Seguridad Proactiva en los Sistemas de Gestión e Información académica: el caso de la UNLP

Francisco Javier Díaz[a,b], María Alejandra Osorio[a], Paula Venosa[a,c], Nicolás Macia[b,c], Paola Amadeo[b,c]

[a] CeSPI, Universidad Nacional de La Plata
Calle 50 y 115 La Plata
Buenos Aires, Argentina
[jdiaz | aosorio | pamadeo] @cespi.unlp.edu.ar

[b] CERT, Universidad Nacional de La Plata
Calle 50 y 115 La Plata
Buenos Aires, Argentina
[pvenosa | nmacia]@cert.unlp.edu.ar

[c] LINTI, Facultad de Informática, Universidad Nacional de La Plata
50 y 120 La Plata
[jdiaz | pvenosa | nmacia | pamadeo] @info.unlp.edu.ar

Resumen. A partir de la incorporación del sistema de gestión académica SIU Guaraní en la UNLP en el año 2004, surgió un ecosistema de soluciones informáticas que posibilitaron que alumnos, docentes, nodocentes y autoridades sean usuarios intensivos de los sistemas de gestión de la información 7x24. Este cambio causó que decenas de miles de usuarios utilicen los sistemas de la UNLP en forma extensiva y extendió también la posibilidad de incidentes de seguridad. Esto evidenció la necesidad de contar con una estrategia que permita atender y mitigar los incidentes que ocurran y disparar una serie de actividades preventivas que reduzcan la posibilidad de existencia de brechas de seguridad, que puedan ser explotadas en forma intencional.

Desde el año 2009 el CeSPI se incorporó a la cultura de la gestión calidad mediante la certificación ISO9001:2008 de los servicios informáticos que brinda, asegurando el mejor servicio y motivando planes de mejora continua de los sistemas de gestión e información. Además, para trabajar los distintos tipos de incidentes de seguridad en la red y los servicios académicos, el CeSPI implementa el CERT en el año 2008 y participa en eventos relacionados de LACNIC, el Proyecto Amparo y en los coloquios técnicos de FIRST. En lo que respecta a la Seguridad Informática, el CeSPI desde el año 2007 brinda certificados digitales para e-ciencia a través de una PKI registrada en TACAR, reconocida por TAGPMA e IGTF.

Se incorpora la prevención y corrección de fallas de seguridad como etapa previa a la puesta en producción de los nuevos servicios así como un escaneo mensual de las diferentes prestaciones a fin de detectar vulnerabilidad. Entre los servicios de prevención se han realizado tests de seguridad sobre sistemas desarrollados por el Consorcio SIU de Universidades Nacionales de Argentina. La gestión de estos servicios fue incorporada al certificado ISO9001:2008 en el año 2012: la cultura de la calidad incorpora la visión de la seguridad preventiva. Esto ha dado lugar naturalmente a la incorporación de más servicios como el diagnóstico realizado por el CERT sobre las redes de los miembros del NAP La Plata de CABASE. Además, se evolucionó en la capacitación planteando cursos de seguridad en la Academia CeSPI al actual Centro de Excelencia del ITU en ciberseguridad.

Palabras Clave: calidad, gestión, ISO 9001, seguridad, CERT, pentest.

