando posibles vulnerabilidades de manera autónoma y proponiendo las actualizaciones y parcheos necesarios de manera automática. Es por tanto una herramienta innovadora que permite, por un lado, detectar y evitar la ejecución de software malicioso y, por otro, mantener actualizados todas las aplicaciones necesarias.

3. Sobre el proceso continuo de identificación y remediación de vulnerabilidades De manera similar al punto anterior, constatar que mientras se aprueba el protocolo específico, la inversión en sistemas de protección IA líderes garantiza un elevado nivel de escaneo y prevención de vulnerabilidades de manera autónoma, con avisos y actuaciones en tiempo real.

4, 5 y 7. Al respecto de las debilidades de acceso y privilegios detectadas en el software contable
Como se ha indicado este sistema descentralizado mantenido por un proveedor externo se encuentra ahora mismo en proceso de reversión de las debilidades de acceso.

Pl. Correo Viejo, 5 - 46001 València
Tel.: 96 315 85 00 - Fax 96 392 49 98 - www.emtvalencia.es

10. Sobre la copia de seguridad de datos y sistemas

Actualmente existe un proceso escrito para este proceso dentro del SGSI en desarrollo que está pendiente de formalización por aprobación. Adicionalmente resaltar que durante 2020 se ha puesto en marcha un sistema de respaldo de copias completo y redundante en el depósito sur situado en Sant Isidro y que los datos almacenados por los usuarios y áreas para el trabajo diario y colaborativo se encuentra almacenados en el cloud de Azure desde la implantación y configuración en marzo de 2020 de sharepoint de Microsoft.

11. Sobre la formación y concienciación

EMT es consciente de la importancia de los planes de formación y concienciación en seguridad. En este sentido, durante el mes de noviembre se ha iniciado una primera prueba piloto de ataques de phishing simulados a cuentas directivas y de personas usuarias de todas las áreas. Con esa información, se ha redactado un informe de motivación para la contratación de un servicio de ataques y formación de un año de duración que permitirá entender el estado de la entidad y formar en función de las debilidades encontradas durante el año 2021. Se adjunta dicho informe en proceso.
Por último, el equipo de sistemas envía periódicamente dos newsletters a todos los componentes de EMT (SistemesInfo y SistemesAlertes) con las que se forma y alerta de posibles peligros a las personas trabajadoras de la entidad, pruebas que ya se aportaron en la auditoría

12. Sobre la gestión del cambio

Actualmente existe un proceso escrito para este proceso dentro del SGSI en desarrollo que está pendiente de su aprobación para poder ser formalizado.

13. Sobre la gestión de servicios externos

A pesar de no existir un procedimiento para la gestión de los servicios externos, en todos los pliegos de condiciones se especifica todos los pasos desde la motivación de la contratación y el servicio hasta las características, requisitos, acuerdos, revisiones, sanciones, confidencialidad y todos los elementos necesarios para contratar, hacer seguimiento y controlar o sancionar la actividad. Al respecto de esta cuestión se han podido revisar varios ejemplos durante la realización de la auditoría como el servicio de soporte de incidencias y mantenimiento que actualmente ofrece la empresa Eltec o el de desarrollo de Oracle Forms y reports que actualmente está adjudicado a la empresa Alfatec.

15 y 16. Sobre el cumplimiento de la legalidad

Para estos puntos concretos, nos remitimos a las alegaciones ya realizadas en el punto 4 de conclusiones acerca de la política de seguridad y la adaptación al reglamento general de protección de datos.

Pl. Correo Viejo, 5 - 46001 València
Tel.: 96 315 85 00 - Fax 96 392 49 98 - www.emtvalencia.es

B)**RESUMEN DE HITOS EN MATERIA DE SEGURIDAD Y SISTEMAS HASTA EL AÑO 2020.**

I: Posición de partida y recursos invertidos en los últimos años

1. Introducción

Desde el año 2018, la seguridad de los sistemas y, en concreto, los riesgos derivados de la ciberseguridad, se han considerado aspectos estratégicos y prioritarios para la compañía. Así consta en los planes de trabajo de dirección por objetivos y se puede demostrar con el volumen de recursos destinados y los avances realizados. Sin embargo, la situación de inicio era muy pobre y aunque la evolución es muy positiva en muy poco tiempo, para EMT era imposible estar al nivel de madurez requerido por la ENS (80%). Aun así, como se hace constar en el informe, se ha situado a la empresa al nivel de los grandes ayuntamientos de la comunidad.

En el presente informe, se analizan y detallan las inversiones, nuevas herramientas de trabajo y mejora de procesos o sistemas realizadas en el área de seguridad informática en los últimos años. El objetivo es que se recoja en la fase de alegaciones el esfuerzo realizado en poco tiempo y los grandes avances conseguidos, así como para poner en valor la importancia de elevar el nivel de inversiones, presupuesto y recursos humanos y materiales necesarios para alcanzar el objetivo marcado en el ENS. El análisis se realiza sobre 4 ejes:

a. Organización y recursos humanos en el área de sistemas
b. Seguridad en comunicaciones e infraestructura
c. Mejoras de organización y gestión de procesos
d. Actualización RGPD

2. Organización y recursos humanos en el área de sistemas

Tras el análisis interno realizado por dirección y gerencia y las conclusiones derivadas de la consultoría de la empresa EY sobre seguridad (sobre la base de

controles de la norma ISO 27002) y adaptación a RGPD, se llegan a las siguientes conclusiones:

1. El área de IT no tiene una segregación clara de funciones o roles, asumiéndose los proyectos en función de la carga de trabajo de las distintas personas y no atendiendo a criterios de especialización o formación.

