Guía de Seguridad de las TIC
CCN-STIC 883D

Perfil de Cumplimiento Específico Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes

Mayo 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO :083-19-183-2

Fecha de Edición: mayo de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 3/2010, de 8 de enero, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del Real Decreto 3/2010, de 8 de enero, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.

A tal fin, tras realizar un estudio de las necesidades de seguridad, de los recursos y tras un análisis de riesgos contemplando las vulnerabilidades y amenazas a las que se ven expuestas las Entidades Locales y en particular las Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente Perfil de Cumplimiento Especifico para Entidades Locales que permita la implantación del ENS en las mismas, con necesidades de categoría MEDIA.

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

Este Perfil de Cumplimiento Específico podrá ser de aplicación a las Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes, en adelante para referirnos a todos ellos indicaremos órgano competente. Estableciéndose los siguientes supuestos:

- **Servicios alojados en el órgano competente**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del órgano competente**.**
- **Servicios del órgano competente externalizados en la modalidad de software como servicio (SaaS)**. En este caso, será necesario que el sistema de información que soporta los servicios externalizados disponga de la conformidad en categoría MEDIA, siendo de aplicación el Perfil de Cumplimiento Específico al Sistema de Información del órgano competente desde el que se accede a los servicios.

3. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad es el conjunto de medidas que son de aplicación para el cumplimiento del ENS. El conjunto de medidas dependerá de los niveles asociados a las dimensiones de seguridad.

Se ha determinado que, para garantizar la seguridad en los sistemas a los que hace referencia este Perfil de Cumplimiento Especifico, la relación de medidas que son de aplicación y la exigencia en el nivel de seguridad de cada medida aplicada, es la que se indica en la siguiente tabla. El "*" indica que la medida correspondiente dispone de criterios específicos de aplicación, los cuales se detallan en el apartado "4. CRITERIOS DE APLICACIÓN DE MEDIDAS".

Dimensiones					SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación	Aplicación
categoría	aplica	=	=	[org.1]	MEDIO	MEDIO
categoría	aplica	=	=	[org.2]	MEDIO	MEDIO
categoría	aplica	=	=	[org.3]	MEDIO	MEDIO
categoría	aplica	=	=	[org.4]	MEDIO	MEDIO
categoría	aplica	+	++	[op.pl.1]	MEDIO	MEDIO
categoría	aplica	+	++	[op.pl.2]	MEDIO	MEDIO
categoría	aplica	=	=	[op.pl.3]	MEDIO	MEDIO
D	n.a.	aplica	=	[op.pl.4]	MEDIO*	n/a*
Todas	n.a.	aplica	aplica	[op.pl.5]	n/a[1]	n/a
A T	aplica	=	=	[op.acc.1]	MEDIO	MEDIO
I C A T	aplica	=	=	[op.acc.2]	MEDIO	MEDIO
I C A T	n.a.	aplica	=	[op.acc.3]	MEDIO*	MEDIO*
I C A T	aplica	=	=	[op.acc.4]	MEDIO	MEDIO
I C A T	aplica	+	++	[op.acc.5]	MEDIO	MEDIO
I C A T	aplica	+	++	[op.acc.6]	MEDIO	MEDIO
I C A T	aplica	+	=	[op.acc.7]	MEDIO	MEDIO

