XIII ENCUENTROS TÉCNICOS DE LOS OCEX 2019

CÁMARA DE CUENTAS DE ANDALUCÍA

Propuesta básica de indicadores para la fiscalización de cumplimiento en materia de ciberseguridad en las Corporaciones Locales

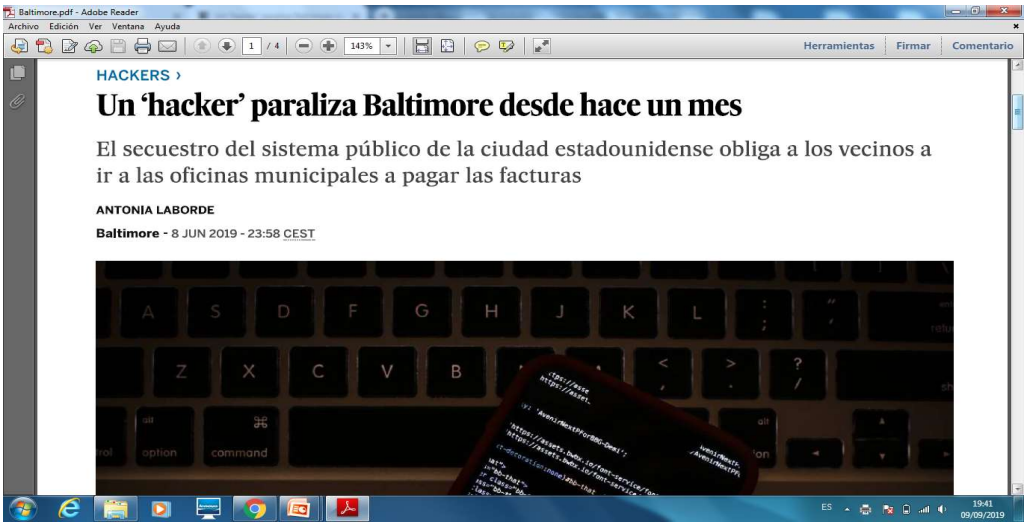
Enrique Benítez Palma
Carlos Vaz Calderón

Cámara de Cuentas de Andalucía

La fiscalización en la era de la administración electrónica

26 y 27 de septiembre de 2019
Centre Cultural La Nau
València

Ciberseguridad y entes locales (1)



Ciberseguridad y entes locales (2)

Ciberseguridad y entes locales (3)

Ciberseguridad y entes locales (4)

Un ciberataque obliga a borrar los ordenadores de Albuixech

levante-emv.com/horta/2019/08/12/ciberataque-obliga-borrar-ordenadores-albuixech/1910612.html

Un ciberataque obliga a borrar los ordenadores de Albuixech

V. S. L. | Albuixech | 12.08.2019 | 19:53

Los informáticos trata de recuperar la información que fue encriptada

El Ayuntamiento de Albuixech sufrió a principios de junio un ataque informático que dejó bloqueados todos los servicios administrativos. Según explicó ayer el Partido Popular, el fallo de seguridad permitió un acceso no autorizado, bloqueando todos los ordenadores que se encontraban conectados a la red interna. El consistorio ha tenido que formatear todos los equipos afectados y ha denunciado el caso ante la Guardia Civil.

El ayuntamiento fue víctima de un ataque mediante un programa informático que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de liberar dicha restricción. Los populares explican que «el secuestro de datos, del que solo se salvó la plataforma Gestiona, por estar está alojada en servidores externos, afectó a casi la totalidad de los programas que utiliza el personal administrativo para gestionar las tareas corrientes del Ayuntamiento (el padrón, además de los documentos que los funcionarios pudieran

Un ciberataque obliga a borrar los ordenadores de Albuixech

Gran diversidad de suelos en toda España

aliseda Inmobiliaria — Descúbrelo

Google ha cerrado el anuncio

Dejar de ver anuncio

¿Por qué este anuncio?

