Junta de Andalucía

Los cambios del nuevo ENS para sistemas de nivel MEDIO. LA EXPERIENCIA PRÁCTICA EN AUDITORÍAS

Junta de Andalucía

ÍNDICE

Junta de Andalucía

1. INTRODUCCIÓN

Junta de Andalucía

1. Introducción

El objeto de este documento es resumir las diferencias entre el nuevo Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y el antiguo Real Decreto 3/2010 de 8 de enero que regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que ha quedado derogado por el primero.

Extraído de la Infografía diferencias ENS 2010 / ENS2022: Infografías ENS (CCN)

Junta de Andalucía

2.OBJETIVOS

Junta de Andalucía

2.1 Objetivos de la formación

Con la sesión de formación se pretende que el usuario de la misma tenga claros los aspectos más importantes del nuevo ENS y sobre todo, las evidencias más importantes con las que se tendrá que contar para abordar con éxito una auditoría de certificación para sistemas de nivel medio

Junta de Andalucía

2.2 Objetivos del nuevo ENS

El nuevo Esquema Nacional de Seguridad (ENS) tiene los siguientes objetivos:

1.- Adecuar el ENS al nuevo marco normativo y al contexto estratégico existente para garantizar la seguridad en la administración digital.

2.- Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas.

3.- Fortalecer la protección contra las tendencias en ciberseguridad, revisando los principios básicos, requisitos mínimos y medidas de seguridad que deben tomar las entidades vinculadas al ENS.

El nuevo ENS está distribuido en:

Extraído de la Infografía contenido esquemático del ENS 2022: Infografías ENS (CCN)

3.ANÁLISIS NUEVO ENS

Junta de Andalucía

3. Análisis del nuevo ENS

Se analizan los principios y artículos que se modifican, así como los cambios de las medidas del Anexo II más significativas.

3.1.- Articulado

- ***Política de Seguridad (art. 12)***: Los organismos o instituciones que tengan vinculación, dependencia o adscripción de una administración pública pueden incluirse subjetivamente en la política de seguridad de ésta.
- ***Responsables de seguridad (art. 13)***: Se clarifica el papel del responsable de la información, responsable del servicio, responsable del sistema, responsable de la seguridad. Excepcionalmente, en ausencia de recursos, el responsable de seguridad y el de sistemas puede recaer en la misma persona, debiendo tomar medidas compensatorias.

Bloques de responsabilidad

Junta de Andalucía

3. Análisis del nuevo ENS

- ***Nueva figura para servicios externalizados (art.13.5): el POC*** (Punto o Persona de Contacto) de Seguridad de la información, que será el responsable de seguridad de la organización contratada, o formará parte del área o tendrá contacto directo con la misma, pero la responsabilidad final será de la entidad del sector público destinataria de los servicios.
- ***Perfiles de cumplimiento específicos (art. 30):*** *Para* facilitar la conformidad con el ENS a determinadas entidades o sector de actividad concreto, se podrán implementar perfiles de cumplimiento concretos que comprenderán medidas de seguridad, que tras su análisis de riesgos resulten de aplicación para la concreta categoría de seguridad.
- ***Protección de Datos (art. 3):*** Los sistemas de información que traten datos personales deberán aplicar el RGPD y LOPDGDD, analizando los riesgos y elaborando, en su caso evaluaciones de impacto para determinar las medidas a implantar.
- ***Entrada en vigor (Disposición transitoria)****:* Todos los sistemas deberán adecuarse a los dispuesto en el Real Decreto en un plazo de 24 meses a partir de su entrada en vigor (05/05/2022).

3. Análisis del nuevo ENS

3.2.- Principios

- Los principios de “Prevención”, “Reacción” y “Recuperación” del ENS 2010 pasan a llamarse “Prevención”, “Detección”, “Respuesta” y “Conservación”, entendiendo “Respuesta” como un concepto que engloba la recuperación, e introduciendo el “Conservación”, ya que el Sistema de Información deberá garantizar la conservación de los datos e información en soporte electrónico.
- Se introduce el concepto de “Vigilancia continua”, que permitirá la detección de actividades o comportamientos anómalos y su respectiva respuesta.
- En los requisitos mínimos de seguridad, se indica la evolución del término de “Seguridad por defecto” según el real decreto de 2010, hacia la denominación “mínimo privilegio” por responder mejor al escenario actual, donde las funcionalidades de los sistemas han de ser mínimas y necesarias para los objetivos.

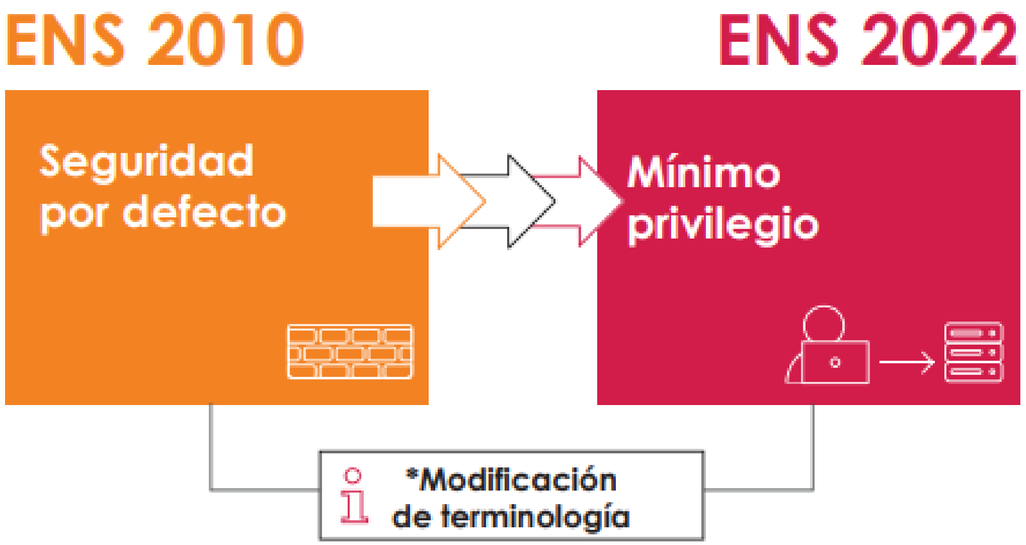
Extraído de la Infografía diferencias ENS 2010 / ENS2022 (CCN)

Junta de Andalucía

3. Análisis del nuevo ENS

3.3.- Requisitos mínimos

- Sólo un cambio de terminología.