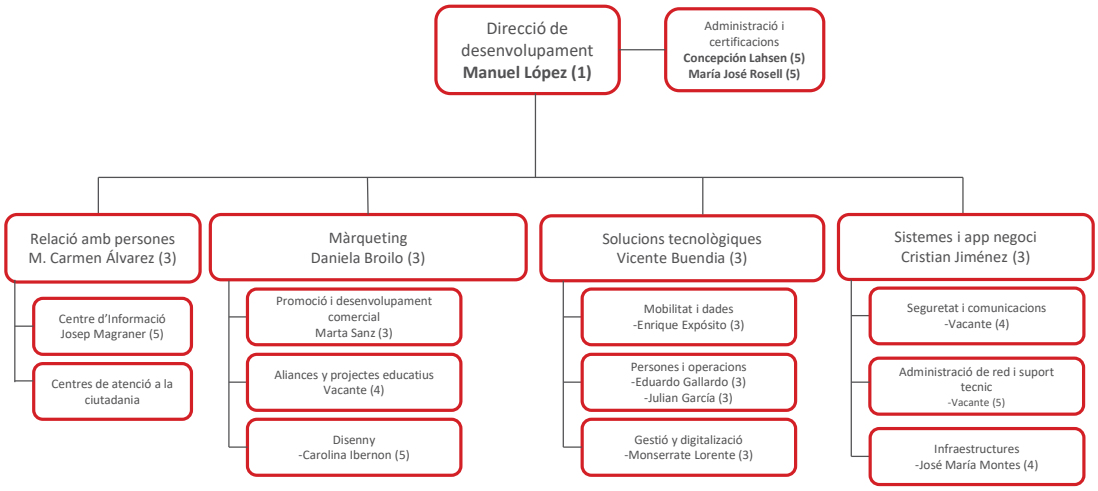
2. La vertiente de seguridad no había sido relevante a nivel organizativo. Los perfiles del área eran de gestores de proyectos, ingeniería y soluciones y no existían perfiles especializados o formados en aspectos de seguridad.

3. El nombramiento de responsable de seguridad era asumido por la dirección del área, algo poco ortodoxo y poco operativo.

Tras este análisis y el estudio de los distintos perfiles y formaciones, se decide cambiar la organización del equipo, generándose 2 direcciones de negociado diferentes: soluciones y desarrollos tecnológicos y sistemas.

En el equipo de sistemas se integraron los dos perfiles con mayor formación en este campo y, ambos, con formaciones y masters específicos en seguridad y ciberseguridad, además, dentro de la política de seguridad se indica que el puesto de responsable de seguridad sólo recaerá en el director de sistemas en funciones hasta la incorporación de un perfil específico para ello.

Adicionalmente, se aprobó reforzar el equipo con dos perfiles adicionales con conocimiento específico de comunicaciones, redes y seguridad. Tras lanzar la promoción interna y declararse desierta, estas plazas van a salir a concurrencia pública en las próximas semanas. Destacar, por tanto, que todo este trabajo en la vertiente de sistemas y seguridad se ha realizado con recursos humanos escasos para la estructura que se entiende óptima para acometer los proyectos.



3. Resumen general de inversiones realizadas y resultados obtenidos

Desde el año 2015 hasta el año 2020 se han invertido 2.139.485,14€ sin tener en cuenta el coste de gestión y desarrollo interno, de los cuales un 90% se han realizado desde el año 2018

a. Seguridad en comunicaciones e infraestructura: 1.314.283,54€

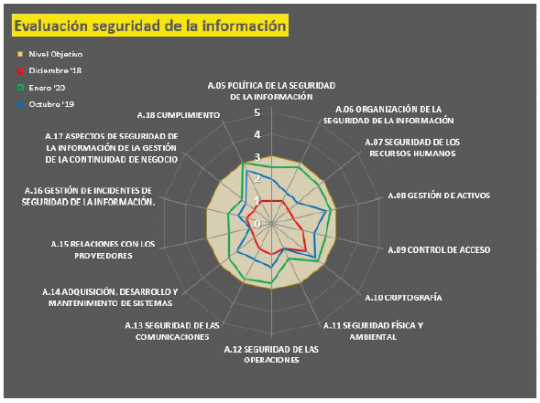
b. Mejoras de organización y gestión de procesos: 779.571,60€

c. Actualización RGPD: 45.630€

Tras este trabajo, el resumen final de la evolución entre 2018 y enero de 2020, queda certificado por la revisión realizada por la consultora independiente EY según los criterios de la norma ISO 27001 (documentación completa que se aportó y revisó durante el proceso de auditoría):

3. Evolución grado de cumplimiento.
Grado de cumplimiento en ciberseguridad.

- Se ha definido un marco de controles que converge los controles de seguridad del ENS e ISO 27002.
- El siguiente gráfico muestra la evolución del nivel de cumplimiento en materia de ciberseguridad de EMT Valencia.



