MODIFICACIONES EN EL ENS (RD 3/2010)

Esteban Sánchez Sánchez
Universidad Politécnica de Cartagena
esteban.sanchez@si.upct.es

ANÁLISIS Y GESTIÓN DE RIESGOS CON PILAR

Universidad Politécnica de Cartagena

- **CAPÍTULO III. REQUISITOS MÍNIMOS**
  - Artículo 18. Adquisición de productos de seguridad.
  - Artículo 27. Cumplimiento de requisitos mínimos.
  - Artículo 29. Guías de seguridad.
- **CAPÍTULO V. AUDITORÍA DE SEGURIDAD**
  - Artículo 34. Auditoría de la seguridad.
- **CAPÍTULO VII. RESPUESTA A INCIDENTES DE SEGURIDAD**
  - Artículo 36. Capacidad de respuesta a incidentes de seguridad de la información.
  - Artículo 37. Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.

Universidad Politécnica de Cartagena

- **DIPOSICIONES ADICIONALES**
  - Disposición adicional quinta. Desarrollo del esquema nacional de seguridad
  - Disposición transitoria única
- **ANEXO II. MEDIDAS DE SEGURIDAD**
  - Arquitectura de seguridad [op.pl.2]
  - Componentes certificados [op.pl.5]
  - Identificación [op.acc.1]
  - Mecanismos de autenticación [op.acc.5]
  - Registro de actividad de los usuarios [op.exp.8]

ANÁLISIS Y GESTIÓN DE RIESGOS CON PILAR

Universidad Politécnica de Cartagena

- Detención de la intrusión [op.mon.1]
- Sistema de métricas [op.mon.2]
- Protección de equipos portátiles [mp.eq.3]
- Borrado y destrucción [mp.si.5]
- Firma electrónica [mp.info.4]
- Sellos de tiempo [mp.info.5]
- Copias de seguridad (backup) [mp.info.9]

ANÁLISIS Y GESTIÓN DE RIESGOS CON PILAR

Universidad Politécnica de Cartagena

- ANEXO III. OBJETO DE LA AUDITORÍA
- CONCLUSIONES FINALES
- GRUPO IRIS-ENS

CAPÍTULO III. REQUISITOS MÍNIMOS

Universidad Politécnica de Cartagena

ARTÍCULO 18. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD

- Se incluye en el título la contratación de servicios de seguridad: ``Adquisición de productos y **contratación de servicios de seguridad´´**

- **Es necesario que los productos tengan certificadas sus funcionalidades de seguridad en base a normas y estándares internacionales** (antes se valoraba positivamente)

  - Salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad. **Una Instrucción Técnica de Seguridad detallará los criterios exigibles.**

CAPÍTULO III. REQUISITOS MÍNIMOS

ARTÍCULO 27. CUMPLIMIENTO DE REQUISITOS MÍNIMOS

- Nuevos apartados:

  - << La relación de medias seleccionadas del anexo II se formalizará en un documento denominado **Declaración de Aplicabilidad, firmado por el responsable de seguridad**. >>

  - **Estas medidas podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente (en la declaración de aplicabilidad)** que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos.

CAPÍTULO III. REQUISITOS MÍNIMOS

ARTÍCULO 29. GUÍAS DE SEGURIDAD

- Nuevo apartado:

  - << **El MINHAP**, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, **aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante Resolución de la Secretaria de Estado de Administraciones Públicas**. Para la redacción y mantenimiento de las instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica. >>

CAPÍTULO V. AUDITORÍA DE LA SEGURIDAD

ARTÍCULO 34. AUDITORÍA DE LA SEGURIDAD

- << **Una instrucción técnica de seguridad** regulará el desarrollo de las auditorías previstas en el presente real decreto. >>

CAPÍTULO VII. RESPUESTA A INCIDENTES DE SEGURIDAD

Universidad Politécnica de Cartagena

ARTÍCULO 36. CAPACIDAD DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- «Las Administraciones Públicas **notificarán al Centro Criptológico Nacional** aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados. **Mediante la correspondiente instrucción técnica de seguridad se determinarán las características de los incidentes sujetos a notificación y el procedimiento para realizarlo**. »

- ¿ LUCÍA ?

CAPÍTULO VII. RESPUESTA A INCIDENTES DE SEGURIDAD

Universidad Politécnica de Cartagena

ARTÍCULO 37. PRESTACIÓN DE SERVICIOS DE RESPUESTA A INCIDENTES DE SEGURIDAD A LAS ADMINISTRACIONES PÚBLICAS

- Se concreta la información que el CCN-CERT puede solicitar a las Administraciones cuando se produzcan incidentes:

  - **<< Registros de auditoría, configuraciones y otra información relevante**, así como los **soportes informáticos** que se estimen necesarios para la investigación del incidente de los sistemas afectados, atendiendo, 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. >>

DISPOSICIONES ADICIONALES

Universidad Politécnica de Cartagena

DISPOSICIÓN ADICIONAL QUINTA. DESARROLLLO DEL ENS (NUEVA)

- Se listan las instrucciones técnicas de seguridad de obligado cumplimiento:

  - 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.

