BANCO DE INNOVACIÓN EN LAS ADMINISTRACIONES PÚBLICAS

TÍTULO

La Sindicatura de Comptes recibe el Premio FIASEP a las buenas prácticas por sus auditorías de ciberseguridad

INFORMACIÓN INICIAL:

PROBLEMA: Existe una necesidad, planteada en los Congresos Nacionales de Auditoría Pública, de un centro estable especializado en la promoción de la auditoría en el sector público que se preocupara por la mejora de la formación y los procedimientos de trabajo de los auditores que actúan en el ámbito de la ciberseguridad.

SOLUCIÓN GLOBAL: Puesta en marcha de una auditoría de controles básicos de ciberseguridad en los ayuntamientos con mayor población de la Comunitat Valenciana.

COSTE APROXIMADO: Los informes llevados a cabo por la Unidad de Auditoría de Sistemas de Información (UASI) se han realizado dentro del marco presupuestado por la Sindicatura de Comptes de la Comunitat Valenciana. En cuanto a los diferentes costes de las recomendaciones a implementar en materia de ciberseguridad por parte de los ayuntamientos, en el informe se detallan diferentes tablas descriptivas de los mismos (https://www.sindicom.gva.es/public/Attachment/2020/7/inf-cbcs-informe-global-05-definitivo_para_publicar-2020-07-20_signed.pdf).

TERRITORIO:

Ayuntamientos de más de 50 000 habitantes de la Comunidad Valenciana.

PÚBLICO DESTINATARIO:

Ciudadanía en general y administraciones públicas locales de los quince ayuntamientos con más población de la Comunidad Valenciana.

ENTIDAD QUE LA HA LLEVADO A CABO:

Unidad de Auditoría de Sistemas de Información (UASI) de la Sindicatura de Comptes de la Comunitat

Valenciana.

DESCRIPCIÓN DE LA POLÍTICA O PROGRAMA:

Considerando que las entidades locales no son ajenas a la problemática planteada por la ciberseguridad, y su cercanía a los ciudadanos, el Consell de la Sindicatura de Comptes acordó incluir en los programas anuales de actuación de 2019 y 2020 la realización de un informe sobre los controles básicos de ciberseguridad (CBCS) de los quince mayores ayuntamientos de la Comunitat Valenciana para evaluar su preparación frente a la actual situación de crecientes ciberamenazas.

Las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, representan la consolidación desde el punto de vista jurídico de la administración electrónica en todas las entidades públicas, y establecen que la tramitación electrónica debe constituir la actuación habitual de las Administraciones, tanto en las relaciones con terceros, como entre Administraciones e intraadministraciones, estableciendo el principio de "digital por defecto".

Como consecuencia de la aplicación de dichas leyes, todas las entidades locales están inmersas en procesos de transformación en la forma de prestación de los servicios a los ciudadanos y de la gestión pública, para un pleno despliegue de la administración electrónica sustentada en sistemas de información cada vez más complejos tecnológicamente e interconectados a través de internet.

Los riesgos para los sistemas de información que soportan los procesos de la administración electrónica aumentan a medida que las amenazas a la seguridad provenientes del ciberespacio evolucionan continuamente y aparecen ataques nuevos cada vez más sofisticados y destructivos que obligan a los entes públicos a hacerles frente de forma proactiva y sistemática, estableciendo mecanismos de defensa que en su fundamento están articulados mediante el Esquema Nacional de Seguridad, de aplicación obligatoria para todo el sector público.

Los actuales sistemas de información son más complejos y están más interconectados que nunca, pero una mayor interconexión origina mayores riesgos de ciberseguridad, ocasiona una mayor probabilidad de que se produzca una perturbación significativa en los sistemas de información de las entidades locales debida a un

ciberataque y, en consecuencia, una interrupción en los servicios prestados a los ciudadanos. Por esta razón, es imperativo que los responsables de los entes públicos gestionen los riesgos asociados con el funcionamiento y uso de sistemas de información que utilizan para desarrollar y prestar los servicios públicos.

