FESABID'13
XIII JORNADAS ESPAÑOLAS DE DOCUMENTACIÓN
TOLEDO
24 y 25 Mayo 2013
creando valor'es

Evaluación con el Esquema Nacional de Seguridad (ENS): la aplicación en el repositorio institucional de la UAB

Universitat de Barcelona

Miquel Térmens Graells
termens@ub.edu
Universitat de Barcelona
Departament de Biblioteconomia i Documentació

UAB
Universitat Autònoma de Barcelona

Núria Casaldàliga
Nuria.Casaldaliga@uab.cat
Universitat Autònoma de Barcelona. Servei de Biblioteques

Cristina Azorín
Cristina.Azorin@uab.cat
Universitat Autònoma de Barcelona. Servei de Biblioteques

Esta evaluación ha contado con la ayuda del proyecto *El acceso abierto (open access) a la ciencia en España: análisis del grado de implantación y de la sostenibilidad de un nuevo modelo de comunicación científica*. 2012-2014. Plan Nacional I+D+i, código CSO2011-29503-C02-01.

Punto de partida

- El Dipòsit Digital de Documents (DDD) de la UAB es el primero de España y el 16º del mundo en el ranking de repositorios

  (fuente: *Ranking web de repositorios, 2013*. http://repositories.webometrics.info/es)

- El Servicio de Bibliotecas de la UAB tiene interés en mejorar la calidad de sus servicios digitales.
  - ¿Cumple el DDD con los niveles mínimos de seguridad y fiabilidad informática?
  - ¿Podemos asegurar la sostenibilidad del repositorio institucional?

- Las auditorías son un instrumento para evaluar el funcionamiento de un servicio y para su planificación.

El repositorio institucional (DDD)

- Conjunto de servicios prestados a la comunidad universitaria para **recopilar**, **gestionar**, **difundir** y **preservar** la producción científica digital y el fondo patrimonial a través de una **colección organizada**, **de acceso abierto** e **interoperable**.
- Fecha de creación: noviembre 2006
- http://ddd.uab.cat


Documentos
Servidor
Conexión a la red
Estadísticas y logs
Software
Edificio Servicios Informáticos
Sistema de discos

Los instrumentos

- Seguridad de las tecnologías de la información y las comunicaciones:
  - Sistemas de gestión de la seguridad: ISO/IEC 27000...
  - Real Decreto 3/2010: Esquema Nacional de Seguridad (ENS)
- Garantías de preservación digital:
  - TRAC - ISO/IEC 16363:2012
  - Drambora
  - DINI

Posibles niveles de análisis

- Listas (*checklists*) de requerimientos
- Análisis de riesgos informáticos
- Autoinformes de auditoría
- Auditorías de seguridad informática
  - Certificación externa

Esquema Nacional de Seguridad (ENS)

- Normativa:
  - *Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*
  - *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.*
- Norma legal de obligado cumplimiento para las administraciones públicas españolas *"y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general"*.
- Determina:
  - Cómo gestionar la seguridad de los sistemas de información.
  - Cómo hacer un análisis de riesgos.
  - Cómo hacer una auditoría.

Cinco puntos básicos del ENS

1. Confidencialidad: consecuencias en caso de revelaciones no autorizadas
2. Integridad: consecuencias en caso de modificaciones no autorizadas
3. Autenticidad: consecuencias si la información no es auténtica
4. Trazabilidad: consecuencias si no se puede seguir el rastro
5. Disponibilidad: consecuencias si la persona autorizada no puede acceder cuando lo requiere

Josep Matas. "Aspectes legals d'actualitat en relació a les dades i la informació pública". Big data week. 2013

Parámetros básicos de la evaluación

- Presunción de que el DDD no tiene la obligación de aplicar el ENS.
- Aplicación del ENS como instrumento de diagnóstico.
  - Uso de las guías de seguridad publicadas por el Centro Criptológico Nacional-STIC
  - Uso del programa PILAR, versión 5.2.3.
- Clasificación del DDD como un sistema de categoría *Básica*: un fallo de seguridad no compromete derechos o servicios fundamentales para los ciudadanos.
- La evaluación se ha hecho en base a entrevistas y el resultado del estudio es un *Informe de evaluación*, no una *auditoría*.

Plan de trabajo

Realización

- Recogida de información: octubre- noviembre 2012
- Informe: enero 2013

Etapas del trabajo

- Identificación de activos
- Valoración de activos
- Análisis de amenazas
- Análisis de impacto
- Salvaguardas aplicadas
- Cálculo del riesgo residual

Documentación generada

- Informe de evaluación provisional
- Informe de evaluación definitivo

Organización del análisis

- Marco organizativo: política de seguridad, normativa general, procedimientos generales.
- Marco operacional: planificación, control de accesos, explotación.
- Medidas de protección: protección de instalaciones, formación del personal, puestos de trabajo, comunicaciones, protección de los sistemas, protección de la información.