Contenido para ti

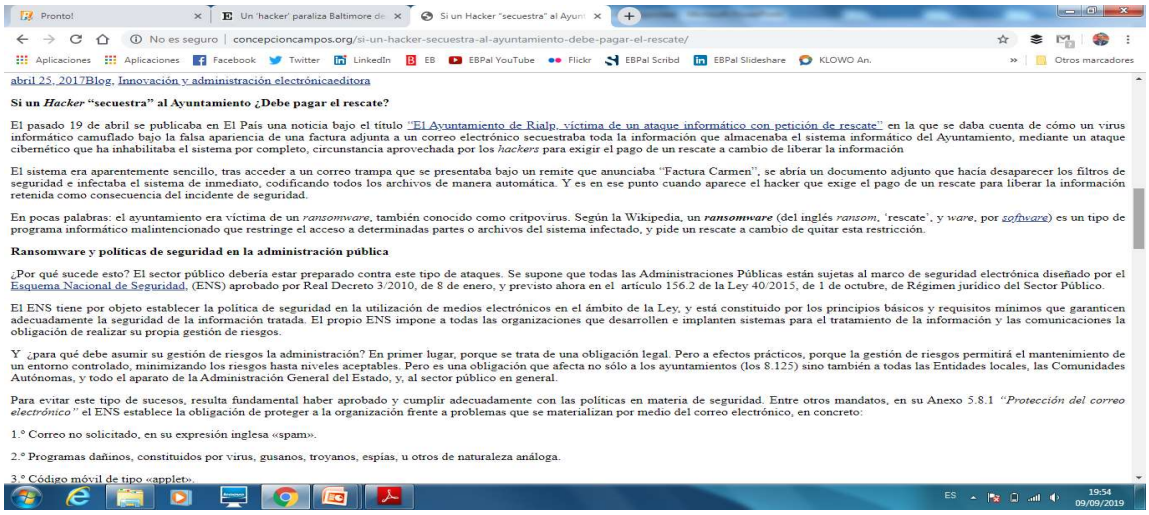
El tiempo en Valencia: La Aemet advierte de que la gota fría podría dejar lluvias torrenciales

09-09-2019

Adiós bronceado, hola infidelidades

09-09-2019

Ciberseguridad y entes locales (5)



concepcioncampos.org/si-un-hacker-secuestra-al-ayuntamiento-debe-pagar-el-rescate/

abril 25, 2017Blog, Innovación y administración electrónicaeditora

Si un *Hacker* "secuestra" al Ayuntamiento ¿Debe pagar el rescate?

El pasado 19 de abril se publicaba en El País una noticia bajo el título "El Ayuntamiento de Rialp, víctima de un ataque informático con petición de rescate" en la que se daba cuenta de cómo un virus informático camuflado bajo la falsa apariencia de una factura adjunta a un correo electrónico secuestraba toda la información que almacenaba el sistema informático del Ayuntamiento, mediante un ataque cibernético que ha inhabilitaba el sistema por completo, circunstancia aprovechada por los *hackers* para exigir el pago de un rescate a cambio de liberar la información

El sistema era aparentemente sencillo, tras acceder a un correo trampa que se presentaba bajo un remite que anunciaba "Factura Carmen", se abría un documento adjunto que hacía desaparecer los filtros de seguridad e infectaba el sistema de inmediato, codificando todos los archivos de manera automática. Y es en ese punto cuando aparece el hacker que exige el pago de un rescate para liberar la información retenida como consecuencia del incidente de seguridad.

En pocas palabras: el ayuntamiento era víctima de un *ransomware*, también conocido como criptovirus. Según la Wikipedia, un ***ransomware*** (del inglés *ransom*, 'rescate', y *ware*, por *software*) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

Ransomware y políticas de seguridad en la administración pública

¿Por qué sucede esto? El sector público debería estar preparado contra este tipo de ataques. Se supone que todas las Administraciones Públicas están sujetas al marco de seguridad electrónica diseñado por el Esquema Nacional de Seguridad, (ENS) aprobado por Real Decreto 3/2010, de 8 de enero, y previsto ahora en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen jurídico del Sector Público.

El ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada. El propio ENS impone a todas las organizaciones que desarrollen e implanten sistemas para el tratamiento de la información y las comunicaciones la obligación de realizar su propia gestión de riesgos.

Y ¿para qué debe asumir su gestión de riesgos la administración? En primer lugar, porque se trata de una obligación legal. Pero a efectos prácticos, porque la gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Pero es una obligación que afecta no sólo a los ayuntamientos (los 8.125) sino también a todas las Entidades locales, las Comunidades Autónomas, y todo el aparato de la Administración General del Estado, y, al sector público en general.