[1] n/a- No aplica

Dimensiones					SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicación	Aplicación
Todas	aplica	=	=	[op.exp.1]	MEDIO	MEDIO
Todas	aplica	=	=	[op.exp.2]	MEDIO	MEDIO
Todas	n.a	aplica	=	[op.exp.3]	MEDIO	MEDIO
Todas	aplica	=	=	[op.exp.4]	MEDIO	MEDIO
Todas	n.a.	aplica	=	[op.exp.5]	MEDIO	MEDIO
Todas	aplica	=	=	[op.exp.6]	MEDIO	MEDIO
Todas	n.a.	aplica	=	[op.exp.7]	MEDIO	MEDIO
T	aplica	+	++	[op.exp.8]	MEDIO	MEDIO
Todas	n.a.	aplica	=	[op.exp.9]	MEDIO	MEDIO
T	n.a.	n.a.	aplica	[op.exp.10]	n/a	n/a
Todas	aplica	+	=	[op.exp.11]	MEDIO	MEDIO
Todas	n.a.	aplica	=	[op.ext.1]	MEDIO	MEDIO
Todas	n.a.	aplica	=	[op.ext.2]	MEDIO	MEDIO
D	n.a.	aplica	=	[op.ext.9]	n/a	n/a
D	n.a.	aplica	=	[op.cont.1]	MEDIO	MEDIO
D	n.a.	n.a.	aplica	[op.cont.2]	n/a	n/a
D	n.a.	n.a.	aplica	[op.cont.3]	n/a	n/a
Todas	aplica	aplica	=	[op.mon.1]	MEDIO	MEDIO
Todas	aplica	+	++	[op.mon.2]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.if.1]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.if.2]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.if.3]	MEDIO	MEDIO
D	aplica	+	=	[mp.if.4]	MEDIO	BAJO
D	aplica	=	=	[mp.if.5]	MEDIO	MEDIO
D	n.a	aplica	=	[mp.if.6]	MEDIO*	n/a*
Todas	aplica	=	=	[mp.if.7]	MEDIO	MEDIO
D	n.a	n.a	aplica	[mp.if.9]	n/a	n/a
Todas	n.a.	aplica	=	[mp.per.1]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.per.2]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.per.3]	MEDIO	MEDIO
Todas	aplica	=	=	[mp.per.4]	MEDIO	MEDIO
Todas	n.a.	n.a.	aplica	[mp.per.9]	n/a	n/a
Todas	aplica	+	=	[mp.eq.1]	MEDIO	MEDIO
A	n.a.	aplica	+	[mp.eq.2]	MEDIO	MEDIO
Todas	aplica	=	+	[mp.eq.3]	MEDIO	MEDIO
D	n.a.	n.a.	aplica	[mp.eq.9]	n/a	n/a
Todas	aplica	=	+	[mp.com.1]	MEDIO	MEDIO

Dimensiones					SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicación	Aplicación
C	n.a	aplica	+	[mp.com.2]	MEDIO	MEDIO
I A	aplica	+	++	[mp.com.3]	MEDIO	MEDIO
Todas	n.a.	n.a.	aplica	[mp.com.4]	ALTO*	ALTO*
D	n.a.	n.a.	aplica	[mp.com.9]	n/a	n/a
C	aplica	=	=	[mp.si.1]	MEDIO*	MEDIO*
I C	n.a.	aplica	=	[mp.si.2]	MEDIO*	MEDIO*
categoría	aplica	=	=	[mp.si.3]	MEDIO*	MEDIO*
categoría	aplica	=	=	[mp.si.4]	MEDIO*	MEDIO*
C	aplica	+	=	[mp.si.5]	MEDIO*	MEDIO*
categoría	n.a.	aplica	=	[mp.sw.1]	MEDIO*	n/a*
categoría	aplica	+	++	[mp.sw.2]	MEDIO*	n/a*
categoría	aplica	=	=	[mp.info.1]	MEDIO	MEDIO
C	aplica	+	=	[mp.info.2]	MEDIO	MEDIO
C	aplica	=	=	[mp.info.3]	n/a	n/a
I A	aplica	+	++	[mp.info.4]	*	*
T	n.a.	n.a.	aplica	[mp.info.5]	ALTO*	ALTO*
C	aplica	=	=	[mp.info.6]	MEDIO	MEDIO
D	aplica	=	=	[mp.info.9]	MEDIO*	MEDIO*
Todas	aplica	=	=	[mp.s.1]	MEDIO*	MEDIO*
Todas	aplica	=	+	[mp.s.2]	MEDIO*	n/a*
D	n.a.	aplica	+	[mp.s.8]	MEDIO*	n/a*
D	n.a.	n.a.	aplica	[mp.s.9]	n/a	n/a