Extraído de la Infografía diferencias ENS 2010 / ENS2022: Infografías ENS (CCN)

3. Análisis del nuevo ENS

3.3.- Medidas de seguridad. Anexo II

➢ Se establecen en cada una de las medidas del Anexo II unos Requisitos base y posibles refuerzos de seguridad (R), alineados con el nivel de seguridad perseguido, que se suman (+) a los requisitos base de la medida, pero que no siempre son incrementales entre sí; de forma que, en ciertos casos, se puede elegir entre aplicar un refuerzo u otro. Se muestran dos ejemplos:

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

En el ENS se distinguen requisitos y refuerzos

REQUISITOS

Son obligatorios para **todas las categorías** en a las que la medida sea de aplicación.

REFUERZOS OBLIGATORIOS

Son obligatorios para **determinada(s) categoría**.

NUEVO!

REFUERZOS OPCIONALES

Son de aplicación discrecional al sistema de información.

3. Análisis del nuevo ENS

- En el Anexo II de medidas de seguridad se han eliminado, modificado y añadido medidas en el marco operacional y las de protección. Respecto al marco operacional, se ha pasado de 31 a 33 medidas. Por otro lado, respecto a medidas de protección, el número de estas ha disminuido de 40 a 36 respecto al nuevo RD:

Extraído de la Infografía diferencias ENS 2010 / ENS 2022: Infografías ENS (CCN)

Junta de Andalucía

4.CAMBIOS PARA SISTEMAS DE NIVEL MEDIO

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL PRCESO DE AUDITORÍA: GUÍA CCN-STIC-808

Org.1	**Política de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Nivel de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Documento formal conteniendo la política de Seguridad de la Información (PSI) acorde al contenido esperado. ☐ En su caso, evidencia de su publicación, o de su difusión interna, en la organización. ☐ Posible procedimiento de identificación de la legislación aplicable y registro actualizado conteniendo la misma. ☐ Acta de constitución del Comité de Seguridad y designación inicial de sus miembros. ☐ Diferentes actas de designación y/o cese de miembros del Comité de Seguridad a lo largo del tiempo. ☐ Documento de aceptación de las funciones de los roles del ENS y miembros del Comité de Seguridad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Org.1 (NI)	**¿Se dispone en la organización de una Política de Seguridad de la Información (PSI) o, en su caso, se ha adherido a la política de seguridad de la institución de la que depende o está vinculada?**		☐ SI ☐ NO
☐ (NI)	¿La PSI de la organización ha sido aprobada por el titular del órgano superior correspondiente, caso de pertenecer al sector público, o por la dirección general, caso de pertenecer al sector privado, teniendo en cuenta los diferentes supuestos que determina el artículo 12 del RD 31/2022?		
☐	La PSI de la organización, en calidad de documento calificado como público, ¿Ha sido publicada y dada a conocer a empleados y colaboradores de la organización? ¿Caso de pertenecer al sector público, ha sido publicada en el Boletín Oficial correspondiente (del Estado, de la Comunidad Autónoma, de la Provincia...)?		

Sin el cumplimiento de lo marcado de color gris (o con (NI)) se considera que la medida no está implementada.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL ARTICULADO

LA CATEGORIZACIÓN YA NO RECAE EN EL RESPONABLE DEL SISTEMA

Art.40 y 41	**Categorización de los sistemas de información**		
	Medida aplica: SI ☐ NO ☐ **Medida auditada**: ☐ ☐O		
Propuesta de evidencias			
	☐ Documento de valoración de servicios e información. ☐ Documento formal en el que los responsables de los servicios y de la información suscriben las valoraciones. ☐ Documento formal en el que el Responsable de Seguridad categoriza el sistema.		
Art. 41	¿El Responsable de Seguridad determina la categoría del sistema mediante un documento formal, en base a las valoraciones de servicios e información soportados por el sistema de información que han realizado sus responsables? ¿En caso de que haya diferentes responsables de seguridad se ha realizado un comité para tomar en cuenta las decisiones de todos ellos?		☐ SI ☐ NO

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO ORGANIZATIVO

Procedimientos de seguridad [org.3]

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Anteriormente, en el RD 3/2010, ya se realizaba lo mismo pero en función de la **calificación de la información**. Ahora, en el RD 311/2022 la calificación exige únicamente USO OFICIAL y USO NO OFICIAL.

	A NIVEL ALTO	M NIVEL MEDIO	B NIVEL BAJO
Acceso	Bajo autorización expresa del propietario.	Únicamente por parte del personal interno de la organización y externos expresamente autorizados.	Acceso libre
Almacenamiento	En repositorios restringidos, debiendo estar cifrado el documento o el soporte mediante clave criptográfica	En repositorios o carpetas restringidos basados en control de acceso	No son necesarias protecciones especiales.
Copias de respaldo	Copias controladas y cifradas	Copias 'standard'	
Etiquetado	"Palabra Confidencial" en cabecera documentos, "Punto rojo" en soportes.	"Palabra Uso interno" en cabecera documentos, "Punto ámbar" en soportes.	"Palabra Pública" en cabecera documentos, "Punto verde" en soportes.
Transmisión	Mediante soportes o canales cifrados (tipo VPN) y con autorización expresa del propietario, registrando los destinatarios.	Emplear canales o soportes cifrados si se trata de comunicaciones externas.	Por cualquier medio
Destrucción	Borrado seguro de 7 o más grabaciones aleatorias o destrucción segura	Borrado seguro de 3 o más grabaciones aleatorias o destrucción segura.	Por cualquier método

NUEVO!

Sobre su contenido

Se dispondrá de una serie de documentos que detallan de forma clara y precisa:

❑ [org.3.4] *La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando como efectuar:*

- *Su control de acceso*
- *Su almacenamiento*
- *La realización de copias*
- *El etiquetado de soportes*
- *Su transmisión telemática*
- *Cualquier otra actividad relacionada con dicha información.*

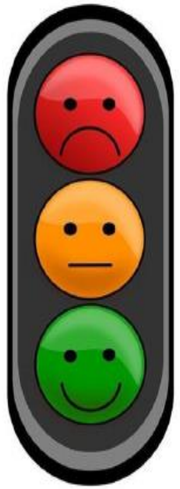
Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO ORGANIZATIVO

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Proceso de autorización [org.4]



Sobre su gestión

[NI] ❑ Verificar que **se registran las autorizaciones concedidas** (y las denegadas) a efectos de trazabilidad, siguiendo un procedimiento formal establecido en la organización.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

ANTES REQUISITO NIVEL MEDIO

Dimensiones: D		
B	M	A
aplica	+R1	+R1

Dimensionamiento / Gestión de la Capacidad [op.pl.4]

Sobre su contenido

REQUISITOS:

NI ***Con carácter previo*** *a la puesta en explotación, se realizará un estudio de capacidad que cubrirá los siguientes aspectos:*

- ❑ [op.pl.4.1] *Necesidades de* ***procesamiento.***
- ❑ [op.pl.4.2] *Necesidades de* ***almacenamiento*** *de información: durante su procesamiento y durante el periodo que deba retenerse.*
- ❑ [op.pl.4.3] *Necesidades de* ***comunicación.***
- ❑ [op.pl.4.4] *Necesidades de* ***personal****: cantidad y cualificación profesional.*
- ❑ [op.pl.4.5] *Necesidades de* ***instalaciones*** *y medios auxiliares.*

❑ ¿Se han considerado las necesidades de software y hardware, al menos con carácter previo a la puesta en explotación de los sistemas?