1 La UNLP y sus servicios informáticos

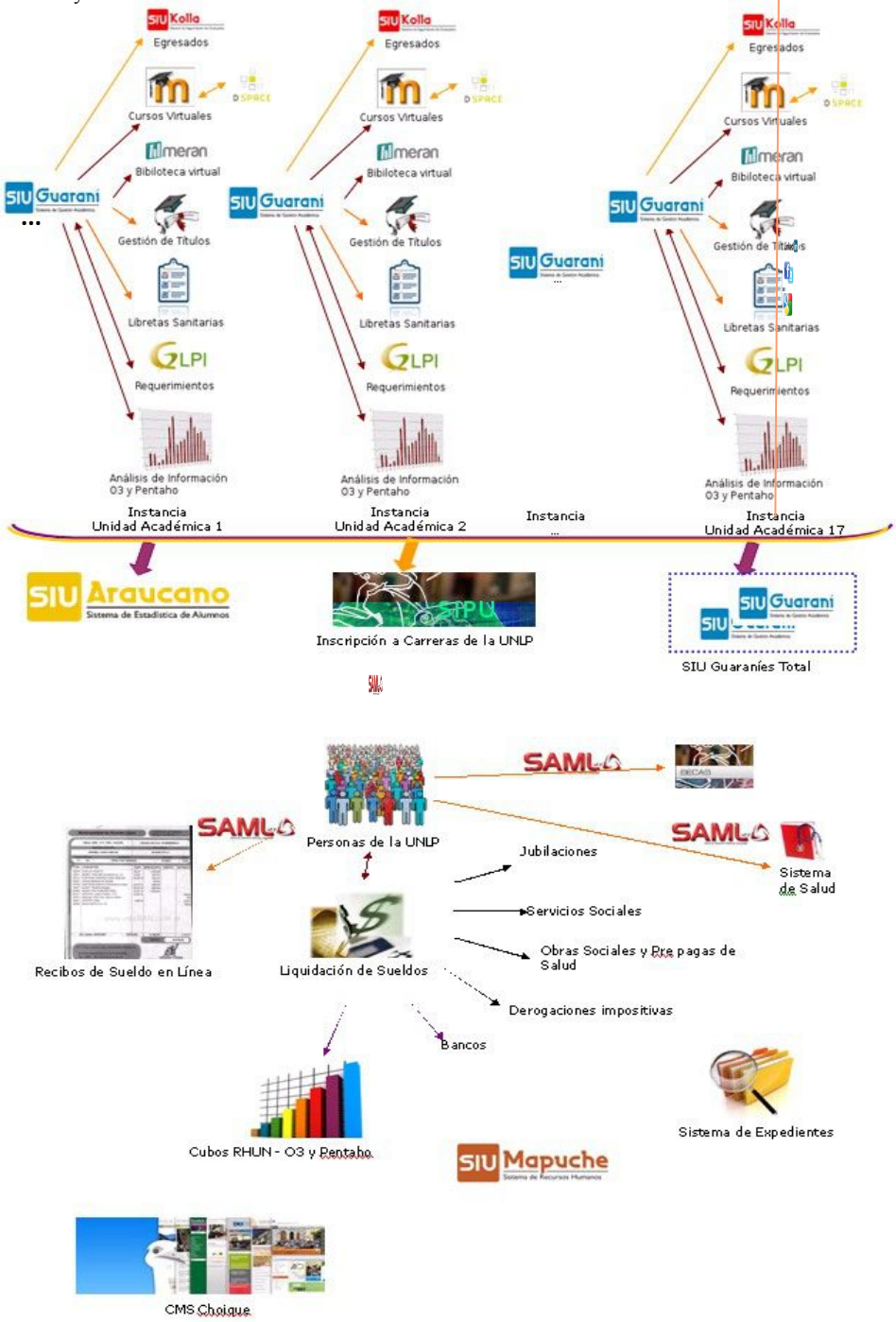
La Universidad Nacional de La Plata es la institución de educación superior pública, de Argentina, 2° en el país en cantidad de alumnos [1]. Fundada en 1905, incluye 18 unidades académicas, 4 escuelas de pre-grado, 154 centros de investigación, 8 secretarias y más de 30 direcciones que dependen del Rectorado y permiten la gestión de más de 111.000 alumnos de grado, 10.126 de postgrado, 12.000 docentes y más de 3.000 administrativos [2] Sus 110 carreras de grado y 187 de postgrado involucran desde las ciencias sociales y humanas, como Ciencias Jurídicas y Sociales y Licenciatura en Griego, hasta Ingeniería Aeronáutica,

Ingeniería en Computación y Licenciatura en Física y en Informática, pasando por las ciencias biológicas y ciencias de la salud, como las carreras de Ciencias Médicas, Odontología y Licenciatura en Biología, Ecología, Licenciado en Biotecnología y Ciencias de la Comunicación. Asimismo la Universidad cuenta con 2 observatorios, 8 museos, 1 albergue universitario, 3 comedores universitarios entre otras dependencias que engloban y constituyen a la UNLP.

