VIII JORNADAS STIC CCN-CERT

La defensa del patrimonio tecnológico frente a los ciberataques

10 y 11 de diciembre de 2014

Actualización del ENS

Carlos F. Gómez Muñoz

Ministerio de Hacienda y Administraciones Públicas
Dirección de Tecnologías de la Información y las Comunicaciones

Carlosf.gomez@seap.minhap.es

Índice

Contexto

- **Art. 42.3 Ley 11/2007: Actualización permanente**
- **Revisión del RD 3/2010 a la luz de**:
  - la experiencia adquirida,
  - de los comentarios recibidos por vías formales e informales y
  - de la evolución de la tecnología y las ciberamenazas
  - y del contexto regulatorio europeo.
- **Alineamiento con el Reglamento (UE) Nº 910/2014 de identidad electrónica y servicios de confianza**
  - Publicado el 28.08.2014
- **Consensuado** en los grupos de trabajo de AGE y demás AA.PP. (2 años de trabajo, 2013 y 2014)
  - Fruto de la colaboración y el esfuerzo colectivo
- **Preparado para tramitación**.

Principales novedades

- Se introduce la **Declaración de Aplicabilidad** para formalizar las medidas de seguridad aplicadas
- Se introducen las **instrucciones técnicas de seguridad** para señalar el modo común de actuar.
- Se implementan los mecanismos para obtener un **conocimiento regular del estado de la seguridad** en las AA.PP.
- Se introduce la **notificación de incidentes de seguridad**
- Se precisan los **elementos necesarios para la investigación de incidentes de seguridad**.
- **Se mejora la eficacia de ciertas medidas** de seguridad del Anexo II.
- **Otras mejoras** editoriales.

Declaración de aplicabilidad y medidas compensatorias

- Se añaden dos nuevos apartado 4 y 5 al artículo **27**:

- La relación de medidas de seguridad se formalizará en una **Declaración de Aplicabilidad**.

- Las medidas de seguridad podrán ser reemplazadas por otras **compensatorias** siempre que se justifique que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos.

- En la Declaración de Aplicabilidad se indicará la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan.

Instrucciones técnicas de seguridad

- Artículo afectado: **29**
- Para armonizar el modo común de actuar en relación con ciertas cuestiones **se introducen las instrucciones técnicas de seguridad**.
- Para la elaboración de las instrucciones técnicas de seguridad se aplicarán los procedimientos consolidados en el ámbito de la Interoperabilidad.
- Se contempla desarrollar instrucciones tales como las siguientes:

a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.
c) Auditoría de la seguridad.
d) Conformidad con el Esquema Nacional de Seguridad.
e) Adquisición de productos de seguridad.
f) Criptología de empleo en el Esquema Nacional de Seguridad.
g) Interconexión en el Esquema Nacional de Seguridad.
h) Requisitos de seguridad en entornos externalizados.

Conocer regularmente el estado de seguridad

- Artículo afectado: **35**

- Se asienta el **mecanismo que permita recoger periódicamente información de las principales variables** para conocer e informar del estado de seguridad, en adecuadas condiciones de eficacia y eficiencia.

- El CCN articulará procedimientos a través de grupos de trabajo del Comité Sectorial de Administración Electrónica y de la Comisión de Estrategia TIC.

Refuerzo de la capacidad de respuesta frente a incidentes de seguridad

- Notificación de incidentes. Artículo afectado: **36**

- Se notificarán los aquellos **incidentes que tengan un impacto significativo** en la seguridad de la información manejada y de los servicios prestados.

- Mediante una *instrucción técnica de seguridad* se determinarán las características de los incidentes sujetos a notificación y el procedimiento para realizarla.

- La figura de la notificación de los hechos que tengan un impacto significativo en la seguridad es una tendencia en proyectos normativos de la UE.

Refuerzo de la capacidad de respuesta frente a incidentes de seguridad

- Soporte y coordinación del CCN-CERT. Artículo afectado: **37**

- Para una mejor respuesta a incidentes de seguridad, se tendrán en cuenta **evidencias tales como**: informes de auditoría, registros de auditoría, configuraciones y otra información relevante, así como los soportes informáticos

- **Atendiendo a** los siguientes aspectos:

  - Cuando sea de aplicación, a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo.