DISPOSICIONES ADICIONALES

Universidad Politécnica de Cartagena

DISPOSICIÓN TRANSITORIA ÚNICA (NUEVA)

- << Las entidades del ámbito de aplicación 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, dispondrán de **un plazo de veinticuatro meses para la adecuación de sus sistemas** a lo dispuesto en el presente real decreto. >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

ARQUITECTURA DE SEGURIDAD [OP.PL.2]

- Modificación de categorías afectadas:
  - Ahora:

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

  - Propuesto: Diferencia entre las medidas a aplicar a los sistemas con categoría media y a los de categoría alta

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	+

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

ARQUITECTURA DE SEGURIDAD [OP.PL.2]

- Medida nueva para categoría media:
  - Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.
- Medidas antes de categoría básica y ahora alta:
  - Sistema de gestión con actualización y aprobación periódica.
  - Controles técnicos internos:
    - 1. Validación de datos de entrada, salida y datos intermedios. »

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

COMPONENTES CERTIFICADOS [OP.PL.5]

- Ahora:
  - << Se utilizarán preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes de reconocida solvencia. >>

- Propuesto:
  - << Se utilizarán preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales **y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.** >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

COMPONENTES CERTIFICADOS [OP.PL.5]

- <<**Una instrucción técnica de seguridad detallará los criterios exigibles.** >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

IDENTIFICACIÓN [OP.ACC.1]

- Nuevo apartado:
  - << En los supuestos contemplados en el Capítulo IV relativo a "**Comunicaciones Electrónicas**", **las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia**, con la siguiente **correspondencia** entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (**bajo, sustancial, alto**) de los sistemas de identificación electrónica previstos en el **Reglamento nº 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de 2014**, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior** y por el que se deroga la Directiva 1999/93/CE. >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

MECANISMO DE AUTENTICACIÓN [OP.ACC.5]

- Ahora:
  - **Se admitirá el uso de cualquier mecanismo de autenticación**: claves concertadas, o dispositivos físicos (en expresión inglesa »tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.
  - En el caso de usar contraseñas se aplicarán reglas básicas

- Propuesto:
  - Como principio general, **se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor**

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

MECANISMO DE AUTENTICACIÓN [OP.ACC.5]

- Propuesto en nivel Medio:
  - << **Se exigirá el uso de al menos dos factores de autenticación** >> (**Antes no se recomendaban claves concertadas pero no se decía explícitamente que no se pudiesen usar**)
  - Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:
    - 1. Presencial.
    - 2. Telemático usando certificado electrónico cualificado.
    - 3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo seguro de creación de firma.

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

REGISTRO DE ACTIVIDAD DE LOS USUARIOS (OP.EXP.8)

- Modificación de los niveles afectados:
  - Ahora:

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

  - Propuesto: Afecta a los sistemas con trazabilidad baja y media

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

REGISTRO DE ACTIVIDAD DE LOS USUARIOS (OP.EXP.8)

- Todas las que había antes sólo para nivel alto se aplican a todos los niveles:
  - << Se registrarán todas las actividades de los usuarios en el sistema, de forma que:
    - a) El registro indicará quién realiza la actividad, cuando la realiza y sobre qué información.
    - b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.
    - c) Deben registrarse las actividades realizadas con éxito y los intentos fracasados.
    - d) La determinación de qué actividades debe en registrarse y con qué niveles de detalle se determinará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]). >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

REGISTRO DE ACTIVIDAD DE LOS USUARIOS (OP.EXP.8)

- Nueva nivel bajo:
  - << Se activarán los registros de actividad en los servidores. >>
- Nueva nivel medio:
  - <<Se revisarán informalmente los registros de actividad buscando patrones anormales. >>
- Nueva nivel alto:
  - << Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada. >>

Universidad Politécnica de Cartagena

DETECCIÓN DE INTRUSIÓN (OP.MON.1)

- Modificación de categorías afectadas:
  - Ahora:

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

  - Propuesto: Afecta a lo sistemas de categoría media

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

SISTEMA DE MÉTRICAS (OP.MON.2)

- Modificación de categorías afectadas:
  - Ahora:

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

  - Propuesto: Afecta a lo sistemas de categoría básica y media

Dimensiones	todas		
Categoría	básica	media	alta
	aplica	+	++

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

SISTEMA DE MÉTRICAS (OP.MON.2)

- Se redistribuyen de la siguiente forma:
  - 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.