El Centro Superior para el Procesamiento de la Información (CeSPI) es el centro de servicios informáticos de la UNLP. Su misión es *Propiciar el uso y apropiación de las Tecnologías de la Información y Comunicación y los cambios sociales necesarios para su aprovechamiento, que contribuyan a mejorar las funciones de educación, investigación científica y tecnológica y extensión universitaria que desarrolla la Universidad Nacional de La Plata; aportando a una sociedad sostenible social y ambientalmente* [3] Creado en 1959, su función es colocar a la tecnología al servicio de la Institución. En el Centro se realizan las tareas relacionadas con los distintos sistemas que brindan servicios a la Universidad. Estos sistemas comprenden la liquidación de sueldos de los empleados, el manejo curricular de los alumnos de las respectivas unidades académicas y servicios asociados como plataformas virtuales, gestión de becas, gestión de libretas sanitarias, pre inscripción a las carreras de grado y los colegios dependientes de la universidad; y la tarea que sostiene éstas actividades: la administración y el soporte técnico de la red de datos, los servicios de Internet y la propia infraestructura del Centro.

En la figura 1 se representan los servicios informáticos ofrecidos y la integración entre ellos[4]:

Fig. 1 – Integración de sistemas, desarrollados y/o mantenidos por el CeSPI, utilizando web services (flechas naranjas) o intercambio de archivos (flechas violetas). Todos estos sistemas generan información que se consolida en distintos repositorios: Guaraní Total para alumnos y Personas UNLP para alumnos, docentes y no docentes. Se relacionan con redes sociales.



En el CeSPI funciona CERTunlp , el CERT académico cuyo ámbito de aplicación es la Red de la Universidad Nacional de La Plata. El mismo fue creado en el marco de la política de calidad del CeSPI, con el propósito de prevenir, detectar, analizar, investigar, registrar los incidentes de seguridad que son reportados.

A partir de la creación de CERTunlp [5], y las tareas realizadas por el mismo, los incidentes de seguridad se gestionan de una forma ordenada y sistemática acelerando la rapidez y eficiencia de las respuestas con el fin de minimizar la pérdida de la información y la calidad e interrupción del servicio.

Dentro de los servicios que un CERT puede brindar [6], además de aquel ya mencionado de tratamiento de incidentes de seguridad, CERTunlp presta servicios reactivos: avisos y alertas; tratamiento y análisis forenses y servicios proactivos: auditoría de red, auditoría de sistemas/aplicaciones, monitoreo, detección de intrusiones. Asimismo se prestan servicios de calidad en la seguridad como son la consultoría y la concientización en seguridad de la Información.

Cabe destacar que, además de los servicios mencionados en el párrafo anterior, el hecho de formar parte de la comunidad de expertos y realizar aportes en la misma es también un objetivo de CERTunlp, el cual trae aparejado la inversión de tiempo y esfuerzo en actividades afines.

A fin de cumplir con el objetivo mencionado, los miembros de CERTunlp participan de la comunidad de LAC-CSIRTs, la cual reúne CERTs de América Latina y el Caribe. Esta participación se concreta no sólo siguiendo foros, asistiendo a reuniones y eventos como ser las instancias de capacitación del proyecto AMPARO, el LACSEC donde se presentan temas actuales de seguridad o el FIRST Technical Colloquium, sino también organizando y coordinando encuentros virtuales donde se intercambia información, ideas y se definen líneas de trabajo en común.

Cabe mencionar también que el equipo de CERTunlp participa anualmente de las capacitaciones y encuentros que organiza OWASP, como son las instancias de los OWASP LaTours realizados los últimos años.

En lo que respecta a la Seguridad Informática, el CeSPI desde el año 2007 brinda certificados digitales para e-ciencia a través de una PKI registrada en TACAR, reconocida por TAGPMA e IGTF[7].