En el escenario general descrito, la realidad de nuestro entorno cercano y del resto de la sociedad española y mundial en el momento de elaborar este informe es la de una crisis sanitaria y socioeconómica sin precedentes provocada por la epidemia de COVID-19. Entre otras muchas cuestiones, esta crisis ha puesto de manifiesto que las administraciones públicas han sido capaces de mantener gran parte de su actividad confiando en el buen funcionamiento y la eficacia de los sistemas de información y comunicaciones (SIC). Obligados por el confinamiento decretado por el Gobierno de la nación para hacer frente a la epidemia, todas las administraciones han recurrido al trabajo en remoto, en sus distintas modalidades técnicas, para mantener su actividad en niveles razonables. Este importante salto cualitativo, impensable en condiciones normales, ha sido posible gracias a unos SIC ampliamente desarrollados.

Al mismo tiempo, esta circunstancia ha mostrado con absoluta claridad la total dependencia de los SIC que existe en la gestión pública, lo que hace que nuestras administraciones sean más vulnerables frente a los ciberataques, y que mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos sea más necesario que nunca. La generalización del trabajo en remoto tiene como contrapartida de su eficiencia un fuerte aumento de la superficie de exposición frente a las ciberamenazas, al que las entidades públicas tienen que hacer frente con las dificultades propias de un periodo de crisis.

Por tanto, el objetivo general de la auditoría ha sido proporcionar una evaluación sobre el grado de ciberseguridad de los mayores ayuntamientos de la Comunitat Valenciana, sobre el cumplimiento de la normativa en materia de seguridad de los sistemas de información y efectuar recomendaciones para la adopción de medidas de ciberhigiene.

Con esta finalidad el trabajo de auditoría ha consistido en:

- El análisis del diseño y la eficacia operativa de los Controles Básicos de Ciberseguridad (CBCS) implantados en los ayuntamientos auditados.
- La identificación de deficiencias de control que puedan afectar negativamente a la integridad,

disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y los activos de los sistemas de información de esas entidades.

- La determinación del nivel de madurez existente en cada uno de los CBCS y a nivel general en las distintas entidades auditadas y sus respectivos índices de cumplimiento.
- La identificación de incumplimientos significativos de la normativa sobre seguridad de la información.

Para conseguir estos objetivos se han auditado los quince municipios de mayor población (superior a los 50 000 habitantes) de la Comunitat Valenciana. En el cuadro 1 pueden verse los entes auditados con los datos de población y las obligaciones reconocidas netas (ORN) de 2018, en millones de euros.

Cuadro 1. Ayuntamientos auditados

Ayuntamiento	Población 2018	ORN 2018
València	791.413	1.046,1
Alicante	331.577	287,2
Elche	230.625	187,4
Castelló de la Plana	170.888	172,9
Torrevieja	82.599	64,8
Torrent	81.245	52,7
Orihuela	76.778	72,1
Gandia	73.829	92,9
Paterna	69.156	65,4
Benidorm	67.558	94,7
Sagunto	65.669	64,2
Alcoy	58.977	56,6
San Vicente del Raspeig	57.785	36,9
Elda	52.404	35,6
Vila-real	50.577	53,8
Ayuntamientos auditados	**2.261.080**	**2.383,3**
Total ayuntamientos CV	**4.963.703**	**4.917,0**
Cobertura de la auditoría	**45,6%**	**48,5%**

Fuente: *Ministerio de Hacienda. Liquidaciones de los presupuestos del ejercicio 2018. Datos actualizados 31/07/2019 (<https://serviciostelematicosext.minhap.gob.es/SGCAL/CONPREL>).*
Las ORN es información consolidada obtenida de la liquidación de cada entidad local.