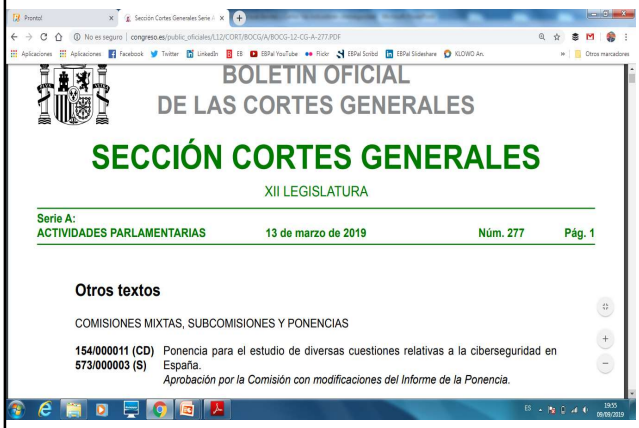
Para evitar este tipo de sucesos, resulta fundamental haber aprobado y cumplir adecuadamente con las políticas en materia de seguridad. Entre otros mandatos, en su Anexo 5.8.1 *"Protección del correo electrónico"* el ENS establece la obligación de proteger a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».

2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3.º Código móvil de tipo «applet».

Ciberseguridad y entes locales (6)



BOLETÍN OFICIAL
DE LAS CORTES GENERALES

SECCIÓN CORTES GENERALES

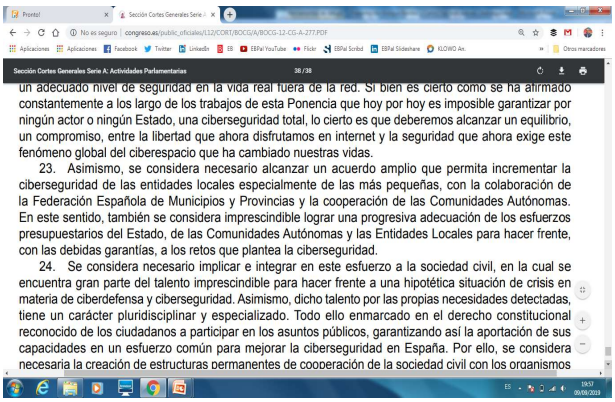
XII LEGISLATURA

Serie A: ACTIVIDADES PARLAMENTARIAS | 13 de marzo de 2019 | Núm. 277 | Pág. 1

Otros textos

COMISIONES MIXTAS, SUBCOMISIONES Y PONENCIAS

154/000011 (CD) Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en
573/000003 (S) España.
Aprobación por la Comisión con modificaciones del Informe de la Ponencia.



Sección Cortes Generales Serie A: Actividades Parlamentarias 38 /38

un adecuado nivel de seguridad en la vida real fuera de la red. Si bien es cierto como se ha afirmado constantemente a los largo de los trabajos de esta Ponencia que hoy por hoy es imposible garantizar por ningún actor o ningún Estado, una ciberseguridad total, lo cierto es que deberemos alcanzar un equilibrio, un compromiso, entre la libertad que ahora disfrutamos en internet y la seguridad que ahora exige este fenómeno global del ciberespacio que ha cambiado nuestras vidas.

23. Asimismo, se considera necesario alcanzar un acuerdo amplio que permita incrementar la ciberseguridad de las entidades locales especialmente de las más pequeñas, con la colaboración de la Federación Española de Municipios y Provincias y la cooperación de las Comunidades Autónomas. En este sentido, también se considera imprescindible lograr una progresiva adecuación de los esfuerzos presupuestarios del Estado, de las Comunidades Autónomas y las Entidades Locales para hacer frente, con las debidas garantías, a los retos que plantea la ciberseguridad.