3.1 MEDIDAS DE APLICACIÓN

De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, aplican un total de 64*[2] medidas para los servicios proporcionados alojados en el órgano competente y de 58*[2] para los servicios del órgano competente externalizados. Son las siguientes:

SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
Marco Organizativo (4): [org.1] Política de seguridad [org.2] Normativa de seguridad [org.3] Procedimientos de seguridad [org.4] Proceso de autorización **Marco Operacional (26):**	**Marco Organizativo (4):** [org.1] Política de seguridad [org.2] Normativa de seguridad [org.3] Procedimientos de seguridad [org.4] Proceso de autorización **Marco Operacional (25):**

[2] Número aproximado de medidas que aplican

SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
[op.pl] Planificación [op.pl.1] Análisis de riesgos [op.pl.2] Arquitectura de seguridad [op.pl.3] Adquisición de nuevos componentes [op.pl.4] Dimensionamiento / Gestión de capacidades [op.acc] Control de acceso [op.acc.1] Identificación [op.acc.2] Requisitos de acceso [op.acc.3] Segregación de funciones y tareas [op.acc.4] Proceso de gestión de derechos de acceso [op.acc.5] Mecanismo de autenticación [op.acc.6] Acceso local (local logon) [op.acc.7] Acceso remoto (remote login) [op.exp] Explotación [op.exp.1] Inventario de activos [op.exp.2] Configuración de seguridad [op.exp.3] Gestión de la configuración [op.exp.4] Mantenimiento [op.exp.5] Gestión de cambios [op.exp.6] Protección frente a código dañino [op.exp.7] Gestión de incidentes [op.exp.8] Registro de la actividad de los usuarios [op.exp.9] Registro de la gestión de incidentes [op.exp.11]Protección de claves criptográficas [op.ext] Servicios externos [op.ext.1] Contratación y acuerdos de nivel de servicio [op.ext.2] Gestión diaria [op.com] Continuidad del servicio [op.com.1] Análisis de impacto [op.mon] Monitorización del sistema [op.mon.1] Detección de intrusión [op.mon.2] Sistema de métricas **Medidas de Protección (34)** [mp.if] Protección de las instalaciones e infraestructuras [mp.if.1] Áreas separadas y con control de acceso [mp.if.2] Identificación de las personas [mp.if.3] Acondicionamiento de los locales [mp.if.4] Energía eléctrica [mp.if.5] Protección frente a incendios [mp.if.6] Protección frente a inundaciones [mp.if.7] Registro de entrada y salida de equipamiento [mp.per] Gestión del personal [mp.per.1] Caracterización del puesto de	[op.pl] Planificación [op.pl.1] Análisis de riesgos [op.pl.2] Arquitectura de seguridad [op.pl.3] Adquisición de nuevos componentes [op.acc] Control de acceso [op.acc.1] Identificación [op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso [op.acc.5] Mecanismo de autenticación [op.acc.6] Acceso local (local logon) [op.acc.7] Acceso remoto (remote login) [op.exp] Explotación [op.exp.1] Inventario de activos [op.exp.2] Configuración de seguridad [op.exp.3] Gestión de la configuración [op.exp.4] Mantenimiento [op.exp.5] Gestión de cambios [op.exp.6] Protección frente a código dañino [op.exp.7] Gestión de incidentes [op.exp.8] Registro de la actividad de los usuarios [op.exp.9] Registro de la gestión de incidentes [op.exp.11] Protección de claves criptográficas [op.ext] Servicios externos [op.ext.1] Contratación y acuerdos de nivel de servicio [op.ext.2] Gestión diaria [op.com] Continuidad del servicio [op.com.1] Análisis de impacto [op.mon] Monitorización del sistema [op.mon.1] Detección de intrusión [op.mon.2] Sistema de métricas **Medidas de Protección (29)** [mp.if] Protección de las instalaciones e infraestructuras [mp.if.1] Áreas separadas y con control de acceso [mp.if.2] Identificación de las personas [mp.if.3] Acondicionamiento de los locales [mp.if.4] Energía eléctrica [mp.if.5] Protección frente a incendios [mp.if.7] Registro de entrada y salida de equipamiento [mp.per] Gestión del personal [mp.per.1] Caracterización del puesto de trabajo