La auditoría se ha centrado en el análisis de la situación de los ocho Controles Básicos de Ciberseguridad (CBCS) definidos en la GPF-OCEX 5313:

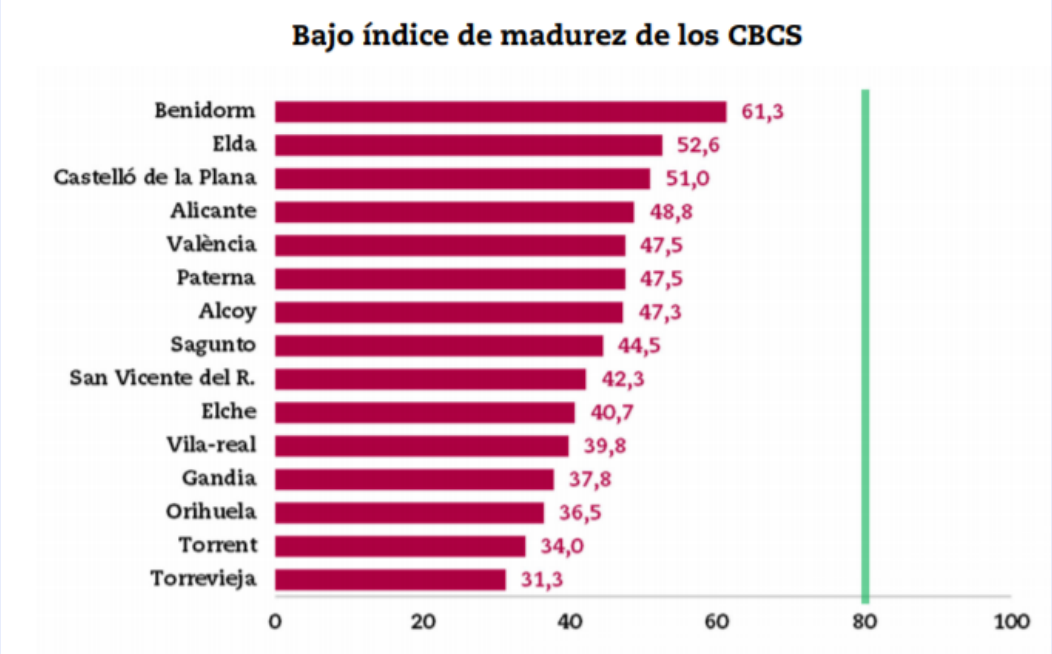
- CBCS 1: Inventario y control de dispositivos físicos.
- CBCS 2: Inventario y control de software autorizado y no autorizado.
- CBCS 3: Proceso continuo de identificación y remediación de vulnerabilidades.
- CBCS 4: Uso controlado de privilegios administrativos.
- CBCS 5: Configuraciones seguras del software y hardware.
- CBCS 6: Registro de la actividad de los usuarios.
- CBCS 7: Copias de seguridad de datos y sistemas.
- CBCS 8: Cumplimiento normativo.

OBSTÁCULOS SUPERADOS:

No se ha detectado ningún obstáculo destacable al que se haya enfrentado la buena práctica.

IMPACTO:

Ninguno de los ayuntamientos auditados alcanza el índice de madurez de los controles básicos de ciberseguridad del 80% requerido por el Esquema Nacional de Seguridad (es decir, solo se puede considerar haber obtenido un "aprobado" en ciberseguridad alcanzando la línea verde del gráfico).