	Dominio	Nivel de Madurez Dic '18	Oct '19	Ene'20	Obj.
A.05	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	1,00	2,00	2,50	3,00
A.06	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1,14	1,50	2,80	3,00
A.07	SEGURIDAD DE LOS RECURSOS HUMANOS	1,00	1,50	2,70	3,00
A.08	GESTIÓN DE ACTIVOS	1,00	2,50	2,75	3,00
A.09	CONTROL DE ACCESO	1,46	2,00	2,50	3,00
A.10	CRIPTOGRAFÍA	2,00	2,50	2,70	3,00
A.11	SEGURIDAD FÍSICA Y AMBIENTAL	1,27	1,27	1,77	3,00
A.12	SEGURIDAD DE LAS OPERACIONES	1,42	2,00	2,70	3,00
A.13	SEGURIDAD DE LAS COMUNICACIONES	1,29	1,79	2,80	3,00
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,00	2,00	2,50	3,00
A.15	RELACIONES CON LOS PROVEEDORES	1,00	1,00	2,00	3,00
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	1,14	1,54	2,04	3,00
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	1,00	1,50	1,70	3,00
A.18	CUMPLIMIENTO	1,13	2,60	3,00	3,00
		1,20	1,84	2,46	3,00

Fruto de ese trabajo, también se ha definido el plan de actuaciones a corto, medio y largo plazo en materia de ciberseguridad, guía que hemos seguido desde entonces para priorizar las acciones en esta materia:

QUICKWINS Acciones inmediatas (0 – 12 meses)	
QW.01	Definición de la política y cuerpo normativo de la Seguridad IT.
QW.02	Definición y aplicación de una política de contraseñas robusta sobre todos los SSII de EMT Valencia.
QW.03	Formalización de la Función de Seguridad de la Información: misión y objetivos, ámbito y organización.
QW.04	Definición e implantación de un proceso de gestión de alertas e incidentes de Seguridad de la Información.
QW.05	Definición e implantación de un proceso de gestión de parches y actualizaciones de seguridad IT.
QW.06	Tests de ingeniería social (Phishing, USB, etc).
QW.07	Encuesta de satisfacción y entendimiento del nivel de concienciación en Seguridad de la Información.
QW.08	Definición de un plan anual de formación y concienciación en materia de Seguridad IT.
QW.09	Definición e implantación de un procedimiento de análisis y gestión de riesgos.
QW.10	Definición e implantación de un procedimiento de revisión de usuarios en los sistemas de información críticos.
QW.11	Definición e implantación de un procedimiento de gestión del teletrabajo.

CORTO PLAZO 12 – 24 meses	
CP.01	Plan anual de auditorías y revisiones técnicas de Seguridad de la Información.
CP.02	Definición e implantación de la política de clasificación de la información.
CP.03	Diseño de solución para la de gestión de activos de información.
CP.04	Definición e implantación de un Plan de Continuidad de Negocio.
CP.05	Creación de un equipo de respuesta ante incidentes de Seguridad IT.
CP.06	Definición de un proceso para incluir el área de Seguridad de la Información en la operación diaria de los procesos y proyectos IT.
CP.07	Definición de la política de contratación, instalación e implementación de servidores y aplicaciones y la gestión de proyectos involucrando al area TIC.
CP.08	Implantación de una herramienta de gestión de dispositivos móviles (MDM) o securizar la conexión a los SSII de EMT a través de dispositivos móviles.
CP.09	Evaluación de amenzas en materia de Seguridad Física y diseño de solución para mitigar las amenazas.
CP.10	Definición e implantación de un Sistema de Gestión de Seguridad de la Información (SGSI).
CP.11	Cifrado de dispositivos y soportes extraíbles.

MEDIO PLAZO 24 meses – 36 meses	
MP.01	Definición e implantación del nuevo modelo de arquitectura de red segura.
MP.02	Bastionado de sistemas y dispositivos informáticos.
MP.03	Definición e implantación de un modelo de reporting y cuadro de mandos integral para la función de Seguridad.
MP.04	Definición e implantación de un proceso de desarrollo seguro (S-SDLC).
MP.05	Definición e implantación de un programa de gestión de identidades y accesos (IAM).
MP.06	Análisis de escenarios de riesgo y definición de un Programa de Prevención de Fugas de Información.
MP.07	Definición de marco de gestión y control de proveedores y modelo de monitorización de medidas de seguridad en servicios TI.
MP.08	Implantación de herramienta de protección de información sensible en BBDD.
MP.09	Cifrado de comunicaciones.
MP.10	Implantación de una solución para evitar el uso de credenciales definidas en claro en el código en aplicaciones o scripts.