SISTEMA ÓRGANO COMPETENTE	SISTEMA EXTERNALIZADO
trabajo [mp.per.2] Deberes y obligaciones [mp.per.3] Concienciación [mp.per.4] Formación [mp.eq] Protección de los equipos [mp.eq.1] Puesto de trabajo despejado [mp.eq.2] Bloqueo de puesto de trabajo [mp.eq.3] Protección de equipos portátiles [mp.com] Protección de las comunicaciones [mp.com.1] Perímetro seguro [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la autenticidad y de la integridad [mp.com.4] Segregación de redes [mp.si] Protección de los soportes de información [mp.si.1] Etiquetado [mp.si.2] Criptografía [mp.si.3] Custodia [mp.si.4] Transporte [mp.si.5] Borrado y destrucción [mp.sw] Protección de las aplicaciones informáticas [mp.sw.1] Desarrollo [mp.sw.2] Aceptación y puesta en servicio [mp.info] Protección de la información [mp.info.1] Datos de carácter personal [mp.info.2] Calificación de la información [mp.info.4] Firma electrónica [mp.info.5] Sellos de tiempo [mp.info.6] Limpieza de documentos [mp.info.9] Copias de seguridad (backup) [mp.s] Protección de los servicios [mp.si.1] Protección del correo electrónico [mp.s.2] Protección de servicios y aplicaciones web	[mp.per.2] Deberes y obligaciones [mp.per.3] Concienciación [mp.per.4] Formación [mp.eq] Protección de los equipos [mp.eq.1] Puesto de trabajo despejado [mp.eq.2] Bloqueo de puesto de trabajo [mp.eq.3] Protección de equipos portátiles [mp.com] Protección de las comunicaciones [mp.com.1] Perímetro seguro [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la autenticidad y de la integridad [mp.com.4] Segregación de redes [mp.si] Protección de los soportes de información [mp.si.1] Etiquetado [mp.si.2] Criptografía [mp.si.3] Custodia [mp.si.4] Transporte [mp.si.5] Borrado y destrucción [mp.info] Protección de la información [mp.info.1] Datos de carácter personal [mp.info.2] Calificación de la información [mp.info.4] Firma electrónica [mp.info.5] Sellos de tiempo [mp.info.6] Limpieza de documentos [mp.info.9] Copias de seguridad (backup) [mp.s] Protección de los servicios [mp.si.1] Protección del correo electrónico

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [OP.PL.3] Adquisición de nuevos componentes

Serán de aplicación los requisitos de categoría MEDIA, en el caso de servicios proporcionados directamente por el órgano competente.

En el caso de servicios del órgano competente externalizados, serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.2 [OP.PL.4] Dimensionamiento/Gestión de capacidades

Serán de aplicación los requisitos de nivel MEDIO, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.3 [OP.ACC.3] Segregación de funciones y tareas

Serán de aplicación los requisitos de nivel MEDIO, en ambos casos (servicios alojados en el órgano competente y servicios del órgano competente externalizados), con las siguientes particularidades:

- En el caso de que no se pueda aplicar por falta de personal, será necesario implementar una medida compensatoria mediante la activación de registros de actividad de todas las actuaciones sobre el sistema de información. Registro que solo podrá ser accesible por personal autorizado.

