Algunas modificaciones en el articulado del nuevo ENS

Artículos 5 a 11. Principios básicos.

- Introduce el principio de vigilancia continua, que permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

Artículo 13. Organización e implantación del proceso de seguridad.

- Introduce la previsión de la Certificación de Responsables de Seguridad.
- Para servicios externalizados, el proveedor deberá designar un POC (Punto o Persona de Contacto) de Seguridad de la Información.

Artículo 16. Profesionalidad

- Las organizaciones determinarán el diseño curricular y experiencia necesaria del personal para el desarrollo de su puesto trabajo.

Artículo 20. Mínimo privilegio (antes Seguridad por Defecto)

- **Se aplicarán guías de configuración de seguridad** para las diferentes tecnologías adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 23. Prevención ante otros sistemas de información interconectados.

- Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la **instrucción técnica de seguridad** correspondiente. Aún sin aprobar, aunque existe la guía CCN-STIC-811 Interconexión en el ENS.

Artículo 24. Registro de la actividad y detección de código dañino

- Habilita la posibilidad de analizar las comunicaciones con la finalidad de impedir accesos no autorizados, detener ataques DoS, evitar la distribución de código dañino y otros daños a redes y sistemas.

Artículo 25. Incidentes de seguridad

- Necesidad de aplicar la “Instrucción Técnica de Seguridad (ITS) de Notificación de Incidentes de Seguridad” que supone la aplicación de la Guía CCN-STIC 817 Esquema Nacional de Seguridad - Gestión de Ciberincidentes.

Artículo 30. Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.

- Posibilidad de implementar perfiles de cumplimiento específicos para entidades. Por ejemplo:
  - ✓ CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (menos de 5.000 habitantes)
  - ✓ CCN-STIC 883B - Perfil Cumplimiento Específico Ayuntamientos de menos de 20.000 habitantes
  - ✓ CCN-STIC 883C - Perfil de Cumplimiento Específico Ayuntamientos de entre 20.000 y 75.000 habitantes
  - ✓ CCN-STIC 883D - Perfil de Cumplimento Específico Diputaciones
- Perfiles de cumplimiento para soluciones. Por ejemplo:
  - ✓ CCN-STIC-885 Perfil de cumplimiento específico para Office 365 Servicio de Cloud Corporativo
- Condiciones para implantación, en modo local, de productos, sistemas o servicios originariamente prestados en la nube o de forma remota. A considerar:
  - ✓ CCN-STIC-858 Implantación de sistemas SaaS en modo local (on-premise)

Artículo 31. Auditoría de la seguridad.

- El plazo de dos años **podrá extenderse durante tres meses** cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos. (Efectos del COVID y confinamiento)

Artículo 33. Capacidad de respuesta a incidentes de seguridad de la información

- Sector público – Notificar al CCN incidentes con impacto significativo.
- Sector privado – Notificar al INCIBE-CERT

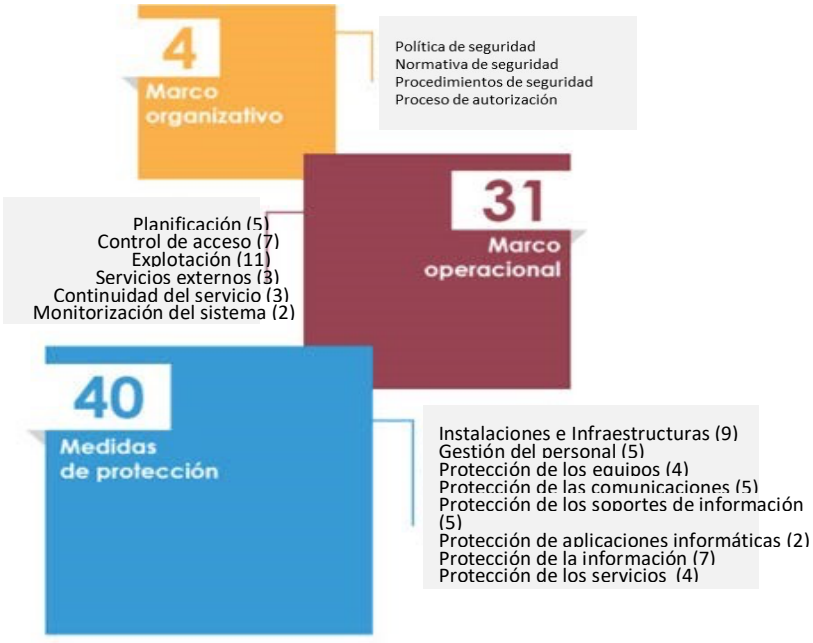
Disposición transitoria única. Adecuación de sistemas