LARGO PLAZO 36 meses – 50 meses	
LP.01	Firma digital y cifrado de correo electrónico (interno y externo).
LP.02	Implantación de herramienta para prevención de fuga de información a través del correo electrónico
LP.03	Implantación de una solución o servicio de Cyberthreat Intelligence.
LP.04	Implantación de una solución o servicio de análisis forense y cibercrimen.
LP.05	Revisión y actualización del plan anual de auditorías de Seguridad de la Información.
LP.06	Revisión y actualización de materiales de soporte del Plan Anual de formación y concienciación
LP.07	Revisión y actualización de las campañas de concientización de Seguridad de la Información.
LP.08	Revisión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
LP.09	Revisión y mantenimiento del Plan de Continuidad de Negocio (BCP).
LP.10	Implantación de una herramienta de gestión de vulnerabilidades (SIEM), mecanismos e inteligencia para la detección de incidentes de Seguridad IT.

4. Seguridad en comunicaciones e infraestructura

Renovación completa de toda la infraestructura de protección, comunicaciones y trabajo ofimático, así como de servidores, base de datos corporativa y el software de protección.

Destacar:

-Renovación de todos los equipos ofimáticos de personas usuarias, servidores y equipos corporativos. Actualización de todos los sistemas operativos de equipos de usuarios y servidores (hasta 2018 una parte importante de ellos tenían licencias ya sin mantenimiento, por ejemplo, una parte importante de los equipos de usuarios tenían instalado Windows 95 o XP).

-Renovación y migración del servidor y cliente del correo. La versión que se usaba hasta 2018 era Lotus Notes del año 2007, con evidentes debilidades demostradas en las auditorias de seguridad que se han realizado por EY. Esta migración se realiza en dos fases, en primer lugar a un servidor físico y con el cliente . Además, durante el año 2020 se ha configurado y puesto en marcha al completo un sistema completo de trabajo corporativo colaborativo y almacenamiento en la nube en Azure (office 365 y Sharepoint)

-Instalación y actualización periódica de los dispositivos y reglas de seguridad perimetral. En este caso, también se realiza en dos fases. En una primera, durante 2018 se instala y configura un clúster completo de

seguridad redundante: para la seguridad perimetral, para el correo y para el análisis de logs. En una segunda, durante el año 2020 se renueva el antivirus corporativo por el sistema , un sistema de protección IA de última generación y residente en la nube con tecnología de protección para endpoints y, que, además cuenta con un módulo, , que revisa los programas y aplicaciones instalados detectando posibles vulnerabilidades de manera autónoma y proponiendo las actualizaciones y parcheos necesarios. Por último, también en 2020, se contrata el sistema , un antígena que detecta de forma autónoma y combate amenazas cibernéticas emergentes en toda la empresa protegiendo de la misma forma redes corporativas, entornos virtuales y en la nube, IoT (Internet de las cosas) y sistemas de control, capaz de monitorizar toda la actividad de la red y los dispositivos conectados.

-Se actualizan y migran los servidores de BBDD a la última versión de Oracle 12 (con importantes mejoras de seguridad y control comparadas con la versión 9 del año 2001) y los servidores de virtualización .

-Renovación del sistema de copias de seguridad ( ) y puesta en marcha de un sistema redundante al principal (situado en las oficinas centrales de EMT), en las instalaciones del depósito de Sant Isidre. Hasta el año 2018 existía una sola infraestructura en las oficinas centrales basada en cinta y con necesidad de manipulación manual diaria.

-Puesta en marcha del SSO entre el directorio activo y CTI (base de datos y aplicaciones de ingresos). Hasta el año 2019, existían usuarios nominativos sin renovación de contraseñas ni logs de actividad.

-Por último, durante el año 2020 se ha licitado y adjudicado la renovación de las comunicaciones corporativas en 4 lotes:

1. Para el recableado completo de las sedes corporativas y la renovación de las instalaciones eléctricas y el sistema SAI. Proyecto ya iniciado y que se prevé terminar en el primer trimestre de 2021.

2. Para la renovación de toda la electrónica de red y su gestión a través de una plataforma integrada, así como el mantenimiento y actualizaciones necesarias.

3. Renovación del contrato de voz y datos, la infraestructura de comunicaciones móviles y fija y de la centralita en la nube.

4. Renovación del servicio de red corporativa multiservicio.

EMT VALÈNCIA

5. Mejoras en gestión de procesos

En la vertiente organizativa y de procesos, también se han realizado importantes inversiones y cambios o actualizaciones desde el año 2015. Para ello se han analizado los informes de las auditorias anuales, la auditoria sobre RGPD y seguridad para ISO 27001 y los recursos con que contaba la empresa, así como las tendencias y necesidades para el plan estratégico y de desarrollo en este ámbito.

Destaca:

-Implantación de herramientas y procesos para dejar absoluta trazabilidad y poder hacer un seguimiento más pormenorizado tanto de las incidencias y averías, como de los proyectos y desarrollos (gestores de proyectos y ticketing y).

-Se ha contratado un nuevo software de gestión de personal y hardware de control de presencia que está en funcionamiento desde enero de 2019 y permite implementar nuevas medidas de seguridad y control de la información y los procesos, así como trazabilidad en las operaciones y desarrollos.