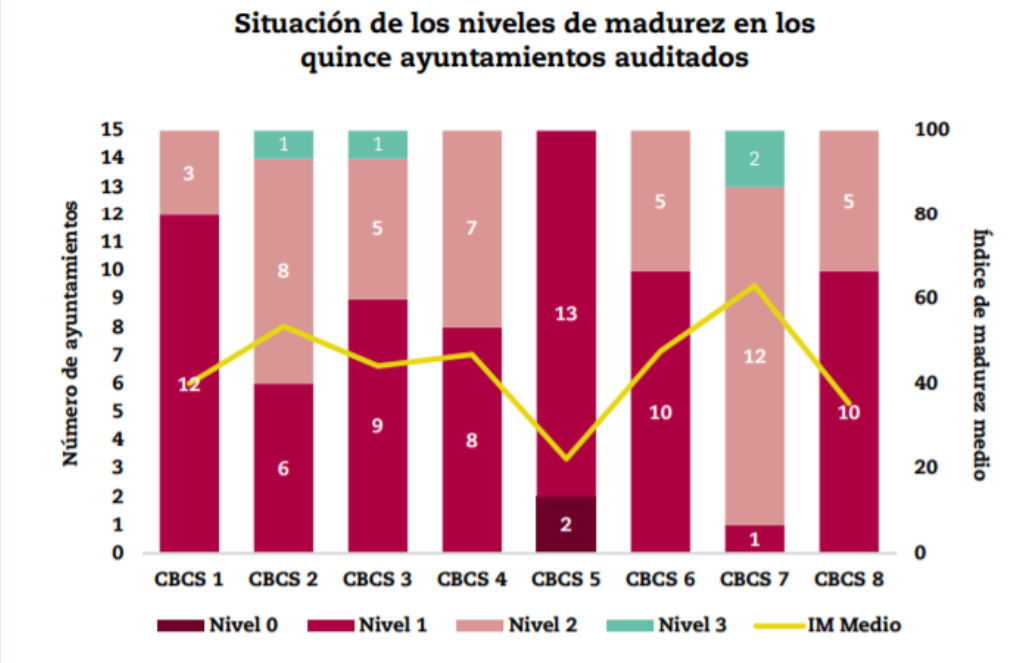


Se puede concluir, por tanto, que los sistemas de información analizados están en riesgo frente a las amenazas de ciberseguridad.

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto que existen incumplimientos generalizados de esa normativa, siendo el índice medio de cumplimiento del CBCS 8 del 44,2%. Los máximos órganos de dirección de los ayuntamientos tienen la responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales y deben impulsar las medidas necesarias para subsanar la deficiente situación existente.

Otra conclusión destaca que en general el nivel de cumplimiento con la normativa relacionada con la seguridad de la información es bastante insatisfactorio.

De un total de 120 controles básicos revisados en los quince ayuntamientos, solo cuatro controles alcanzan el nivel de madurez N3 establecido como objetivo en el Esquema Nacional de Seguridad. En el siguiente gráfico se muestra de forma resumida los niveles de madurez observados para los ocho controles básicos en el conjunto de los quince ayuntamientos, y el índice de madurez (IM) medio de cada CBCS observado en ellos.



En este sentido, todos los ayuntamientos deben adoptar medidas para mejorar su ciberseguridad: mantener una adecuada ciberhigiene y un sólido sistema de protección frente a las ciberamenazas es más necesario que

nunca. La situación provocada por la epidemia de COVID-19 ha mostrado con rotundidad la total dependencia de los sistemas de información y las comunicaciones que existe actualmente en la gestión pública, lo que hace que las administraciones públicas sean más vulnerables que nunca frente a los ciberataques y ha puesto de relieve que mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos es de vital importancia.

Es necesario un mayor compromiso y concienciación de los órganos de gobierno de los ayuntamientos con la seguridad de los sistemas de información y las comunicaciones, lo que inevitablemente conlleva una mayor inversión económica y en recursos humanos cualificados: no existe coste cero en materia de seguridad de la información.

Por todo ello, esta buena práctica impulsada por Sindicatura de Comptes ha sido premiada con el VIII Premio de las Buenas Prácticas en Gestión, Auditoría y Transparencia en el Sector Público, otorgado por la Fundación FIASEP para la formación e investigación en auditoría del sector público (https://www.sindicom.gva.es/la-unidad-de-auditoria-de-sistemas-de-informacion-de-la-sindicatura-de-comptes-recibe-el-premio-nacional-de-la-fundacion-fiasep-a-las-buenas-practicas).

CALENDARIO DE IMPLANTACIÓN Y REFERENCIA TEMPORAL:

Los datos recabados en los informes corresponden a los ejercicios de los años 2018 y 2019.

DOCUMENTACIÓN DE CONSULTA Y APOYO:

https://www.sindicom.gva.es/auditoria-delos-controles-basicos-de-ciberseguridad-delos-mayores-ayuntamientos-de-la-comunitat-valenciana-ejercicios-2019-y-2020

https://www.sindicom.gva.es/public/Attachment/2020/7/inf-cbcs-informe-global-05-definitivo_para_publicar-2020-07-20_signed.pdf