24. Se considera necesario implicar e integrar en este esfuerzo a la sociedad civil, en la cual se encuentra gran parte del talento imprescindible para hacer frente a una hipotética situación de crisis en materia de ciberdefensa y ciberseguridad. Asimismo, dicho talento por las propias necesidades detectadas, tiene un carácter pluridisciplinar y especializado. Todo ello enmarcado en el derecho constitucional reconocido de los ciudadanos a participar en los asuntos públicos, garantizando así la aportación de sus capacidades en un esfuerzo común para mejorar la ciberseguridad en España. Por ello, se considera necesaria la creación de estructuras permanentes de cooperación de la sociedad civil con los organismos

Puntos importantes

- Normativa vigente actualizada.
- Esquema Nacional de Seguridad (ENS).
- Guías prácticas de fiscalización: GPF 5311, 5312, 5313, 5330, 5340 y 5370.
- Vulnerabilidades.
- Formación adecuada del personal y actualización.

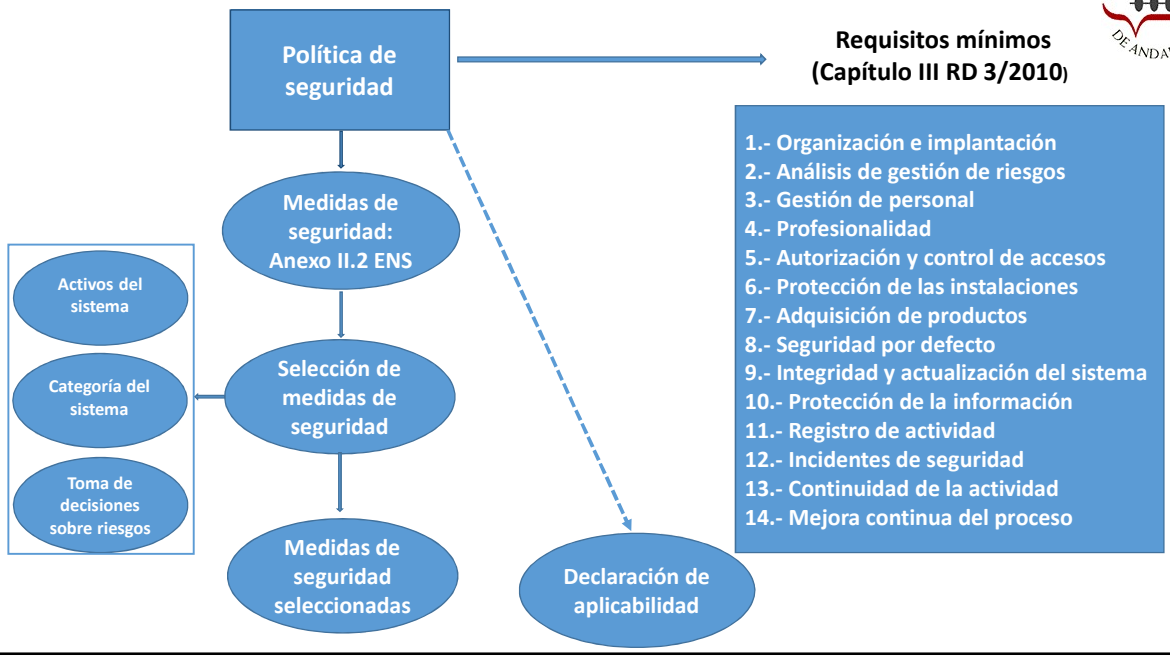
I.- APROXIMACIÓN AL CONCEPTO DE ENS

Principios básicos y requisitos mínimos para una protección adecuada de la información, con la finalidad de asegurar el cumplimiento de los objetivos de la organización mediante el uso de los sistemas de información