-Se ha mejorado el servicio de alojamiento del portal web, incorporando una monitorización 24/7 de funcionamiento y seguridad (la empresa adjudicataria cumple con la norma ISO 27001 y los compromisos del ENS).

-Se ha comenzado el proyecto para finalizar un sistema de protocolos SGSI completo. Actualmente, una vez detectados y esbozados todos los documentos necesarios para cumplir con la norma ISO 27000, existe un protocolo trabajado para los principales aspectos (Política de seguridad, Gestión de usuarios, Gestión de accesos, Gestión de cambios, Política de copias de seguridad, Política de actuación en incidentes de seguridad y uso de móviles y teletrabajo), el siguiente objetivo es aprobar las grandes líneas y el compromiso necesario en el consejo de administración.

6. Actualización RGPD e inicio de certificación ISO 27001

Durante el año 2018 y 2019 se ha realizado una auditoría completa de la empresa en el ámbito de la protección de datos y la certificación ISO 27001 de seguridad informática.

Pl. Correo Viejo, 5 - 46001 València
Tel.: 96 315 85 00 - Fax 96 392 49 98 - www.emtvalencia.es

Resultado de este proceso, destacar:

5. Actualización interna de procesos y formularios a las nuevas necesidades RGPD

6. Creación del puesto de Delegada de Protección de Datos y gestión a través de herramienta trazable y segura de todas las peticiones y validaciones.

7. Creación del Comité RGPD (una persona responsable por área o equipo) para el seguimiento de estado, incidencias o nuevas medidas.

II: Actuación sobre sistemas descentralizados

Tras el análisis realizado con el equipo de revisión de la Sindicatura de Comptes, se ha iniciado un proyecto con el proveedor del software para mejorar las principales debilidades detectadas. En este sentido, existe ya un plan de trabajo con el proveedor y una oferta de servicio con las siguientes partidas:

-Contratación licencia módulo de auditoria: 3.375€/año

-Mejoras de seguridad y procesos (roles de menú, password, etc): 1.833,50€

Actualmente el expediente de gasto está en proceso de informe de motivación y EMT se compromete a poner en marcha todas las medidas antes de febrero de 2021. Se adjunta el plan de trabajo pactado con el proveedor y los presupuestos como prueba de trabajo en curso.

LOPEZ FUENTES, MANUEL ANGEL (FIRMA)
Firmado digitalmente por LOPEZ FUENTES, MANUEL ANGEL (FIRMA)
Fecha: 2020.12.21 12:15:39 +01'00'

SERRANO BALBUENA MARTA ELIA - 05677626F
Firmado digitalmente por SERRANO BALBUENA MARTA ELIA - 05677626F
Fecha: 2020.12.21 14:19:39 +01'00'

ANEXO II

Informe sobre las alegaciones presentadas

ANÁLISIS DE LAS ALEGACIONES EFECTUADAS POR LA EMPRESA MUNICIPAL DE TRANSPORTES DE VALÈNCIA, SAU, AL BORRADOR DEL INFORME DE AUDITORÍA DE CIBERSEGURIDAD DEL EJERCICIO 2020

Mediante el escrito de esta Sindicatura de 3 de diciembre de 2020 se remitió a la Empresa Municipal de Transportes de València, SAU (EMT) el borrador del Informe de auditoría, para que efectuase las alegaciones que considerase oportunas. Con fecha 21 de diciembre de 2020 se recibieron por el registro electrónico las alegaciones formuladas[1] y respecto a estas se señala lo siguiente:

Primera alegación

Apartado 4, "Conclusiones", del borrador del Informe, primer subapartado: "Bajo índice de madurez de los controles de ciberseguridad"

Comentarios

En la alegación se indica que EMT ha conseguido en un corto periodo de tiempo un cambio muy significativo del estado de madurez de la ciberseguridad. El escrito de alegaciones contiene un apartado "B) RESUMEN DE HITOS EN MATERIA DE SEGURIDAD Y SISTEMAS HASTA EL AÑO 2020" para corroborar dicha afirmación. En síntesis, se alega que durante los últimos años:

- Se han realizado trabajos de auditoría por parte de consultoras externas que muestran, durante los últimos dos años, una notable mejora en los niveles de seguridad de todas las áreas analizadas.

- Se han realizado relevantes inversiones en materia de seguridad, particularmente en los últimos dos años.

- Se ha iniciado la implantación de un SGSI, cuya documentación soporte se encuentra en estado de elaboración o revisión.

- Se han implantado mejoras en los sistemas y soluciones tecnológicas de seguridad de comprobada eficacia, algunas de las cuales durante la propia realización del trabajo y como parte del plan de actuaciones existente.

En la realización de la auditoría hemos podido comprobar que se habían realizado mejoras en los controles de ciberseguridad respecto de la situación precedente y que había diversas iniciativas en marcha para continuar en esa línea. En las valoraciones del nivel de madurez de los controles hemos tenido en cuenta todas las mejoras ya implantadas y en funcionamiento en el momento de nuestra revisión, pero no estaba

[1] Las alegaciones recibidas se acompañan en el anexo 1. Por razones de seguridad se ha eliminado la referencia concreta a algún elemento de seguridad en el documento adjunto, por esa razón aparece algún espacio en blanco.

dentro de los objetivos del trabajo realizar un análisis comparativo con la situación existente hace dos años, que por la información aportada en la alegación era claramente peor.