2 Calidad en los sistemas de gestión e información académica

En el CeSPI, de un tiempo a esta parte, se produce un cambio en la manera de trabajar y de relacionar las diferentes áreas de la institución, fomentando el trabajo en equipo y la interrelación entre las mismas. La demanda de servicios de distinta índole y criticidad, como sistemas de software para la gestión académica, de becas, de libretas sanitarias, de soporte para la toma de decisiones, de soporte tecnológico y consultoría entre otros, a nivel nacional e internacional, también aumentó en forma considerable. Se hizo necesario entonces contar con una herramienta de validez internacional, de probada eficacia que facilite el desarrollo y mantenimiento de un sistema de gestión controlado y disciplinado. Es así como se comenzó en el año 2007

con la capacitación del personal y directivos en las posibilidades y limitaciones de las normas de calidad existentes a nivel internacional, resultado la norma ISO 9001:2008 la más adecuada a la realidad de la institución.

En el año 2009 el CeSPI implementa el Sistema de Gestión de Calidad y alcanza la certificación ISO 9001:2008 para dos procesos:

- Gestión de Requerimientos de Servicios e Información de Sistemas Académicos.
- Servicios de Consultoría y Auditoría Tecnológica.

La entidad certificadora es TÜV Rheinland[8], organismo de certificación e inspección de origen alemán y presencia internacional en más de 61 países y 130 años de experiencia en certificación de calidad, seguridad y medio ambiente.

Se han superado tanto las auditorías internas como las externas de certificación, seguimiento y re-certificación de la norma ISO 9001:2008, con acreditación a nivel nacional OAA (Organismo Argentino de Acreditación) e internacional a través de TGA/DAX Organismo Alemán de Acreditación DAX y IATF: International Automotive Task Force.

Tras seis años de trabajo en la cultura de la calidad, claramente se puede ver una mejora en los servicios ofrecidos así como una mejor sistematización, mejora en la imagen y en la percepción del trabajo realizado. Además, la cultura de la calidad que se instala motiva además para incorporar nuevos aspectos como la seguridad, la reducción del impacto ambiental, la reducción de consumo energético o actividades vinculadas con la comunidad, por ejemplo con derechos humanos o cuestiones de no discriminación o reducción de la brecha digital, que actualmente son denominadas de responsabilidad social.

Es así como en el año 2012 el alcance se amplía a dos procesos:

- Gestión de Requerimientos de Sistemas Académicos, de Seguridad de la Información y de Minería y Análisis de Datos.
- Servicios de Auditoría y Consultoría Tecnológica.

El nuevo alcance pone el foco en la Seguridad de la Información, incluyendo un proceso propio, procedimientos y una metodología particular para dar un curso efectivo a los requerimientos de esta índole.

3 El sub alcance “Requerimientos de auditorías de seguridad de sistemas y Q&A”

El CERTunlp brinda servicios proactivos relacionados con la evaluación periódica de seguridad de redes, servidores y servicios y Pentest de aplicaciones Web. Sobre esta última prestación se ha certificado ISO 9001:2008 como un sub alcance, definiendo un proceso propio, con sus procedimientos y registros, que se describen la próxima sección.

Los servicios proactivos realizados por CERTunlp son:

● Evaluación periódica de seguridad de redes, servidores y servicios: CERTunlp, realiza periódicamente sobre la red del CeSPI, auditorías de seguridad de red, servidores y servicios, para detectar servicios activos no autorizados, configuraciones inadecuadas, vulnerabilidades en servicios, sistemas operativos obsoletos, filtros de acceso insuficientes y otros problemas de seguridad similares.
Para la tarea descripta, se utiliza principalmente la herramienta Nessus [9].

Las auditorías de red también tienen en cuenta vulnerabilidades nuevas. Por ejemplo, en el año 2014 se incorporaron testeos para evaluar posibles problemas de Poodle [10], heartbleed [11] y shellshock[12]. Estos testeos también formaron parte de auditorías realizadas en el marco de trabajos de consultoría, como ser el diagnóstico realizado por el CERTunlp para miembros del NAP La Plata de CABASE[13].