NI *NOTA: Se entiende por software y hardware a las aplicaciones, CPU y memoria de servidores y estaciones de trabajo, VM necesarias, balanceadores de ser necesarios, etc.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

PLAN DE CAPACIDAD

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: D		
B	M	A
aplica	+R1	+R1

Dimensionamiento / Gestión de la Capacidad [op.pl.4]

Sobre su gestión

Refuerzo R1 (Mejora continua de la Gestión de la Capacidad):

- [op.pl.4.r1.1] *Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.*
- [[op.pl.4.r1.1] *Se emplearán herramientas y recursos para la **monitorización** de la capacidad.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

ANTES REQUISITO NIVEL ALTO

Dimensiones: Todas		
B	M	A
n.a.	aplica	aplica

Componentes certificados [op.pl.5]

Sobre su contenido

REQUISITOS:

- [op.pl.5.1] ***Se utilizará el Catálogo*** *de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación* ***(CPSTIC) del CCN****, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas del RD 311/2022.*
- [op.pl.5.2] ***Si el sistema suministra un servicio de seguridad a un tercero*** *bajo el alcance del ENS,* ***el producto*** *o productos que suministren dicho servicio* ***deben superar un proceso de cualificación*** *y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento.*

- ¿Caso de no existir en el catálogo CPSTIC, o ante cualquier causa de fuerza mayor, se emplean otros productos certificados según se indica en el art. 19 del RD 311/2022, de 3 de mayo?

  NOTA: En dicho supuesto podrían ser aceptables productos al corriente de otras certificaciones de seguridad de producto, como es Common Criteria (norma ISO/IEC 15408).

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

ENS 2010

CON RESPECTO AL MARCO OPERACIONAL

Nivel MEDIO

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.

En concreto, se separarán al menos las siguientes funciones:

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de cualquier otra función.

DISMINUYE NIVEL DE EXIGENCIA

ENS 2022

Sobre su contenido

REQUISITOS:

*El sistema de control de acceso se organizará de forma que se exija la concurrencia de **dos o más personas para realizar tareas críticas**, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.*

- [op.acc.3.1] Siempre que sea posible, las capacidades de **desarrollo** y **operación** no recaerán en la misma persona.
- [op.acc.3.2] *Siempre que sea posible, las personas que **autorizan** y **controlan el uso**, serán distintas.*

NUEVO!

Dimensiones: C I T A		
B	M	A
n.a.	aplica	+R1

Segregación de funciones y tareas [op.acc.3]

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

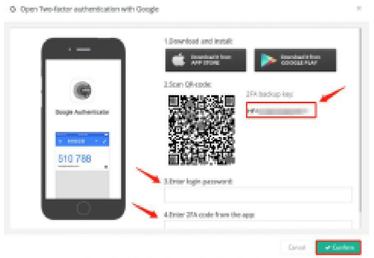
CON RESPECTO AL MARCO OPERACIONAL

Mecanismos de autenticación

RD 3/2010

- Op.acc.5 Mecanismos de autenticación.
- Op.acc.6 Acceso local
- Op.acc.7 Acceso remoto

Certificado Digital



NUEVO!

RD 311/2022

- Op.acc.5 Mecanismo de autenticación (usuarios externos)
- Op.acc.6 Mecanismo de autenticación (usuarios de la organización)

Usuarios de la organización: Esta medida se refiere a personal de la organización, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Usuarios externos: Esta medida se refiere a personal que no es de la organización, como puede ser un ciudadano que accede a una sede electrónica, si se trata del sector público, o un cliente que accede a un portal con interacción, si se trata del sector privado.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: C I T A

B	M	A
+[R1oR2oR3oR4]+R8+R9	+[R1oR2oR3oR4]+R5+R8+R9	+[R1+R2oR3oR4]+R5+R6+R7+R8+R9

(usuarios internos [op.acc.6]

Sobre su contenido

REQUISITOS:

❑ [op.acc.6.1] **Antes de proporcionar las credenciales** a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.

NUEVO!

Dimensiones: C I T A

B	M	A
+[R1oR2oR3oR4]	+[R2oR3oR4]+R5	+[R2oR3oR4]+R5

(usuarios externos) [op.acc.5]

Dimensiones: C I T A

B	M	A
+[R1oR2oR3oR4]+R8+R9	+[R1oR2oR3oR4]+R5+R8+R9	+[R1+R2oR3oR4]+R5+R6+R7+R8+R9

(usuarios internos [op.acc.6]

Sobre su contenido

REQUISITOS:

❑ [op.acc.5-6.2] *Antes de activar el mecanismo de autenticación,* ***el usuario reconocerá que las ha recibido*** *y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.*

NI ❑ [op.acc.5-6.3] *Las credenciales estarán bajo el control exclusivo del usuario y* ***se activarán una vez estén bajo su control efectivo****.(o se fuerza el cambio de credenciales al primer acceso del mismo).*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

(*) Cortesía de la Unidad de Seguridad TIC de la Agencia Digital de Andalucía (ADA), modificado

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Configuración de seguridad [op.exp.2]

Sobre su contenido

REQUISITOS (continuación):

(NI) ❑ [op.exp.2.3]*Se aplicará la regla de «**seguridad por defecto**», es decir:*

- *Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.*
- *Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.*
- *El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.*

❑ [op.exp.2.4]*Las **máquinas virtuales** estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2+R3

Gestión de la Configuración de seguridad [op.exp.3]

NUEVO!