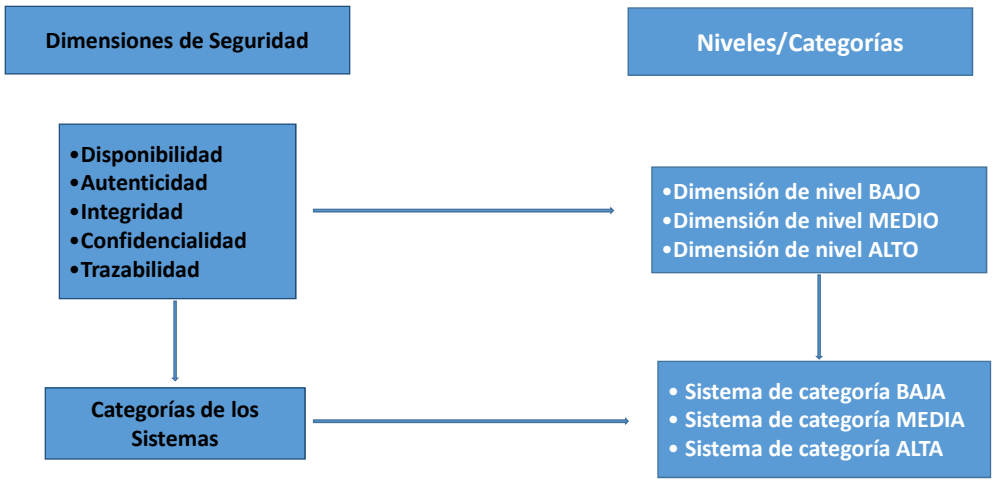
PRINCIPIOS BÁSICOS DEL PROCESO DE SEGURIDAD

1.- DEBE SER INTEGRAL
2.- BASADO EN EL ANÁLISIS Y GESTIÓN DE RIESGOS
3.- BASADO EN LA PREVENCIÓN, DETECCIÓN Y REACCIÓN
4.- LINEAS DE SEGURIDAD (CAPAS DE DEFENSA)
5.- REEVALUACIÓN PERIÓDICA
6.- DEBE CONTEMPLAR SEGREGACIÓN DE FUNCIONES

II.- HERRAMIENTAS DE IMPLEMENTACIÓN



III.- SELECCIÓN DE MEDIDAS DE SEGURIDAD. ANEXO II ENS



IV.- MEDIDAS DE SEGURIDAD A SELECCIONAR. ANEXO II ENS

IV.1.- Número de medidas de seguridad

Grupos de medidas de protección	Áreas	Categoría de las Dimensiones			
		Nº total de medidas	Baja	Media	Alta
Marco organizativo	**1**	**4**	**4**	**+0**	**+0**
Marco operacional	**6**	**31**	**15**	**+10**	**+6**
	Planificación	5	3	+1	+1
	Control de acceso	7	6	+1	+0
	Explotación	11	6	+4	+1
	Servicios Externos	3	0	+2	+1
	Continuidad del Servicio	3	0	+1	+2
	Monitorización del sistema	2	0	+1	+1
Medidas de Protección	**8**	**40**	**25**	**+8**	**+7**
	De las instalaciones e infraestructuras	8	6	+1	+1
	Del personal	5	3	+1	+1
	De los equipos	4	2	+2	+0
	De las comunicaciones	5	2	+1	+2
	De los soportes de información	5	4	+1	+0
	De las aplicaciones informáticas	2	1	+1	+0
	De la información	7	5	+0	+2
	De los servicios	4	2	+1	+1
Total	**15**	**75**	**44**	**+18**	**+13**

IV.2 Dimensiones de medidas de seguridad

Las 75 medidas se pueden aplicar a **una o varias de las cinco dimensiones** contempladas en el ENS

Categoría	Número de Dimensiones				Total	
	1 Dimensión	2 Dimensiones	4 Dimensiones	5 Dimensiones	Nº Medidas	%
Baja	8	3	5	28	44	58,67%
Media	+7	1	1	9	+18	24,00%
Alta	10	0	0	3	+13	17,33%
Total	**25**	**4**	**6**	**40**	**75**	**100,00%**
Porcentaje	**33,33%**	**5,33%**	**8,00%**	**53,33%**	**100,00%**	

IV.3.- Intensidad de las medidas

El ENS establece el nivel de intensidad aplicable a cada medida según la categoría de las dimensiones, Baja, Media, Alta. Es lo que el ENS denomina "**incremento de las exigencias**".