4.4 [MP.COM.4] Segregación de redes

Serán de aplicación los requisitos de nivel ALTO, en el caso de servicios proporcionados directamente por el órgano competente, del siguiente modo:

- Los flujos de información se separarán en segmentos de forma que:
  - El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
  - Si se emplean comunicaciones inalámbricas, será en un segmento separado.
  - Los segmentos de red se implementarán por medio de redes virtuales (VLAN).

En el caso de servicios del órgano competente externalizados, serán de aplicación al sistema de información del órgano competente los requisitos de nivel ALTO, en la

forma indicada en el párrafo anterior, mientras que en el sistema de información del órgano competente corresponderá a este la aplicación de esta medida.

4.5 [MP.IF.6] Protección frente a inundaciones

Serán de aplicación los requisitos de nivel MEDIO, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.6 [MP.SI] Protección de los soportes de información

Para el conjunto de medidas de "mp.si Protección de los soportes de información", serán de aplicación en nivel MEDIO y categoría MEDIA, en ambos casos (servicios alojados en el órgano competente y servicios del órgano competente externalizados), con las siguientes particularidades:

- La medida "[mp.si.1] Etiquetado" aplicará a los dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga) cuando estos contengan información relacionada con los servicios dentro del alcance del ENS y a los documentos (formato electrónico y soporte papel) que forman parte del Sistema de Gestión de la Seguridad de la Información (SGSI).
- La medida "[mp.si.5] Borrado y destrucción", también será de aplicación para los discos duros del equipamiento.

4.7 [MP.SW.1] Desarrollo de aplicaciones

Serán de aplicación los requisitos de categoría MEDIA, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.8 [MP.SW.2] Aceptación y puesta en servicio

Serán de aplicación los requisitos de categoría MEDIA, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el

sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.9 [MP.INFO.4] Firma Electrónica

Serán de aplicación los requisitos en diferentes niveles para esta medida, en ambos casos (servicios alojados en el órgano competente y servicios del órgano competente externalizados), con las siguientes particularidades:

- MEDIO: cuando se utilice firma electrónica para la actividad administrativa y esta sea necesaria para garantizar la verificación y validación de la firma electrónica.
- BAJO: cuando se utilice firma electrónica para funcionalidades distintas de la actividad administrativa.
- N.A. (no aplica): cuando no se utilice la firma electrónica en relación con los servicios que se encuentran dentro del alcance.

4.10 [MP.INFO.5] Sellos de tiempo

Serán de aplicación los requisitos de nivel ALTO para aquella información que sea susceptible de ser utilizada como evidencia electrónica, con las siguientes particularidades:

- En el caso de servicios proporcionados directamente por órgano competente.
- En caso de servicios del órgano competente externalizados, será aplicable al órgano competente solo si el servicio de sellado de tiempos no es proporcionado también por el proveedor del servicio externalizado.

4.11[MP.INFO.9] Copias de seguridad (backup)

Serán de aplicación los requisitos de nivel MEDIO, con las siguientes particularidades:

- En el caso de servicios proporcionados directamente por el órgano competente, serán de aplicación.
- En caso de servicios del órgano competente externalizados, serán de aplicación solo cuando el proveedor no proporcione también el servicio de copias de seguridad, o bien cuando exista información en el sistema de información del órgano competente susceptible de ser respaldada.

4.12[MP.S.1] Protección del Correo Electrónico

Serán de aplicación los requisitos de categoría MEDIA, en ambos casos (servicios alojados en el órgano competente y servicios del órgano competente externalizados),

siempre y cuando el correo electrónico intervenga en la prestación de los servicios dentro del alcance del ENS.

4.13[MP.S.2] Protección de los servicios y aplicaciones web

Serán de aplicación los requisitos de nivel MEDIO, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

4.14[MP.S.8] Protección frente a la denegación de servicio

Serán de aplicación los requisitos de nivel MEDIO, en el caso de servicios alojados en el órgano competente.

En el caso de servicios del órgano competente externalizados, no serán de aplicación al sistema de información del órgano competente, mientras que en el sistema de información del proveedor esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.