Sobre su contenido y gestión

REQUISITOS:

NI ***Se gestionará de forma continua la configuración*** *de los componentes del sistema de forma que:*

NI ❑ [op.exp.3.1]***Se mantenga*** *en todo momento la regla de "**funcionalidad mínima**".*

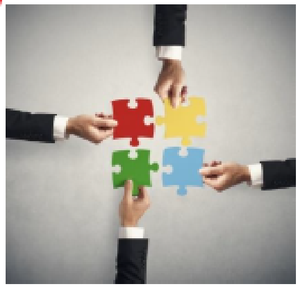
❑ [op.exp.3.2]***Se mantenga*** *en todo momento la regla de "**mínimo privilegio**".*

NI ❑ [op.exp.3.3]*El sistema **se adapte** a las nuevas necesidades, previamente autorizadas.[se gestiona de forma continua la configuración de los componentes del sistema]*

NI ❑ [op.exp.3.4]*El sistema reaccione a **vulnerabilidades** notificadas.*

NI ❑ [op.exp.3.5]*El sistema reaccione a posibles **incidentes**,*

NI ❑ [op.exp.3.6]La configuración de seguridad solamente **podrá editarse por personal debidamente autorizado**.



Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2+R3

Gestión de la Configuración de seguridad [op.exp.3]

Sobre su contenido y gestión

Refuerzo R1 (Mantenimiento regular de la configuración):

- [op.exp.3.r1.1]*Existirán* ***configuraciones hardware/software autorizadas*** *y mantenidas regularmente para los servidores, elementos de red y estaciones de trabajo.*
- [op.exp.3.r1.2]***Se verificará periódicamente la configuración hardware/software*** *del sistema para asegurarse que no se han introducido ni instalado elementos no autorizados.*
- [op.exp.3.r1.3]*Se mantendrá una* ***lista de servicios autorizados*** *para servidores y estaciones de trabajo.* **'White list'**

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Mantenimiento y actualizaciones de seguridad [op.exp.4]

Sobre su contenido y gestión

REQUISITOS:

NI ***Mantener de forma sistemática*** *el equipamiento* ***físico y lógico*** *que constituye el sistema. Se aplicará:*

NI ❑ [op.exp.4.1]*Se atenderá a las* ***especificaciones de los fabricantes*** *en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.*

❑ [op.exp.4.2]*Se dispondrá de un* ***procedimiento*** *para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.*

NI ❑ [op.exp.4.3]*El mantenimiento solamente podrá realizarse por* ***personal debidamente autorizado.***

NUEVO!

NOTA: Esta atención se concreta en un seguimiento continuo de los anuncios de defectos. Se entiende por mantenimiento del equipamiento, por ejemplo, a la liberación de espacio en disco cuando sea necesario, limpieza de archivos obsoletos, comprobación de las luces de estado en las máquinas físicas, verificación del funcionamiento correcto de aparatos, instalación de parches de seguridad cuando se requiera, etc.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Mantenimiento y actualizaciones de seguridad [op.exp.4]

Sobre su contenido y gestión

Refuerzo R1 (Pruebas en preproducción):

- ❑ [op.exp.4.r1.1]***Antes de poner en producción*** *una nueva versión o una versión parcheada* ***se comprobará, en un entorno de prueba controlado*** *y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.*

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
n.a.	aplica	+R1

Gestión de Cambios [op.exp.5]

Sobre su contenido y gestión

REQUISITOS:

*Se mantendrá un **control continuo de cambios** realizados en el sistema, de forma que:*

- [op.exp.5.1]***Los cambios se planificarán** para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio **se registrarán asignándoseles un número de referencia que permita su seguimiento**, de forma equivalente a como se registran los incidentes.*
- [op.exp.5.2]***La información a registrar para cada petición de cambio será suficiente** para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlos hasta su desestimación o implementación.*
- [op.exp.5.3]*Las **pruebas de preproducción**, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.*
- [op.exp.5.4]*Mediante un **análisis de riesgos** se determinará si los cambios son relevantes **para la seguridad del sistema**. Aquellos cambios que impliquen una situación de **riesgo de nivel ALTO serán aprobados explícitamente**, de forma previa a su implantación, **por el Responsable de la Seguridad**.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
n.a.	aplica	+R1

Gestión de Cambios [op.exp.5]

Sobre su contenido y gestión

- [op.exp.5.5] *Una vez implementado el cambio, se realizarán las **pruebas de aceptación** convenientes. Si son positivas, **se actualizará la documentación de configuración** (Diagramas de red, manuales, el inventario, etc.), siempre que proceda.*

NUEVO!

ISO/IEC 20000-1:2018 - 8.2.6 Gestión de la Configuración:

Los CI deben estar controlados. Los cambios a los CI deben ser trazables y auditables para mantener la integridad de la información de configuración. La información de configuración debe actualizarse después de implementar cambios en los CI.

La organización debe verificar la exactitud de la información de configuración a intervalos planificados. Donde se encuentren deficiencias, la organización debe llevar a cabo las acciones necesarias.

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1+R2	+R1+R2+R3+R4

Protección frente a código dañino [op.exp.6]

Sobre su contenido y gestión

REQUISITOS:

- [op.exp.6.1]*Se dispondrá de* ***mecanismos de prevención y reacción*** *frente a código dañino,* ***incluyendo el correspondiente mantenimiento*** *de acuerdo a las recomendaciones del fabricante.*
- (NI) [op.exp.6.2]***Se instalará*** *software de protección frente a código dañino* ***en todos los equipos:*** *puestos usuario, servidores y elementos perimetrales.*
- [op.exp.6.3]*Todo fichero procedente de* ***fuentes externas será analizado*** *antes de trabajar con él.*
- [op.exp.6.4] *Las* ***bases de datos de detección de código dañino*** *permanecerán* ***permanentemente actualizadas****.*
- (NI) [op.exp.6.5]*El software de detección de código dañino instalado en los* ***puestos de usuario*** *deberá estar configurado de forma adecuada e implementará* ***protección en tiempo real*** *de acuerdo a las recomendaciones del fabricante.*

NUEVO!

De la Guía CCN-STIC 808

- ¿Se requiere una contraseña de administración o se dispone de cualquier otro mecanismo que impida que el usuario final detenga o altere el funcionamiento de la solución?
- *La licencia de uso de la solución ¿Cubre la totalidad de equipos operativos presentes en la organización?*

Sobre su contenido y gestión

NUEVO!