Grupos de medidas de protección	Áreas	Incremento de las exigencias según el nivel de la dimensión							Nº de medidas
		B=M=A	B=M<A	B<M=A	B<M<A	M=A	M<A	A	
Marco organizativo	-	4	0		0	0	0	0	4
Marco operacional	6	8	0	2	5	10	0	6	31
	Planificación	1	0	0	2	1	0	1	5
	Control de acceso	3	0	1	2	1	0	0	7
	Explotación	4	0	1	1	4	0	1	11
	Servicios Externos	0	0	0	0	2	0	1	3
	Continuidad del Servicio	0	0	0	0	1	0	2	3
	Monitorización del sistema	0	0	0	0	1	0	1	2
Medidas de Protección	8	15	3	4	3	4	4	7	40
	Instalaciones e infraestructuras	5	0	1	0	1	0	1	8
	Personal	3	0	0	0	1	0	1	5
	Equipos	0	1	1	0	1	1	0	4
	Comunicaciones	0	1	0	1	0	1	2	5
	Soportes de información	3	0	1	0	0	1	0	5
	Aplicaciones informáticas	0	0	0	1	1	0	0	2
	Información	3	0	1	1	0	0	2	7
	Servicios	1	1	0	0	0	1	1	4
Total	**15**	**27**	**3**	**6**	**8**	**14**	**4**	**13**	**75**
Peso relativo	**100%**	**36,00%**	**4,00%**	**8,00%**	**10,67%**	**18,67%**	**5,33%**	**17,33%**	**100%**

IV.- NÚMERO DE PRUEBAS A SELECCIONAR

Dado que las medidas del ENS han de aplicarse a cada una de las dimensiones, se contemplan un total de **257 pruebas**, para elegir entre las más apropiadas.

Marco	Áreas	Número de Dimensiones a las que aplicar					Nº Pruebas
		1	2	4	5	Total	
Marco organizativo	1	0	0	0	4	4	20
Marco operacional	6	7	1	6	17	31	118
	Planificación	1	0	0	4	5	21
	Control de acceso	0	1	6	0	7	26
	Explotación	2	0	0	9	11	47
	Servicios Externos	1	0	0	2	3	11
	Continuidad del Servicio	3	0	0	0	3	3
	Monitorización del sistema	0	0	0	2	2	10
Medidas de Protección	8	18	3	0	19	40	119
	Instalaciones e infraestructuras	4	0	0	4	8	24
	Personal	1	0	0	4	5	21
	Equipos	2	0	0	2	4	12
	Comunicaciones	2	1	0	2	5	14
	Soportes de información	2	1	0	2	5	14
	Aplicaciones informáticas	0	0	0	2	2	10
	Información	5	1	0	1	7	12
	Servicios	2	0	0	2	4	12
Total Nº de Medidas		**25**	**4**	**6**	**40**	**75**	**257**
Peso relativo Nº de Medidas		**33,33%**	**5,33%**	**8,00%**	**53,33%**	**100%**	
Nº Pruebas (Medidas/Dimensión)		**25**	**8**	**24**	**200**	**257**	
Peso relativo Nº de Pruebas		**9,73%**	**3,11%**	**9,34%**	**77,82%**	**100%**	

IV.2.- RESUMEN DE PRUEBAS SEGÚN NÚMERO DE DIMENSIONES Y CATEGORÍA

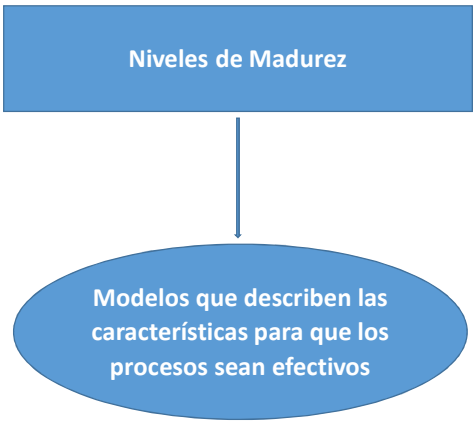
Categoría	Número de Pruebas				Total	
	1 Dimensión	2 Dimensiones	4 Dimensiones	5 Dimensiones	Número	Porcentaje
Baja	8	6	20	140	174	67,70%
Media	7	2	4	45	58	22,57%
Alta	10	0	0	15	25	9,73%
Total	**25**	**8**	**24**	**200**	**257**	**100,00%**
Porcentaje	**9,73%**	**3,11%**	**9,34%**	**77,82%**	**100,00%**	

Por tanto, para auditoría:

Selección de medidas	Número Pruebas	Porcentaje
Pruebas para 5 Dimensiones de categoría BAJA	140	54,47%
Pruebas para categoría BAJA	174	67,70%
Pruebas que afectan a las 5 Dimensiones	200	77,82%
Pruebas para categoría BAJA y MEDIA	232	90,27%

V.- IMPLEMENTACIÓN DEL ENS. CCN-STIC 804

La CCN-STIC 804 explica y desarrolla cada una de las 257 medidas de seguridad contempladas en el Anexo II del RD 3/2010



V.- IMPLEMENTACIÓN DEL ENS. CCN-STIC 804

Nivel	Descripción
L0	Inexistente. Esta medida no está siendo aplicada en este momento.
L1	Inicial/ad hoc Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a su naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
L2	Repetible, pero intuitivo. Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.
L3	Proceso definido. Se dispone de un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.