Deficiencias detectadas (I)

Marco organizativo

control	[nivel actual]	[requerido por ENS]
[org] Marco organizativo	L0-L3	L2
[org.1] Política de Seguridad	L0-L3	L2
[org.2] Normativa de seguridad	L3	L2
[org.3] Procedimientos de seguridad	L0	L2
[org.4] Proceso de autorización	L3	L2

Deficiencias detectadas (II)

Marco operacional

control	[nivel actual]	[requerido por ENS]
[op] Marco operacional	L0-L4	L2
[op.pl] Planificación	L2-L4	L2
[op.pl.1] Análisis de riesgos	L3	L2
[op.pl.2] Arquitectura de seguridad	L2-L4	L2
[op.pl.3] Adquisición de nuevos componentes	L2	L2
[op.acc] Control de acceso	L0-L4	L2
[op.acc.1] Identificación	L2-L4	L2
[op.acc.2] Requisitos de acceso	L3	L2
[op.acc.4] Proceso de gestión de derechos de acceso	L3-L4	L2
[op.acc.5] Mecanismo de autenticación	L0-L3	L2
[op.acc.6] Acceso local (local logon)	L0-L2	L2
[op.acc.7] Acceso remoto (remote login)	L0-L3	L2
[op.exp] Explotación	L2-L4	L2
[op.exp.1] Inventario de activos	L4	L2
[op.exp.2] Configuración de seguridad	L3	L2
[op.exp.4] Mantenimiento	L2-L3	L2
[op.exp.6] Protección frente a código dañino	L2-L4	L2

Deficiencias detectadas (III)

Medidas de protección

control	[nivel actual]	[requerido por ENS]
[mp] Medidas de protección	L0-L5	L2
[mp.if] Protección de las instalaciones e infraestructuras	L4	L2
[mp.if.1] Áreas separadas y con control de acceso	L4	L2
[mp.if.2] Identificación de las personas	L4	L2
[mp.if.3] Acondicionamiento de los locales	L4	L2
[mp.if.4] Energía eléctrica	L4	L2
[mp.if.5] Protección frente a incendios	L4	L2
[mp.if.7] Registro de entrada y salida de equipamiento	L4	L2
[mp.per] Gestión del personal	L2	L2
[mp.per.2] Deberes y obligaciones	L2	L2
[mp.per.3] Concienciación	L2	L2
[mp.per.4] Formación	L2	L2
[mp.eq] Protección de los equipos	L2	L2
[mp.eq.1] Puesto de trabajo despejado	L2	L2
[mp.com] Protección de las comunicaciones	L3	L2
[mp.com.3] Protección de la autenticidad y de la integridad	L3	L2
[mp.si] Protección de los soportes de información	L0-L4	L2
[mp.si.1] Etiquetado	L0	L2
[mp.si.3] Custodia	L3	L2
[mp.si.4] Transporte	L4	L2
[mp.info] Protección de la información	L3-L5	L2
[mp.info.6] Limpieza de documentos	L3	L2
[mp.info.9] Copias de seguridad (backup)	L5	L2

ENS como metodología de autoevaluación

- **Sí** es adecuado el modelo PDCA (Plan-Do-Check-Act): planifica, haz, comprueba y actúa.
  - Los procedimientos de seguridad no siempre están documentados, aunque se lleven a la práctica de forma intuitiva.
  - Las medidas de seguridad en la mayoría de casos se aplican a TODA la Universidad.
  - Es difícil delimitar la infraestructura del repositorio
  - Debe haber designación de roles

Seguridad del DDD

- **Sí** dispone de medidas adecuadas de seguridad acordes con su categoría, aunque presenta algunas deficiencias:
  - Establecimiento formal de los responsables del repositorio (de la seguridad, de los datos y del servicio)
  - Redacción de unos procedimientos específicos
  - Fomentar una mayor difusión de las medidas de seguridad entre el personal implicado en la gestión del repositorio.

Próximos pasos

- Realización de una evaluación profunda de preservación digital según ISO/IEC 16363:2012
  - ¿El DDD además de seguro está preparado para ser preservado a largo plazo?
- Realización de nuevas evaluaciones según ENS de otros repositorios institucionales.
  - Se buscan candidatos

¡Gracias por la atención!

Miquel Térmens Graells

termens@ub.edu

Dipòsit Digital de Documents de la UAB

ddd.bib@uab.cat