Además hemos constatado que, en el marco general de mejora de la seguridad, gran parte de las recomendaciones emitidas en el Informe se encuentran en fase de implantación o están siendo planificadas, bien como consecuencia del presente trabajo, bien como parte del plan de actuaciones existente.

En este sentido se valora positivamente la disposición de la Dirección para mejorar los controles del sistema de información y comunicaciones de la EMT y atender las recomendaciones efectuadas, cuyo diseño y eficacia operativa podrán ser evaluados en un posterior informe de seguimiento a realizar por la Sindicatura.

Dado que en esta y otras alegaciones se alude a que EMT está en un proceso de mejora del sistema de seguridad y de las deficiencias identificadas, se añade un párrafo al final del apartado de recomendaciones para recoger, con carácter general, dicha circunstancia.

Consecuencias en el Informe

Añadir, al final del apartado 5, "Recomendaciones", un párrafo con la siguiente redacción:

"Durante la fase de alegaciones la Dirección de EMT ha enfatizado en el proceso de mejora del sistema de seguridad de la información emprendido por la entidad durante los dos ejercicios anteriores y en su intención de atender las recomendaciones realizadas. En las valoraciones del nivel de madurez de los controles hemos tenido en cuenta solo las mejoras ya implantadas y en funcionamiento en el momento de nuestra revisión, existiendo otras iniciativas en marcha, en fase de planificación o de implantación, para atender buena parte de las recomendaciones que hemos realizado, cuyo diseño y eficacia operativa podrán ser evaluadas en un posterior informe de seguimiento."

Segunda alegación

Apartado 4, "Conclusiones", del borrador del Informe, segundo subapartado: "Se requiere mayor concienciación y más recursos dedicados a la seguridad de la información"

Comentarios

La EMT señala que entre el 2015 y el 2020 la inversión en materia de seguridad y sistemas ha sido de 2.139.485,14 euros y que el 90% de las partidas se han configurado o licitado desde el año 2018, lo que ha permitido incrementar el nivel de madurez y seguridad de la entidad. No obstante, en la alegación se indica que "se coincide con esta conclusión".

Aunque se han aumentado las inversiones en la materia, se partía de un punto muy bajo y todavía hay mucho recorrido de mejora.

Véanse comentarios en la alegación anterior.

Consecuencias en el Informe

Se mantiene la redacción del Informe.

Tercera alegación

Apartado 4, "Conclusiones", del borrador del Informe, tercer subapartado: "Insuficiente gobernanza de la seguridad de la información"

Comentarios

En relación con lo alegado en el primer párrafo: "El ENS no especifica qué órgano o puesto directivo en concreto tiene la potestad para aprobar la política de seguridad y el nombramiento de los distintos roles o configuración del comité de seguridad", consideramos que un documento de políticas de seguridad de la información (PSI) debe ser aprobado al máximo nivel jerárquico. En el presente caso está aprobado por un director de área, lo que no tiene mucha lógica y plantea dudas razonables sobre la capacidad para exigir el cumplimiento de la PSI al establecer responsabilidades y compromisos para el Comité ejecutivo de EMT, que está en una posición jerárquica superior a la persona que aprueba la PSI.

Según el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la PSI debe ser aprobada por "el titular del órgano superior correspondiente" y "se considerarán órganos superiores los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local".

Y el apartado 3.1, "Política de seguridad [org.1]", del ENS señala:

"La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.

b) El marco legal y regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

d) **La estructura del comité o los comités para la gestión y coordinación de la seguridad**, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso."

Por otra parte, la guía de seguridad de las TIC *CCN-STIC-805 Política de Seguridad de la Información* establece que: "23. La Política de Seguridad de la Información es un documento que será aprobado formalmente por la alta dirección de la organización y tendrá carácter imperativo sobre toda la organización".

A su vez, la guía de seguridad de las TIC *CCN-STIC-801 Responsabilidades y funciones en el ENS* abunda en el mismo criterio y señala: "25. Así pues, la figura de la Dirección de la entidad (personificada en su titular) cobra una importancia capital: de la Dirección depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento".

Además, el órgano que apruebe la PSI debe ser aquel entre cuyas competencias se encuentre la determinación y asignación presupuestaria del organismo, circunstancia lógica, a la vista de que el cumplimiento del ENS supone, en la mayoría de los casos, la debida asignación de recursos que requiere su implantación.

Desde el punto de vista de las normas ISO 27001/27002, dado el contenido que debe tener una PSI/SGSI, solo el máximo órgano de la EMT tiene atribuciones para ello (véase apartado 2 del Informe). La UNE-EN ISO/IEC 27001 establece en su apartado 5, "Liderazgo", que "la alta dirección debe establecer una política de seguridad de la información". En ese mismo sentido se manifiesta la UNE-EN ISO/IEC 27002: "Las organizaciones deberían definir una política de seguridad de la información al máximo nivel que sea aprobada por la dirección y establezca el enfoque de la organización para gestionar sus objetivos de seguridad de la información".