- Los sistemas preexistentes a su entrada en vigor, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente Distintivo de Conformidad.
- Los nuevos sistemas de información aplicarán lo establecido en el presente real decreto desde su concepción.

MODIFICACIONES EN DETALLE DEL ANEXO II DEL ENS

MEDIDAS

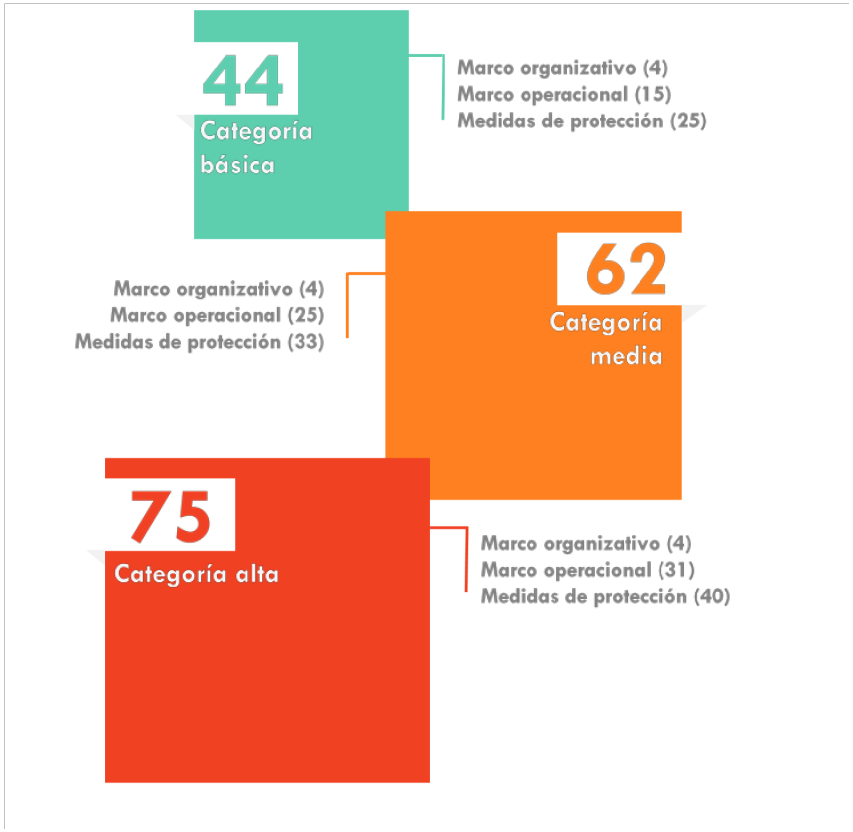
RD 2015



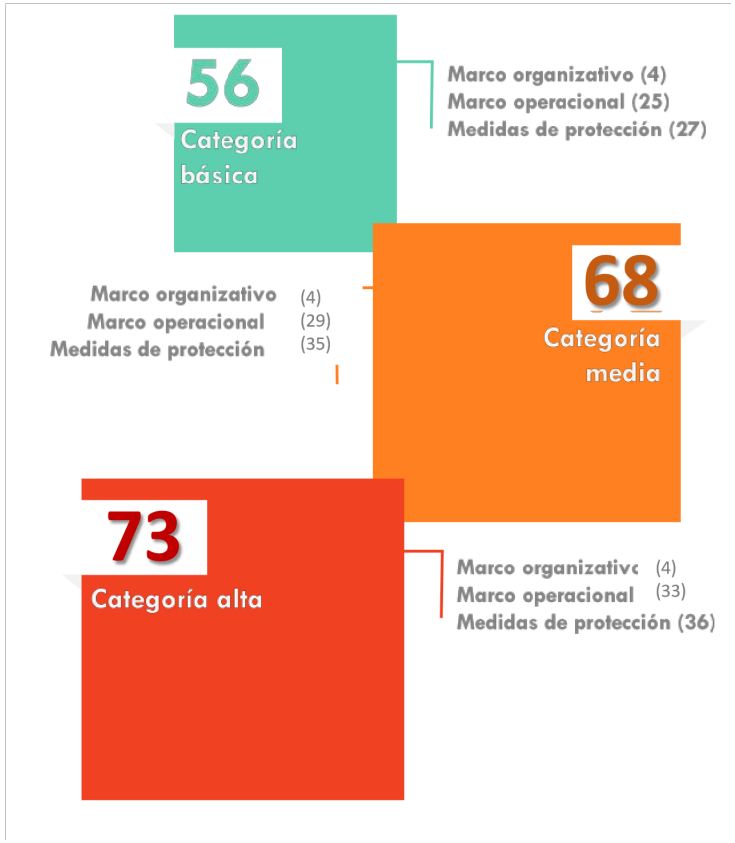
NUEVO RD

Por categorías.

RD 2015



NUEVO RD



PLANIFICACIÓN

- ✓ Se han **reforzado significativamente la exigencia en la arquitectura en el dimensionamiento/gestión de la capacidad**.
- ✓ **CONTROL DE ACCESO:** piedra angular de la seguridad por el alto riesgo acceso no autorizado
- ✓ Se **incrementan significativamente los requisitos de identificación**.
- ✓ Se **refuerzan levemente los requisitos de acceso y la protección de gestión de derechos de acceso**
- ✓ Se **aligeran las exigencias en materia de segregación de tareas**

EXPLOTACIÓN

- ✓ **Reforzadas significativamente** en la **configuración de seguridad y su gestión, mantenimiento** y **actualizaciones de seguridad**, la **protección frente a código dañino** y el **registro de la actividad** de los usuarios

✓ **Aumenta moderadamente su exigencia en gestión de cambios e incidentes** (se exige desde categoría BÁSICA)

✓ **Se elimina el control relativo a la protección de los registros de actividad**, ya contemplado en otras medidas.

RECURSOS EXTERNOS

✓ Se incorporan **nuevas medidas destinadas a los recursos externos provistos**, cada vez más frecuentes en la administración digital: **protección de la cadena de suministro, interconexión de sistemas,**