Refuerzo R1 (Escaneo periódico):

- [op.exp.6.r1.1] *Todo el sistema se* ***escaneará regularmente*** *para detectar código dañino.*

Refuerzo R2 (Revisión preventiva del sistema):

- [op.exp.6.r2.1] *Las* ***funciones críticas se analizarán al arrancar el sistema*** *en prevención de modificaciones no autorizadas.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Gestión de Incidentes [op.exp.7]

Dimensiones: Todas		
B	M	A
aplica	+R1+R2	+R1+R2+R3

Sobre su contenido y gestión

REQUISITOS:

(NI) ❑ [op.exp.7.1]*Se dispondrá de un **proceso integral para hacer frente a los incidentes** que puedan tener un impacto en la seguridad del sistema que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de **clasificación y el escalado** de la notificación.*

(NI) ❑ [op.exp.7.2] *La gestión de **incidentes que afecten a datos personales** tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el RD 311/2022 del ENS.*

(NI) ❑ ***Refuerzo R1 (Notificación):***

*[op.exp.7.r1.1]Se dispondrá de soluciones de **ventanilla única para la notificación de incidentes al CCN-CERT**, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.*

CAU

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: T		
B	M	A
aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Registro de la actividad [op.exp.8]

Sobre su contenido y gestión

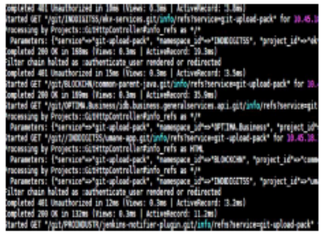
Refuerzo R1 (Revisión de los registros):

- [op.exp.8.r1.1] ***Se revisarán informalmente, de forma periódica**, los registros de actividad buscando patrones anormales.*

Refuerzo R2 (Sincronización del reloj del sistema):

- [op.exp.8.r2.1] *El sistema deberá **disponer de una referencia de tiempo (timestamp)** para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.*

NUEVO!



Sobre su contenido y gestión

Refuerzo R3 (Retención de registros):

- [op.exp.8.r3.1] *En la **documentación de seguridad del sistema** se deberán **indicar los eventos de seguridad** que serán auditados **y el tiempo de retención** de los registros antes de ser eliminados.*

Refuerzo R4 (Control de acceso):

- [op.exp.8.r4.1] ***Los registros de actividad** y, en su caso, las copias de seguridad solamente podrán ser accedidos o eliminarse por **personal debidamente autorizado**.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
n.a.	aplica	+R1

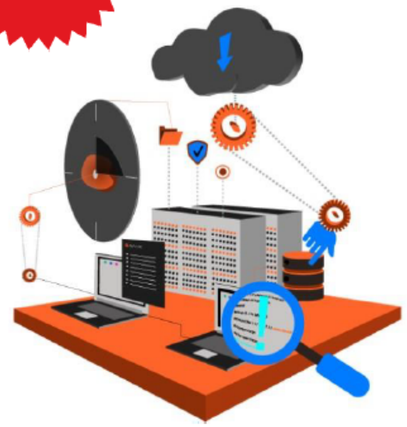
Interconexión de sistemas [op.ext.4]

Sobre su contenido y gestión

REQUISITOS:

- [op.ext.4.1] *Todos los intercambios de información y prestación de servicios con **otros sistemas** deberán ser objeto de una autorización previa. **Todo flujo de información estará prohibido salvo autorización expresa**.*
- [op.ext.4.2] *Para cada interconexión **se documentará explícitamente**: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.*

NUEVO!



Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de servicios en la Nube [op.nub.1]

Sobre su contenido y gestión

REQUISITOS:

- ❑ op.nub.1.1]*Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el* ***conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten****: Software como Servicio (Software as a Service SaaS), Plataforma como Servicio (Platform as a Service PaaS) e Infraestructura como Servicio (Infrastructure as a Service IaaS) definidas en las guías CCN-STIC que sean de aplicación.*
- (NI) ❑ [op.nub.1.2]*Cuando se utilicen* ***servicios en la nube suministrados por terceros****, los sistemas de información que los soportan deberán ser* ***conformes con el ENS*** *o* ***cumplir con las medidas desarrolladas en una guía CCN-STIC*** *que incluirá, entre otros, requisitos relativos a:*
  - *Auditoría de pruebas de penetración (pentesting).*
  - *Transparencia.*
  - *Cifrado y gestión de claves.*
  - *Jurisdicción de los datos.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de servicios en la Nube [op.nub.1]

NUEVO!

Sobre su contenido y gestión

Refuerzo R1 (Servicios certificados):

- ❑ [op.nub.1.r1.1]*Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar **certificados bajo una metodología de certificación reconocida** por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.*
- ❑ [op.nub.1.r1.2]***Si el servicio en la nube es un servicio de seguridad** deberá cumplir con los requisitos establecidos en [op.pl.5].*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO OPERACIONAL

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Detección de intrusión [op.mon.1]

Sobre su contenido y gestión

REQUISITOS:

NI [op.mon.1.1]*Se dispondrán de **herramientas de detección o prevención** de intrusiones.*

De la Guía CCN-STIC 808

NI ¿Se dispone de elementos que analicen el tráfico de red y muestren eventos de seguridad en caso de detectar posibles intrusiones en la misma? Por ejemplo, sondas IDS/IPS, capacidad IDS/IPS en los cortafuegos, panel de monitorización de eventos en Cloud, etc.

Sobre su contenido y gestión

NUEVO!

Refuerzo R1 (Detección basada en reglas):

[op.mon.1.r1.1]*El sistema dispondrá de **herramientas de detección o prevención** de intrusiones **basadas en reglas**.*

ens Esquema Nacional de Seguridad

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO AL MARCO DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	+R1+R2	+R1+R2+R3+R4+R5+R6

Vigilancia [op.mon.3]

Sobre su contenido y gestión

REQUISITOS:

- [op.mon.3.1]*Se dispondrá de un* ***sistema automático de recolección*** *de eventos de seguridad.*

Refuerzo R1 (Correlación de eventos):

- [op.mon.3.r1.1]*Se dispondrá de un* ***sistema automático de recolección de eventos*** *de seguridad* ***que permita la correlación*** *de los mismos.*

Refuerzo R2 (Análisis dinámico):

- [op.mon.3.r2.1]*Se dispondrá de soluciones de* ***vigilancia que permitan determinar la superficie de exposición*** *con relación a vulnerabilidades y deficiencias de configuración.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1

Deberes y obligaciones [mp.per.2]

Sobre su contenido y gestión

Refuerzo R1 (Confirmación expresa):

- [mp.per.2.r1.1] *Se ha de obtener la **confirmación** expresa de que **los usuarios conocen las instrucciones de seguridad** necesarias y obligatorias **y su aceptación**, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Formación [mp.per.4]

De la Guía CCN-STIC 808

- (NI) ❑ *¿Se dispone de un Plan de Formación general, orientado a las necesidades del personal, que incluya acciones formativas respecto a la seguridad de la información, donde conste la formación concreta realizada por el personal de la organización y la planificada para ser llevada a cabo?*
- (NI) ❑ *¿Se diferencia la formación impartida al personal general, de la específica para directivos, para técnicos y especialmente para personas con responsabilidades de seguridad?*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