V.- IMPLEMENTACIÓN DEL ENS. CCN-STIC 804

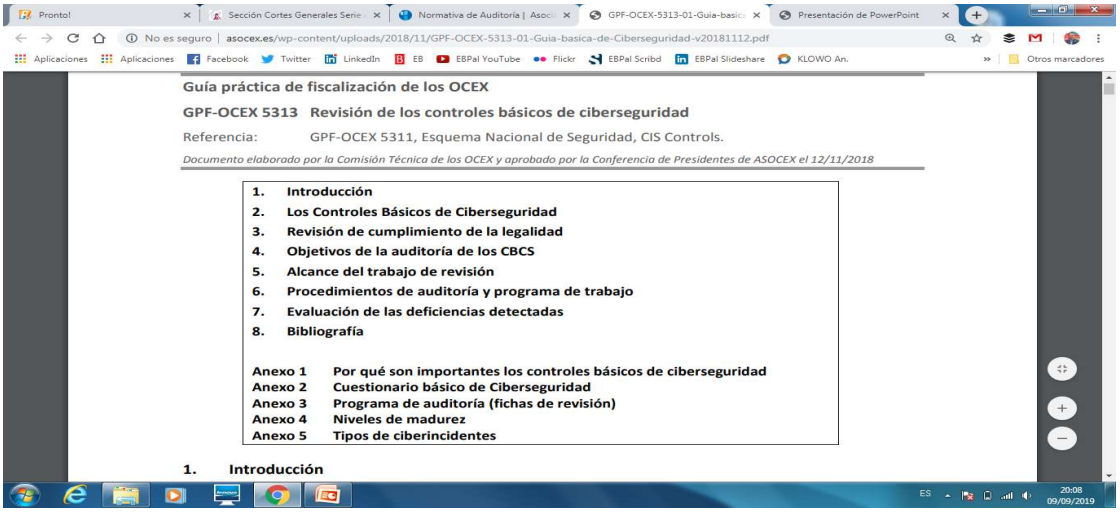
Nivel	Descripción
L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	Optimizado. 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.

V.- IMPLEMENTACIÓN DEL ENS. CCN-STIC 804

Niveles de Madurez exigidos por la CCN-STIC 804 en la implantación del ENS

Nivel de la dimensión	Categoría del sistema	Nivel de madurez mínimo
BAJO	BÁSICA	L2- Repetible pero intuitivo
MEDIO	MEDIA	L3- Proceso definido
ALTO	ALTA	L4- Gestionado y medible

Los Controles Básicos de Ciberseguridad



Guía práctica de fiscalización de los OCEX

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

Referencia: GPF-OCEX 5311, Esquema Nacional de Seguridad, CIS Controls.