CONTINUIDAD DEL SERVICIO

✓ **Se incorpora medios alternativos** (que engloba todas las referentes a personal, equipos, instalaciones… alternativas que se han eliminado de las medidas de protección),

SERVICIO EN LA NUBE

✓ Se introduce una nueva medida para la **protección de servicios en la nube** ✓

Esquema Nacional de Seguridad

MONITORIZACIÓN DEL SISTEMA

- ✓ Se ha **reforzado** significativamente la exigencia de las **medidas de detección de intrusión y sistema de métricas**
- ✓ Se ha incorporado una **nueva medida de vigilancia**, alentada por las más recientes prácticas internacionales, dirigida a asegurar el mantenimiento de la monitorización constante de la seguridad del sistema.

PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

- ✓ Se han realizado **cambios editoriales** y **eliminado las instalaciones alternativas** ✓

GESTIÓN DEL PERSONAL

- ✓ Se ha **incrementado levemente la exigencia en deberes y obligaciones** y eliminado personal alternativo

PROTECCIÓN DE LOS EQUIPOS

- ✓ Se incorpora **nueva medida en relación con los dispositivos conectados a la red**
- ✓ Se **elimina la medida referida a medios alternativos**

PROTECCIÓN DE LAS COMUNICACIONES

- ✓ Experimentan un leve **incremento de exigencia la protección de la confidencialidad, y la separación de flujos de información** en la red.
- ✓ Se obliga a cifrar las redes privadas virtuales, cuando la comunicación discurra fuera del propio dominio de seguridad.
- ✓ **Se aligera el perímetro seguro**

PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

- ✓ Se refuerzan levemente el **borrado y destrucción**

PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

- ✓ **Se incrementa significativamente la exigencia en aceptación y puesta en servicio**, a la vista de los nuevos vectores de ataque propiciados vulnerabilidades en el software

PROTECCIÓN DE LA INFORMACIÓN

- ✓ Se **aligera calificación de la información**

- ✓ **Se incrementa exigencia en datos de carácter personal** y **copias de seguridad**

PROTECCIÓN DE LOS SERVICIOS

- ✓ Se añade una **nueva medida para la protección de la navegación web**
- ✓ Se **aumenta la exigencia de protección frente a denegación de servicio**
- ✓ Se eliminan medios alternativos.

MEDIAS NUEVAS

- ✓ Las medidas que hacían referencia a **medios, instalaciones y personal alternativo** ([op.ext.9], [mp.if.9], [mp.per.9], [mp.eq.9] [mp.com.9], [mp.s.9]), se han aglutinado en la nueva medida [op.cont.4] medios alternativos.
- ✓ [mp.info.3] antigua medida de **cifrado**, se recoge ahora en otras medidas en las que se hace referencia expresa al **cifrado de dispositivos portátiles, protección de la confidencialidad, criptografía y transporte** ([mp.eq.3], [mp.com.2], [mp.si.2] y [mp.si.4] respectivamente).

- ✓ [op.ext.3] **Protección de la cadena de suministro** para categoría ALTA.
- ✓ [op.ext.4] **Interconexión de sistemas** desde categoría MEDIA.
- ✓ **[op.nub] medida para sistemas que suministran servicios en la nube** a los organismos del sector público para todos los niveles y categorías.
- ✓ [op.cont.4] **Medios alternativos.** Para nivel ALTO. Aúna todas las referencias que se hacían a medios, instalaciones y personal alternativo.
- ✓ [op.mon.3] **Vigilancia.** Aplica a todas las categorías.
- ✓ [mp.eq.4] **Otros dispositivos conectados a la red**. Aplica a todas las categorías.
- ✓ [mp.s.3] **Protección de la navegación web**. Aplica a todas las categorías y se refuerza incluyendo la monitorización para categoría ALTA.

Medidas que refuerzan significativamente la exigencia

- ✓ [op.pl.4] **Dimensionamiento/gestión de la seguridad**. Cambios editoriales, ampliada a nivel BAJO y aumento exigencia a todos los niveles incluyendo la mejora continua de la gestión de la capacidad a niveles MEDIO y ALTO.
- ✓ [op.acc.1] **Identificación**. Cambios editoriales y aumento de exigencia a niveles MEDIO y ALTO incluyendo la identificación avanzada.
- ✓ [op.exp.2] **Configuración de seguridad.** Cambios editoriales y ampliada en categoría MEDIA y ALTA incluyendo la configuración de máquinas virtuales.
- ✓ [op.exp.3] **Gestión de la configuración de seguridad.** Cambios editoriales, ampliada a categoría BÁSICA y aumento de exigencias (se incluye exigencia a personal autorizado) en categorías MEDIA y ALTA.
- ✓ [op.exp.4] **Mantenimiento y actualizaciones de seguridad.** Actualizada (se incluye exigencia a personal autorizado) y ampliada en categorías MEDIA y ALTA.
- ✓ [op.exp.6] **Protección frente a código dañino.** Actualizada y ampliada. Aumenta requisitos en categoría MEDIA y ALTA, incluyendo el escaneo periódico y la lista blanca de aplicaciones autorizadas.

- ✓ [op.exp.8] **Registro de actividad.** Actualizada y aumento de exigencias en categoría BÁSICA y MEDIA incluyendo la sincronización de reloj, retención de registros y control de acceso a los mismos

- ✓ [op.mon.1] **Detección de intrusión.** Cambios editoriales y aumenta exigencia en todas las categorías incluyendo la detección basada en reglas desde categoría MEDIA y ejecución de acciones predeterminadas para categoría ALTA.

- ✓ [op.mon.2] **Sistema de métricas.** Actualizada y aumento de exigencia en todas las categorías, incluyendo la evaluación del sistema de gestión de la seguridad desde categoría MEDIA.