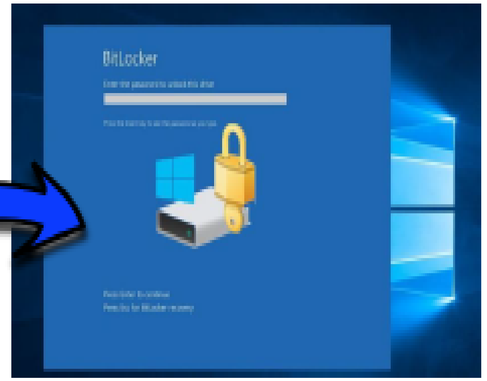
Dimensiones: Todas		
B	M	A
aplica	+R1	+R1+R2

Protección de los portátiles [mp.eq.3]

Sobre su contenido y gestión

Refuerzo R1 (Cifrado del disco):

- [mp.eq.3.r1.1] *Se protegerá el dispositivo portátil mediante **cifrado del disco duro** cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.*



Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: C		
B	M	A
aplica	+R1	+R1

Otros dispositivos conectados a la red [mp.eq.4]

Sobre su contenido y gestión

REQUISITOS:

- ❑ [mp.eq.4.1] *Los dispositivos presentes en el sistema deberán contar con una **configuración de seguridad** adecuada de manera que **se garantice el control del flujo** definido de entrada y salida de la información.* (NI)
- ❑ [mp.eq.4.2] *Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la **funcionalidad necesaria para eliminar información** de soportes de información (ver [mp.si.5]).*

Refuerzo R1 (Productos certificados):

- ❑ [mp.eq.4.r1.1] *Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5 – **Componentes certificados**].*

Refuerzo R2 opcional (Control de dispositivos conectados a la red):

- ❑ [mp.eq.4.r2.1] *Se dispondrá de soluciones que permitan **visualizar los dispositivos presentes** en la red, **controlar su conexión/desconexión** a la misma y **verificar su configuración de seguridad**.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Perímetro seguro [mp.com.1]

Sobre su contenido y gestión

REQUISITOS:

NI ❑ [mp.com.1.1] *Se dispondrá un **sistema de protección perimetral** que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.*

❑ [mp.com.1.2] ***Todos los flujos** de información a través del perímetro **deben estar autorizados previamente.***

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

NUEVO!

De la Guía CCN-STIC 808

NI ❑ *Caso de disponerse de varias sedes o centros de datos ¿disponen todos ellos de protección perimetral?*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
n.a.	+[R1oR2oR3]	+[R2oR3]+R4

Separación de flujos de información en la red [mp.com.4]

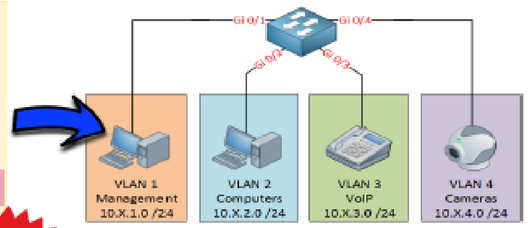
ANTES REQUISITO NIVEL ALTO

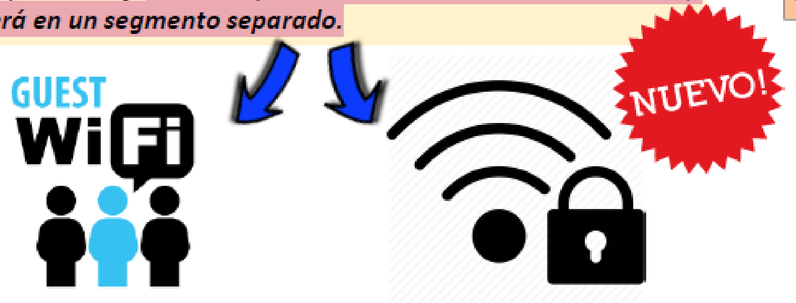
Sobre su contenido y gestión

REQUISITOS:

Los flujos de información se separarán en segmentos de forma que:

- [mp.com.4.1] ***El tráfico por la red se segregará*** *para que cada equipo solamente tenga acceso a la información que necesita.*
- [mp.com.4.2] *Si se emplean* ***comunicaciones inalámbricas, será en un segmento separado.***





Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
n.a.	+[R1oR2oR3]	+[R2oR3]+R4

Separación de flujos de información en la red [mp.com.4]

Sobre su contenido y gestión

O Refuerzo R1 (Segmentación lógica básica):

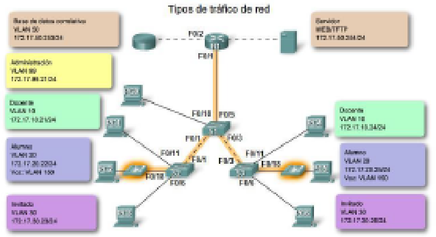
- ❑ [mp.com.4.r1.1] *Los segmentos de red se implementarán por medio de **redes de área local virtuales** (Virtual Local Area Network **VLAN**).*
- ❑ [mp.com.4.r1.2] *La red que conforma el sistema deberá segregarse en **distintas subredes contemplando como mínimo:***
  - *Usuarios*
  - *Servicios*
  - *Administración*

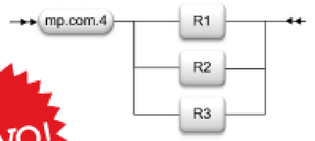
O Refuerzo R2 (Segmentación lógica avanzada):

- ❑ [mp.com.4.r2.1] *Los segmentos de red se implementarán por medio de **redes privadas virtuales** (Virtual Private Network **VPN**).*

O Refuerzo R3 (Segmentación física):

- ❑ [mp.com.4.r3.1] *Los segmentos de red se implementarán con **medios físicos separados**.*





NUEVO!

