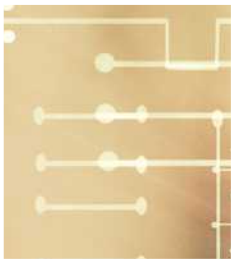
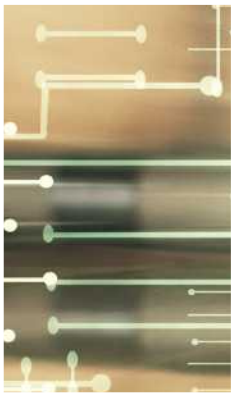
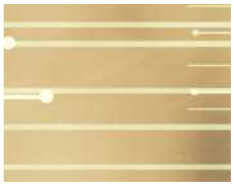
EL CONSULTOR
DE LOS AYUNTAMIENTOS



Ciberseguridad

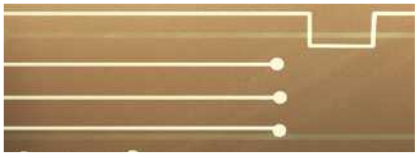
Un nuevo reto para el Estado y los Gobiernos Locales

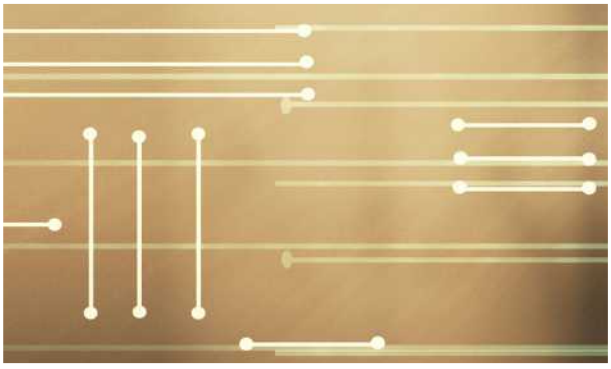




Directora

Dolors Canals Ametller





Wolters Kluwer

EL CONSULTOR
DE LOS AYUNTAMIENTOS

Ciberseguridad

Un nuevo reto para el Estado y los Gobiernos Locales

Directora

Dolors Canals Ametller

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
http://www.wolterskluwer.es

Primera edición: Abril 2021

Depósito Legal: M-7649-2021
ISBN versión impresa: 978-84-7052-846-0
ISBN versión electrónica: 978-84-7052-847-7

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

se trata de un control de último recurso por si todos los demás han fallado frente a determinados ciberataques.

5. Situación al máximo nivel de detalle

Los CBCS son controles globales formados por varios subcontroles detallados que se muestran en la siguiente tabla. Los aspectos que se comprueban en cada CBCS se especifican con el máximo detalle en la GPF-OCEX 5313.

Control	Subcontrol
CBCS 1 Inventario y control de dispositivos físicos	CBCS 1-1: Inventario de activos físicos autorizados
	CBCS 1-2: Control de activos físicos no autorizados
CBCS 2 Inventario y control de *software* autorizado	CBCS 2-1: Inventario de SW autorizado
	CBCS 2-2: SW soportado por el fabricante
	CBCS 2-3: Control de SW no autorizado
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	CBCS 3-1: Identificación de vulnerabilidades
	CBCS 3-2: Priorización
	CBCS 3-3: Resolución de vulnerabilidades
	CBCS 3-4: Parcheo
CBCS 4 Uso controlado de privilegios administrativos	CBCS 4-1: Inventario y control de cuentas de administración
	CBCS 4-2: Cambio de contraseñas por defecto
	CBCS 4-3: Uso dedicado de cuentas de administración
	CBCS 4-4: Mecanismos de autenticación
	CBCS 4-5: Auditoría y control
CBCS 5 Configuraciones seguras del *software* y *hardware*	CBCS 5-1: Configuración segura
	CBCS 5-2: Gestión de la configuración

Control	Subcontrol
CBCS 6 Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)	CBCS 6-1: Activación de *logs* de auditoría
	CBCS 6-2: Almacenamiento de *logs*: Retención y protección
	CBCS 6-3: Centralización y revisión de *logs*
	CBCS 6-4: Monitorización y correlación
CBCS 7 Copia de seguridad de datos y sistemas	CBCS 7-1: Realización de copias de seguridad
	CBCS 7-2: Realización de pruebas de recuperación
	CBCS 7-3: Protección de las copias de seguridad
CBCS 8 Cumplimiento de legalidad	CBCS 8-1: Cumplimiento del ENS
	CBCS 8-2: Cumplimiento de la LOPD/RGPD
	CBCS 8-3: Cumplimiento de la Ley 25/2013

Analizando los resultados obtenidos con un mayor grado de detalle, a nivel de subcontrol, podemos ver en el gráfico siguiente el índice de madurez medio obtenido para cada uno de los 26 subcontroles que se han analizado en los quince ayuntamientos, y se constata que en ninguno de ellos se ha alcanzado el objetivo establecido del 80%.