  - A la posible confidencialidad de datos de carácter institucional u organizativo.

Medidas de seguridad que se mejoran

Se introducen **precisiones orientadas a aumentar la eficacia de ciertas medidas de seguridad del Anexo II. Principalmente las siguientes**:

- 3.4 Proceso de autorización [org.4]
- 4.1.2. Arquitectura de seguridad [op.pl.2]
- 4.1.5 Componentes certificados [op.pl.5] + medidas relacionadas
- 4.2.5. Mecanismo de autenticación [op.acc.5]
- 4.3.8. Registro de la actividad de los usuarios [op.exp.8]
- 4.3.9. Registro de la gestión de incidentes [op.exp.9]
- 4.6.1. Detección de intrusión [op.mon.1]
- 4.6.2. Sistema de métricas [op.mon.2]
- 5.4.3. Protección de la autenticidad y de la integridad [mp.com.3]
- 5.5.5. Borrado y destrucción [mp.si.5]
- 5.7.4. Firma electrónica [mp.info.4]
- 5.7.7. Copias de seguridad [mp.info.9]

4.2.1. Identificación [op.acc.1]

Se alinea con el Reglamento (UE) Nº 910/2014 de identidad electrónica y servicios de confianza.

Las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia

Si se requiere un nivel BAJO en la dimensión de autenticidad (Anexo I)

- nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento nº 910/2014)

Si se requiere un nivel MEDIO en la dimensión de autenticidad (Anexo I)

- nivel de seguridad sustancial o alto (artículo 8 del Reglamento nº 910/2014)

Si se requiere un nivel ALTO en la dimensión de autenticidad (Anexo I)

- nivel de seguridad alto (artículo 8 del Reglamento nº 910/2014) »

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

4.2.5. Mecanismo de autenticación [op.acc.5]

Se alinea con el Reglamento (UE) Nº 910/2014 de identidad electrónica y servicios de confianza.

Se generaliza la redacción para usar las expresiones ‘algo que se sabe’, ‘algo que se tiene’ y ‘algo que se es’.

- Antes de proporcionar credenciales a usuarios, identificación y registro de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración.
- Se contemplan varias posibilidades de registro de los usuarios
- Se modulan en los tres niveles bajo/medio/alto el uso de los factores de autenticación y las condiciones relativas a las credenciales.

dimensiones	ICAT		
nivel	bajo	medio	alto
	aplica	+	++

4.6.2. Sistema de métricas [op.mon.2]

Se alinea con el informe del estado de la seguridad previsto en el artículo 35.

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:
Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría MEDIA:
Además, se recopilaran datos para valorar el sistema de gestión de incidentes, permitiendo conocer
- número de incidentes de seguridad tratados
- tiempo empleado para cerrar el 50% de los incidentes
- tiempo empleado para cerrar el 90% de las incidentes

Categoría ALTA
Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:
- recursos consumidos: horas y presupuesto »

5.7.4. Firma electrónica [mp.info.4]

Se alinea con el Reglamento (UE) Nº 910/2014 de identidad electrónica y servicios de confianza.

Firma / certificados cualificados

dimensiones	I A		
nivel	bajo	medio	Alto
	aplica	+	++

Nivel BAJO
Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:
d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:
    1. Certificados.
    2. Datos de verificación y validación.
e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2.
f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Nivel ALTO
1. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.
2. Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. »

Retos a la fecha

- Como dice la Estrategia de Ciberseguridad Nacional: "*Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados*."
- Tramitar el proyecto de modificación del Real Decreto 3/2010.
- Elaborar las *Instrucciones Técnicas de Seguridad*.
- Desarrollar el soporte relativo a la conformidad con el ENS.
- Continuar el esfuerzo de desarrollo de instrumentos de apoyo a la adecuación al ENS: guías y herramientas.

- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Síguenos en Linked in