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

SISTEMA DE MÉTRICAS (OP.MON.2)

- 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 »

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

PROTECCIÓN DE PORTÁTILES (MP.EQ.3)

- Ahora:
  - << Los equipos **que abandonen las instalaciones** de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.. >>

- Propuesto:
  - << Los equipos que **sean susceptibles de abandonar** las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.. >>

Universidad Politécnica de Cartagena

BORRADO Y DESTRUCCIÓN (MP.SI.5)

- Modificación de los niveles afectados y de la dimensión afectada:
  - Ahora:

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	=

  - Propuesto: Afecta a la disponibilidad los sistemas con disponibilidad de nivel bajo

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+	=

ANEXO II. MEDIDAS DE SEGURIDAD

BORRADO Y DESTRUCCIÓN (MP.SI.5)

- Pasan a ser de nivel bajo:

  - << La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

  - Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido. >>

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

FIRMA ELECTRÓNICA [MP.INFO.4]

- Se ha modificado completamente su redacción:

  - Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.
  - La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.

  - En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27.

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

FIRMA ELECTRÓNICA [MP.INFO.4]

- Nueva redacción nivel Medio:

  - Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

  - Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

  - **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.

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

COPIAS DE SEGURIDAD (BACKUP) [MP.INFO.9]

- Modificación de los niveles afectados:
  - Ahora:

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

  - Propuesto: Afecta a todos los niveles

dimensiones	D		
Nivel	bajo	medio	alto
	aplica	=	=

Universidad Politécnica de Cartagena

COPIAS DE SEGURIDAD (BACKUP) [MP.INFO.9]

- Se realizarán copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada.

- Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

ANEXO II. MEDIDAS DE SEGURIDAD

Universidad Politécnica de Cartagena

COPIAS DE SEGURIDAD (BACKUP) [MP.INFO.9]

- Las copias de respaldo deberán abarcar:
  - a) Información de trabajo de la organización.
  - b) Aplicaciones en explotación, incluyendo los sistemas operativos.
  - c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
  - d) Claves utilizadas para preservar la confidencialidad de la información.

ANEXO III. AUDITORÍA DE LA SEGURIDAD

Universidad Politécnica de Cartagena

OBJETO DE LA AUDITORÍA

- En las evidencias que permiten sustentar objetivamente el cumplimiento de la auditoría se añade lo siguiente:

  - << Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el Artículo 18 relativo a productos certificados. >>

CONCLUSIONES FINALES

Universidad Politécnica de Cartagena

- Se han cambiado los niveles afectados, de forma tal que en unos casos se “facilita” el cumplimiento (Arquitectura de seguridad-op.pl.2) y en otros casos se añaden medidas nuevas.

- Se definirán “Instrucciones Técnicas de Seguridad” de obligado cumplimiento

  - ¿A qué se refiere la ITS de “Interconexión en el Esquema Nacional de Seguridad”?

CONCLUSIONES FINALES

Universidad Politécnica de Cartagena

- Se “enlaza” el ENS con estándares internacionales y con directivas de la UE. Por ejemplo:
  - En la medida Op.acc.1 (Autenticación) se mapean las valoraciones sobre Autenticidad del ENS con la clasificación del Reglamento de la UE nº 910/2014 sobre transacciones electrónicas seguras,
  - La nueva redacción de la medida mp.info.4 (de firma electrónica); en este último caso, las universidades tendrán que revisar su política de firma (si la tuvieran y si tuvieran algún sistema de nivel medio en Integridad y Autenticidad) para ver que es acorde con la nueva propuesta.

CONCLUSIONES FINALES

Universidad Politécnica de Cartagena

- Ojo al cambio en mecanismos de autenticación para el nivel medio.

- Ojo a disposición transitoria: 24 meses para adecuación a cambios... ¿margen para adecuación al ENS?

CONCLUSIONES FINALES

Universidad Politécnica de Cartagena

- Ojo al cambio en mecanismos de autenticación para el nivel medio.

- Ojo a disposición transitoria: 24 meses para adecuación a cambios... ¿margen para adecuación al ENS?

GRUPO IRIS-ENS

Universidad Politécnica de Cartagena

- **Objetivos principal:** Articular un foro de discusión y de intercambio de información que ayude a aquellas instituciones de RedIRIS para las que resulta de aplicación el ENS.

- **Direcciones de interés:**

  - http://www.rediris.es/cert/tareas/actividades/ens/
  - http://wiki.rediris.es/ens/Portada

- **Últimas normas:**

  - Normativa uso de aulas
  - Normativa de uso de red de comunicaciones

GRACIAS POR SU ATENCIÓN