Finalmente, es importante destacar que la conclusión objeto de la alegación, aunque tiene un componente de cumplimiento de la normativa en materia de seguridad de la información, se refiere fundamentalmente al cumplimiento de los controles en materia de ciberseguridad, que es un área crítica del sistema de control interno de la EMT. Por tanto, debemos comparar la situación en este punto concreto, no solo con lo previsto por la normativa aplicable, sino por las mejores prácticas en materia de control interno. Desde ambos puntos de vista consideramos que el "órgano superior correspondiente" o la "alta dirección" es el Consejo de Administración, si bien podría ser discutible que fuera el presidente o el director gerente, pero no consideramos razonable que sea un puesto directivo de inferior rango jerárquico a los anteriores.

En relación con los comentarios de la alegación referentes a la figura del responsable de seguridad, se acepta parcialmente la alegación y se reconsidera y matiza la redacción del Informe.

Finalmente, respecto del último párrafo de la alegación, solo cabe señalar que un "comité de crisis" no se corresponde con la figura de un Comité de Gestión de la Seguridad de la Información que se menciona en el Informe.

Consecuencias en el Informe

Se matiza la redacción quedando la conclusión (apartado 4 del Informe) alegada así:

"**Insuficiente gobernanza de la seguridad de la información**

La EMT dispone de una *Política de seguridad de la información* (PSI), que **no ha sido aprobada por el Consejo de Administración**, máximo órgano de dirección de EMT, tal como requieren el ENS y la norma UNE-EN ISO/IEC 27001/27002, ni cumple con todos los requisitos establecidos en ambas normas.

La gestión de la seguridad de los sistemas de información requiere establecer una organización de la seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte y los mecanismos de coordinación y resolución de conflictos, designando un **Comité de Gestión de la Seguridad de la Información**, de forma que la gobernanza de la seguridad de la información esté adecuadamente estructurada.

La PSI que apruebe el Consejo de Administración debe recoger con claridad las responsabilidades sobre la gestión, administración y seguridad de los sistemas descentralizados (aquellos gestionados de manera autónoma por los departamentos), ya que la actual PSI no refleja fielmente las particularidades del modelo organizativo de la entidad. La administración de sistemas de información, que de manera general se realiza por parte del Área de Desarrollo, es asumida en determinados casos por los propios departamentos de la entidad, que administran las aplicaciones específicas que soportan los procesos críticos de sus departamentos. Esta situación no resulta recomendable, ya que dificulta la capacidad operativa del responsable de seguridad como figura que debe velar por la aplicación homogénea de medidas de seguridad en el conjunto de los sistemas de la entidad y su coherencia en un entorno de sistemas administrados por distintos departamentos. Además, existe un elevado riesgo de que los departamentos carezcan de las competencias profesionales requeridas para la administración de sistemas y de que los intereses departamentales no se encuentren alineados con los principios de la seguridad de la información aprobados por la organización."

Cuarta alegación

Apartado 4, "Conclusiones", del borrador del Informe, cuarto subapartado: "La situación de los controles de acceso privilegiado debe ser mejorada"

Comentarios

La EMT especifica que las principales debilidades encontradas están en los sistemas descentralizados gestionados por proveedores externos y que serán subsanadas en el corto plazo. Del mismo modo se indica que existe una propuesta de trabajo y presupuesto para su ejecución. Se adjunta la propuesta en las alegaciones recibidas.

Hemos verificado la existencia de la propuesta y plan de trabajo, que incluye las modificaciones necesarias en cuanto a la gestión adecuada de derechos de acceso y privilegios administrativos de los usuarios y la aplicación adecuada del principio de mínimo privilegio.

Véanse también comentarios a la primera alegación.

Consecuencias en el Informe

Añadir un tercer párrafo en el subapartado "La situación de los controles de acceso privilegiado debe ser mejorada", del apartado 4, "Conclusiones", con la siguiente redacción:

"Durante el trámite de alegaciones la EMT nos ha informado de la existencia de una propuesta de trabajo para la resolución de estas deficiencias. Hemos verificado la existencia de dicha propuesta y del plan de trabajo, que incluye las modificaciones necesarias en cuanto a la gestión adecuada de derechos de acceso y privilegios administrativos de los usuarios, registros de actividad y aplicación adecuada del principio de mínimo privilegio. Al emitir el presente informe esas acciones estaban en fase de implantación."

El párrafo 6, en el apartado 6 ("Sobre el control de acceso de datos y programas") del apéndice 2, queda redactado así:

"La gestión de derechos de acceso no alcanza los niveles de control adecuados, particularmente para la aplicación contable. Hemos evidenciado que en dicho sistema no se ha aplicado adecuadamente el criterio de mínimo privilegio en el ejercicio de provisión de derechos de acceso a los usuarios, siendo esta una deficiencia de control que consideramos significativa. Hemos evidenciado que se encuentra en curso una modificación de los perfiles de determinados usuarios para adecuar sus privilegios a los requerimientos de sus puestos de trabajo. Durante la fase de alegaciones, se nos ha informado de la existencia de una propuesta y plan de trabajo para hacer extensiva esta modificación a todos los usuarios del sistema. Hemos verificado la documentación que soporta la existencia de dicho plan de trabajo y que esta iniciativa se encuentra en fase de implantación al emitir el presente informe."