Categoría MEDIA

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: C		
B	M	A
n.a.	aplica	aplica

Marcado de soportes [mp.si.1]

Sobre su contenido y gestión

REQUISITOS:

- [mp.si.1.1] *Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia - vídeos, cursos, presentaciones - etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas,* ***llevarán las marcas o metadatos*** *correspondientes* ***que indiquen el nivel de seguridad de la información contenida*** *de mayor calificación.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Criptografía [mp.si.2]

ANTES NIVEL ALTO

Sobre su contenido y gestión

REQUISITOS:

- ❑ [mp.si.2.1]***Se usarán mecanismos criptográficos*** *que garanticen la confidencialidad y la integridad de la información contenida*
- ❑ [mp.si.2.2]*Se emplearán algoritmos y parámetros* ***autorizados por el CCN****.*

Refuerzo R1 (Productos certificados):

- ❑ *[mp.si.2.r1.1] Se emplearán* ***productos certificados*** *conforme a lo establecido en [op.pl.5 Componentes certificados].*

Refuerzo R2 (Copias de seguridad):

- ❑ *[mp.si.2.r2.1]* ***Las copias se seguridad se cifrarán*** *utilizando algoritmos y parámetros autorizados por el CCN.*

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Desarrollo de aplicaciones [mp.sw.1]

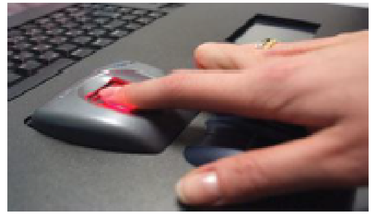
Sobre su contenido y gestión

Refuerzo R1 (Mínimo privilegio):

- ❑ *[mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.*

Refuerzo R2 (Metodología de desarrollo seguro):

- ❑ *[mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:*
  - *Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.*
  - *Incluirá normas de programación segura: control de asignación y liberación de memoria, desbordamiento de memoria (overflow).*
  - *Tratará específicamente los datos usados en pruebas.*
  - *Permitirá la inspección del código fuente.*



Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1

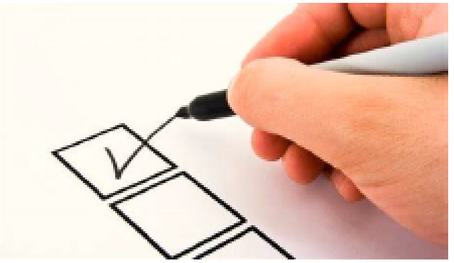
Aceptación y puesta en servicio [mp.sw.2]

Sobre su contenido y gestión

REQUISITOS:

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

- [mp.sw.2.1]*Se comprobará que:*
  - (NI) *Se cumplen los **criterios de aceptación en materia de seguridad**.*
  - *No se deteriora la **seguridad de otros componentes** del servicio.*



Refuerzo R1 (Pruebas):

[mp.sw.2.r1.1]*Las **pruebas** se realizarán en un **entorno aislado (preproducción).***

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	+R1	+R1

Aceptación y puesta en servicio [mp.sw.2]

De la Guía CCN-STIC 808

- (NI) ❑ *¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual 'Guía de instalación y configuración segura del sistema' dirigida a los administradores?*
- (NI) ❑ *¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual 'Guía de uso seguro del sistema' dirigida a los usuarios?*
- ❑ *¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual 'Guía de la relación entre cliente y proveedor' dirigida a los administradores?*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Datos personales [mp.info.1]

Sobre su contenido y gestión

REQUISITOS:

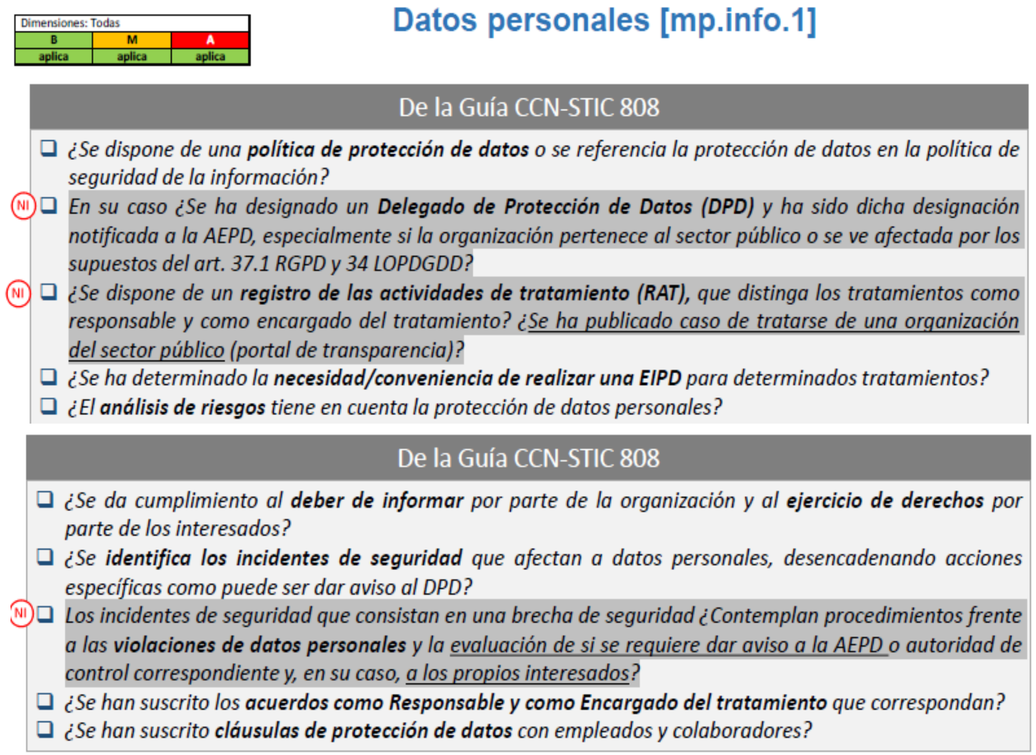
NI ❑ [mp.info.1.1] *Cuando el sistema **trate datos personales**, el Responsable de la Seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas **de acuerdo a la naturaleza, alcance, contexto y fines del mismo**, así como de los **riesgos para los derechos y libertades** de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.*

aepd agencia española protección datos

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN



Dimensiones: Todas		
B	M	A
aplica	aplica	aplica

Datos personales [mp.info.1]

De la Guía CCN-STIC 808

- ❑ *¿Se dispone de una **política de protección de datos** o se referencia la protección de datos en la política de seguridad de la información?*
- NI ❑ *En su caso ¿Se ha designado un **Delegado de Protección de Datos (DPD)** y ha sido dicha designación notificada a la AEPD, especialmente si la organización pertenece al sector público o se ve afectada por los supuestos del art. 37.1 RGPD y 34 LOPDGDD?*
- NI ❑ *¿Se dispone de un **registro de las actividades de tratamiento (RAT)**, que distinga los tratamientos como responsable y como encargado del tratamiento? ¿Se ha publicado caso de tratarse de una organización del sector público (portal de transparencia)?*
- ❑ *¿Se ha determinado la **necesidad/conveniencia de realizar una EIPD** para determinados tratamientos?*
- ❑ *¿El **análisis de riesgos** tiene en cuenta la protección de datos personales?*