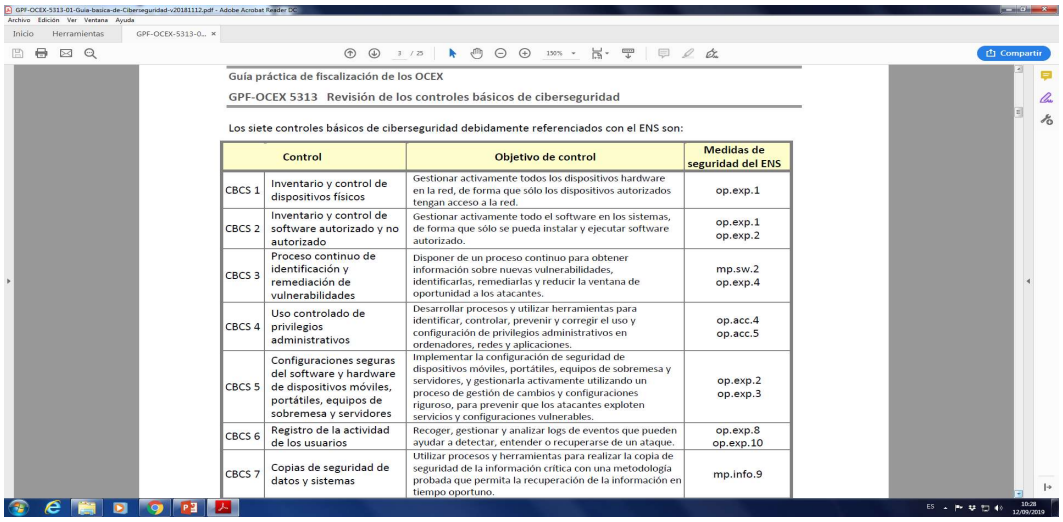
Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 12/11/2018

1. Introducción
2. Los Controles Básicos de Ciberseguridad
3. Revisión de cumplimiento de la legalidad
4. Objetivos de la auditoría de los CBCS
5. Alcance del trabajo de revisión
6. Procedimientos de auditoría y programa de trabajo
7. Evaluación de las deficiencias detectadas
8. Bibliografía

Anexo 1 Por qué son importantes los controles básicos de ciberseguridad
Anexo 2 Cuestionario básico de Ciberseguridad
Anexo 3 Programa de auditoría (fichas de revisión)
Anexo 4 Niveles de madurez
Anexo 5 Tipos de ciberincidentes

1. Introducción

Los CBCS



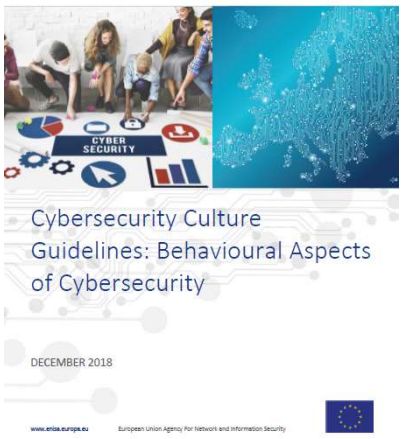
Guía práctica de fiscalización de los OCEX

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

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

Control		Objetivo de control	Medidas de seguridad del ENS
CBCS 1	Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.	op.exp.1
CBCS 2	Inventario y control de software autorizado y no autorizado	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Implementar la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	mp.info.9

La clave: las personas



A related model is that developed by Fogg (2009) that seeks to identify the type of cue needed to encourage the appropriate action, dependent on an individual's motivation and ability to perform the act (see Figure 5). According to the B=MAT model, the likelihood of a behaviour occurring is a product of motivation (M), Ability (A), and the appropriate trigger (T).

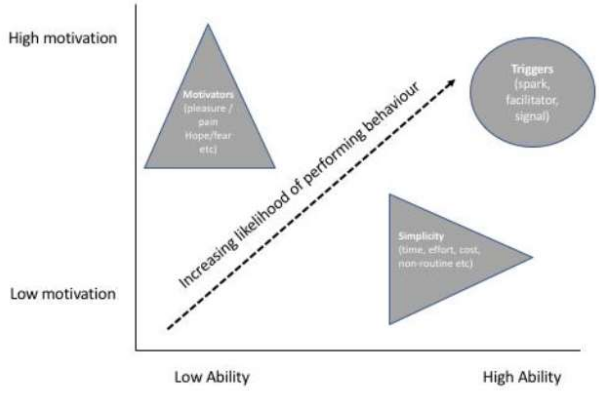


Figure 5: B=MAT model (adapted from Fogg, 2009)

El factor humano

XIII ENCUENTROS TÉCNICOS DE LOS OCEX 2019

CÁMARA DE CUENTAS DE ANDALUCÍA

Propuesta básica de indicadores para la fiscalización de cumplimiento en materia de ciberseguridad en las Corporaciones Locales

Enrique Benítez Palma
Carlos Vaz Calderón

Cámara de Cuentas de Andalucía

La fiscalización en la era de la administración electrónica

26 y 27 de septiembre de 2019
Centre Cultural La Nau
València