Quinta alegación

Apartado 4, "Conclusiones", del borrador del Informe, quinto subapartado: "Insuficiente grado de adecuación a la normativa de ciberseguridad"

Comentarios

La EMT señala, en síntesis, que durante los años 2019 y 2020 se han completado hitos legalmente requeridos en el marco de adecuación al RGPD y que, dado que en el presente trabajo no se han analizado todos los aspectos del RGDP, no se puede concluir que no hay una suficiente adecuación.

La valoración respecto a la adecuación a la normativa de ciberseguridad incluida en el apartado de conclusiones no hace referencia expresa a las carencias concretas

identificadas, sino a la responsabilidad de impulsar medidas equivalentes al Esquema Nacional de Seguridad, incluyendo los tratamientos de datos personales.

La valoración del cumplimiento normativo, detallado en el apéndice 2, apartado 14, se ha realizado de manera diferenciada para la adecuación al ENS y a la normativa de protección de datos. En dicho apartado se especifican carencias relevantes relativas a la adecuación al ENS que son las que han tenido efecto negativo al cuantificar el índice de madurez del CBCS 8.

Consecuencias en el Informe

Se matiza la redacción del apartado 4, "Conclusiones", quinto subapartado, quedando así:

"La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel insatisfactorio de adecuación a la normativa de ciberseguridad. El Ayuntamiento de València y el Consejo de Administración de la EMT tienen la responsabilidad de impulsar un grado de implementación de medidas equivalentes al Esquema Nacional de Seguridad, en el marco del cumplimiento de la normativa en materia de protección de datos, y deben promover las acciones necesarias para subsanar esa situación."

Sexta alegación

Apartado 5, recomendación nº 1 del borrador del Informe

Comentarios

Confirma lo señalado en el Informe.

Consecuencias en el Informe

No se modifica.

Séptima alegación

Apartado 5, 2ª recomendación del borrador del Informe

Comentarios

Confirma lo señalado en el Informe.

Consecuencias en el Informe

No se modifica.

Octava alegación

Apartado 5, 3ª recomendación del borrador del Informe

Comentarios

Confirma lo señalado en el Informe.

Consecuencias en el Informe

No se modifica.

Novena alegación

Apartado 5, recomendaciones 4, 5 y 7 del borrador del Informe

Comentarios

La alegación es análoga a la cuarta alegación y las consecuencias en el Informe propuestas en aquella son válidas para la presente.

Consecuencias en el Informe

No se modifican las recomendaciones.

Décima alegación

Apartado 5, recomendación nº 10 del borrador del Informe

Comentarios

La EMT resalta la puesta en marcha del nuevo sistema de respaldo durante 2020. En el trabajo realizado hemos verificado y valorado la calidad técnica de la solución implantada, que efectivamente dispone de las características adecuadas para satisfacer las necesidades de la organización.

No obstante, se han evidenciado determinadas carencias desde el punto de vista de la gestión y medición de los niveles de servicio que limitan la madurez del control que deben ser subsanadas.

Consecuencias en el Informe

No se modifica.

Undécima alegación

Apartado 5, recomendación nº 11 del borrador del Informe

Comentarios

Confirma lo señalado en el Informe.

Consecuencias en el Informe

No se modifica.

Duodécima alegación

Apartado 5, recomendación nº 12 del borrador del Informe

Comentarios

Confirma lo señalado en el Informe.

Consecuencias en el Informe

No se modifica.

Decimotercera alegación

Apartado 5, recomendación nº 13 del borrador del Informe

Comentarios

La EMT señala la inclusión en los pliegos del detalle necesario para llevar a cabo una adecuada gestión de los servicios. Si bien hemos verificado la inclusión de dichos contenidos en algunos casos, también hemos observado que en otros pliegos no están correctamente incorporados. Del mismo modo, las acciones emprendidas para la medición del cumplimiento de las obligaciones y niveles de servicio no forman parte de un proceso rutinario ni se han establecido formalmente indicadores.

Se constata por consiguiente que, si bien el control puede ser aplicado de manera eficaz, no se encuentra asegurada su aplicación en todos los casos, limitando el nivel de madurez.

Consecuencias en el Informe

No se modifica.

Decimocuarta alegación

Apartado 5, recomendaciones nº 15 y 16 del borrador del Informe

Comentarios

Nos remitimos a la alegación nº 5.

Consecuencias en el Informe

No se modifica.

Alegaciones sexta a decimocuarta

Como se ha señalado en la primera alegación, en el escrito de alegaciones se alude a que EMT está en un proceso de mejora del sistema de seguridad y de las deficiencias identificadas, por ello se añade un párrafo al final del apartado de recomendaciones para recoger, con carácter general, dicha circunstancia.