De la Guía CCN-STIC 808

- ❑ *¿Se da cumplimiento al **deber de informar** por parte de la organización y al **ejercicio de derechos** por parte de los interesados?*
- ❑ *¿Se **identifica los incidentes de seguridad** que afectan a datos personales, desencadenando acciones específicas como puede ser dar aviso al DPD?*
- NI ❑ *Los incidentes de seguridad que consistan en una brecha de seguridad ¿Contemplan procedimientos frente a las **violaciones de datos personales** y la evaluación de si se requiere dar aviso a la AEPD o autoridad de control correspondiente y, en su caso, a los propios interesados?*
- ❑ *¿Se han suscrito los **acuerdos como Responsable y como Encargado del tratamiento** que correspondan?*
- ❑ *¿Se han suscrito **cláusulas de protección de datos** con empleados y colaboradores?*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: C		
B	M	A
n.a.	aplica	aplica

Calificación de la información [mp.info.2]

■ Sobre su contenido y gestión

REQUISITOS:

- ❑ [mp.info.2.1]*Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de* ***materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción*** *en su manejo por su sensibilidad y confidencialidad.*
- ❑ [mp.info.2.2]*La política de seguridad (*)* ***establecerá quién es el responsable de cada información*** *manejada por el sistema.*
- ❑ [mp.info.2.3]*La política de seguridad recogerá, directa o indirectamente, los* ***criterios que, en cada organización, determinarán el nivel de seguridad requerido.***

(*) o alguna norma interna o procedimiento de calificación de la información que la desarrolle.

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

Dimensiones: C		
B	M	A
n.a.	aplica	aplica

Calificación de la información [mp.info.2]

Sobre su contenido y gestión

REQUISITOS (continuación):

- [mp.info.2.4]***El responsable de cada información*** *seguirá los criterios determinados en el apartado anterior para* ***asignar a cada información el nivel de seguridad requerido****, y será responsable de su* ***documentación y aprobación formal****.*
- [mp.info.2.5]***El responsable de cada información*** *en cada momento tendrá en exclusiva la potestad de modificar el* ***nivel de seguridad*** *requerido, de acuerdo a los apartados anteriores.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: D		
B	M	A
aplica	+R1	+R1+R2

Copias de seguridad (backup) [mp.info.6]

Sobre su contenido y gestión

Refuerzo R1 (Pruebas de recuperación):

- [mp.info.6.r1.1]*Los procedimientos de copia de seguridad y restauración deben **probarse regularmente**; la frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.*

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: Todas		
B	M	A
aplica	aplica	+R1

Protección de la navegación web [mp.s.3]

Sobre su contenido y gestión

REQUISITOS:

El **acceso de los usuarios internos a navegar por internet** se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- (NI) ❑ [mp.s.3.1] *Se establecerá una **normativa de uso** destacando el uso que se autoriza y las limitaciones de uso personal. En particular se concretará el uso permitido de conexiones cifradas.*
- (NI) ❑ [mp.s.3.2] *Se llevarán a cabo **regularmente actividades de concienciación** sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.*
- ❑ [mp.s.3.3] ***Se formará al personal encargado de la administración del sistema** en monitorización del servicio y respuesta a incidentes.*
- ❑ [mp.s.3.4] ***Se protegerá la información** de resolución de direcciones web y de establecimiento de conexiones.*
- (NI) ❑ [mp.s.3.5] ***Se protegerá a la organización en general y al puesto de trabajo** en particular frente a problemas que se materializan vía navegación web*

NUEVO!

Sobre su contenido y gestión

REQUISITOS (continuación):

- ❑ [mp.s.3.6] *Se protegerá contra la actuación de programas dañinos: páginas activas, descargas de código ejecutable, **previniendo la exposición del sistema a vectores de ataque** del tipo spyware, ransomware, etc.*
- ❑ [mp.s.3.7] *Se establecerá una **política ejecutiva de control de cookies**, en particular para evitar la contaminación entre uso personal y uso organizativo.*

NUEVO!

Junta de Andalucía

4. Cambios para sistemas de nivel MEDIO

CON RESPECTO MEDIDAS DE PROTECCIÓN

Dimensiones: D		
B	M	A
n.a.	aplica	+R1

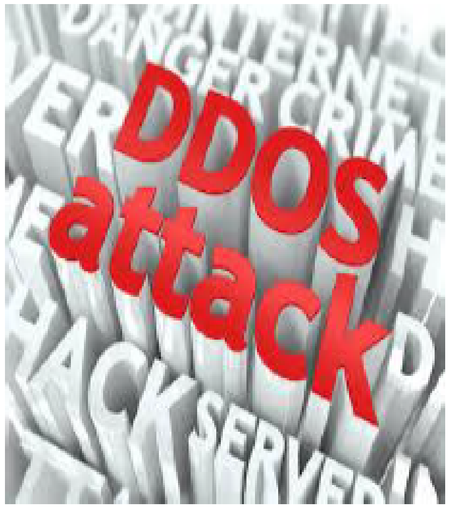
Protección frente a la denegación de servicio [mp.s.4]

Sobre su contenido y gestión

REQUISITOS:

*Se establecerán **medidas preventivas** frente a ataques de denegación de servicio y denegación de servicio distribuido (Denial of Service DoS, Distributed Denial of Service DDoS). Para ello:*

- ❑ [mp.s.4.1] *Se planificará y dotará al sistema de **capacidad suficiente** para atender con holgura a la carga prevista.*
- ❑ [mp.s.4.2] ***Se desplegarán tecnologías para prevenir** los ataques conocidos.*



Junta de Andalucía

5. CONCLUSIONES

Junta de Andalucía

5. Conclusiones

¿Motivaciones para la actualización del ENS?

1. Mejorar la confianza de la ciudadanía en el uso de los medios electrónicos (más de 10 años del último ENS).
2. Asemejar al concepto de “mejora continua” de las normas ISO.
3. Adaptación al marco legal actual.
4. Avance de las tecnologías.
5. Intensificación de controles para hacer frente a ciberamenazas y ciberincidentes.
6. Aumentar la extensión del ENS.
7. Utilización de la acumulación de experiencias en aplicación del ENS.

6. REFERENCIAS

6. Referencias

- BOE del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

- BOE del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

- Infografías sobre el ENS 2022 desarrollado por el Centro Criptológico Nacional. Infografías ENS (CCN)

- Página sobre el ENS del Centro Criptológico Nacional. https://ens.ccn.cni.es/es/

7. RUEGOS Y PREGUNTAS

Junta de Andalucía


Junta de Andalucía