Fuente: SINDICATURA DE COMPTES DE LA CV (2020), Gráfico 7.

Dos subcontroles correspondientes a la gestión de copias de seguridad (el 7.1 y el 7.3) alcanzan los niveles de madurez más elevados. Este resultado permite evidenciar que las entidades priorizan la aplicación de medidas de recuperación, de coste de gestión medio/bajo, frente a controles preventivos y detectivos con mayor coste de implantación y gestión.

Otros dos de los subcontroles mejor valorados corresponden a procesos de inventariado de activos, tanto físicos (1.1) como elementos *software* (2.1). En la mayor parte de los entes auditados se hace uso de una herramienta cuyo uso ha sido promovido y facilitado por las diputaciones provinciales para la gestión automatizada de dichos inventarios.

En el otro extremo, hay tres subcontroles con un índice de madurez muy deficiente, que tienen un perfil semejante, ya que son complejos desde un punto de vista técnico y requieren de un gran esfuerzo de recursos para alcanzar la efectividad (5.2, 6.4 y 1.2), y que, por tanto, ofrecen una relación coste/beneficio no muy favorable, lo que limita su implantación en entornos de escasos medios personales y presupuestarios. Además, dos de estos tres subcontroles son detectivos, más complejos que los preventivos. El único subcontrol preventivo (la gestión de la configuración) también es técnicamente complejo y suele estar reemplazado por compensatorios técnicamente simples, pero de limitada efectividad.

6. Insatisfactorio grado de cumplimiento normativo

En las auditorías realizadas se observó, en general, un nivel de cumplimiento de la legalidad vigente (ENS, LOPD/RGPD y Ley 25/2013) bastante insatisfactorio, tal como refleja el índice medio de cumplimiento del CBCS 8 del 44,2%, que recoge el grado de cumplimiento de varias normas en materia de seguridad de los sistemas de información.

Los máximos órganos de dirección de las entidades locales 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 puesta de manifiesto.

7. Situación de las Diputaciones provinciales

En 2019 la *Sindicatura de Comptes* publicó el *Informe sobre auditoría operativa de la gestión y recaudación delegada en las diputaciones de la Comunitat Valenciana*.

Como parte de dicha auditoría se revisó si los controles generales de tecnologías de la información (CGTI) existentes garantizaban de forma razonable la seguridad de los sistemas de información y la adecuada ejecución de las aplicaciones de gestión tributaria en las tres diputaciones de la Comunidad Valenciana.

La finalidad de los controles generales de un entorno informatizado es establecer un marco general de control y confianza sobre las actividades del sistema informático y asegurar razonable de forma razonable la consecución de los objetivos generales de control interno y el correcto funcionamiento de los controles de aplicación.

Con la pandemia SARS-CoV-2 (Covid-19), el mundo digital ha desplazado de una sacudida al mundo físico. El teletrabajo y los interminables confinamientos domiciliarios han comportado un aumento inimaginable del uso de la Internet, redes sociales y plataformas digitales. Con ello, las instancias públicas, las empresas, los profesionales y los ciudadanos son y somos también más vulnerables en el entorno digital. Las amenazas individuales han ido en aumento y, en paralelo, se han incrementado los ciberataques a organismos estatales, autonómicos, y también a ayuntamientos, mucho más frágiles y expuestos a fallos de seguridad en la transición hacia una administración electrónica plena.

Al hilo de esta realidad, la presente monografía se divide en dos partes bien diferenciadas aunque interconectadas. La primera, más teórica, aborda las incidencias del ciberespacio y la ciberseguridad en las funciones del Estado y del sistema judicial, así como la prevención y denuncia de los ciberdelitos.

La segunda parte, más práctica, se centra en los riesgos que la cibercriminalidad comporta para las administraciones municipales, así como las garantías y sistemas de seguridad que resultan necesarios en su actuación a través medios informáticos, telemáticos y digitales. El objetivo de esta monografía no es otro que el de contribuir a la formación del personal al servicio de los Gobiernos locales en los conceptos y elementos básicos de seguridad digital, así como en los ataques informáticos habituales y en los instrumentos de seguridad apropiados.

La voluntad de l@s coautor@s es también divulgar la «cultura de la ciberseguridad». Sin duda, la consecución de la seguridad en el ciberespacio, cada vez más extenso, más complejo tecnológicamente y bajo un orden establecido extramuros del Estado, es una responsabilidad que nos incumbe a tod@s.

ISBN: 978-84-7052-846-0
9 788470 528460 3652K29199

Wolters Kluwer