● Pentests de aplicaciones web: CERTunlp, realiza pruebas de penetración sobre aplicaciones Web desarrolladas en la organización. Estas pruebas permiten identificar problemas de seguridad, tanto en la configuración como en el desarrollo de tales sistemas.

El proceso se lleva a cabo en la fase de pruebas antes de su entrada a producción e implica la realización de una serie de chequeos basados en recomendaciones de OWASP [14][15][16][17].

La sistematización de las solicitudes de servicios de Pentest de aplicaciones Web, incluidas dentro del alcance Requerimientos de Sistemas Académicos, de Seguridad de la Información y Minería y Análisis de Datos, se pueden ver reflejadas en la figura 2:

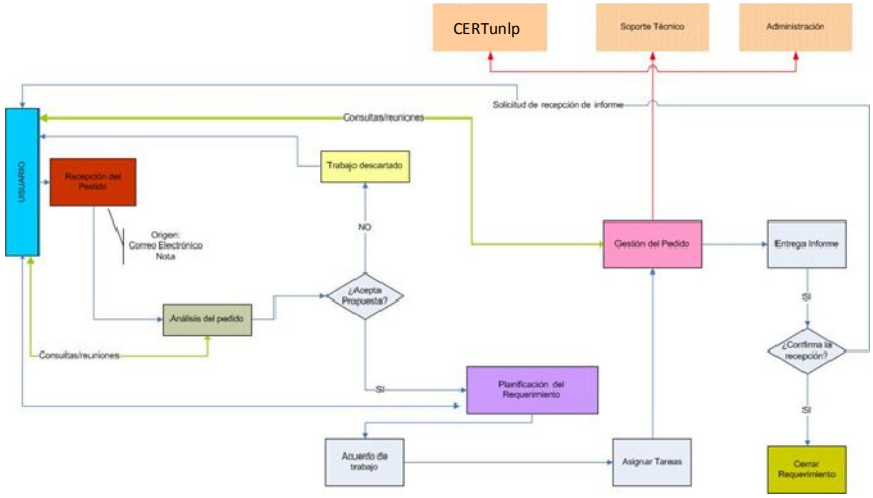


Fig. 2 – Diagrama de Procesos. Sub alcance Requerimientos de Seguridad y Q&A

El personal responsable del Pentest recibe la solicitud de un usuario habilitado, vía correo electrónico o nota. Este pedido se analiza y se realizan reuniones con el usuario para definir el objetivo, los activos y el alcance, así como también los requisitos para llevar a cabo el pedido, sin lugar a dudas. El pedido se registra en un sistema de gestión de incidentes, el GLPI.

Se confecciona el acuerdo de trabajo, firmando un formulario de autorización de los trabajos de auditoría de seguridad junto con el tipo de pruebas cuya realización se solicitará a CERTunlp.

Estas pruebas están relacionadas a distintos aspectos de seguridad que pueden evaluarse, teniendo en cuenta la naturaleza de la aplicación y tomando como base el OWASP Top Ten.

Pensando en los chequeos habituales, podemos agrupar las vulnerabilidades que se analizan teniendo en cuenta los atributos o aspectos de la aplicación con los que se relacionan, y podemos decir que el pentest analiza básicamente:

- Protección de sesiones de usuario: problemas en el manejo de sesiones, problemas en atributos de cookies, fijación de cookies de sesiones, fallas de inyección en formularios de autenticación, problemas en el almacenamiento criptográfico, problemas en el manejo del cambio de contraseñas, falla en las políticas de contraseña, problemas de fuerza bruta, problemas de encripción de las comunicaciones.

- Protección de información en Base de datos: inyecciones SQL, problemas en el almacenamiento criptográfico, problemas de encriptación de las comunicaciones.

- Protección de los usuarios y sus transacciones: CSRF, fallas de inyección XSS, problemas de encriptación de las comunicaciones, problemas de Phishing, Problemas de DOS, uso de forwards y redirects sin validar.

- Protección de la Aplicación: referencia insegura de objetos, configuración de seguridad inadecuada, revelación innecesaria de información, problemas de DOS, Inclusión de archivos local y remota, ejecución de código, falla en la restricción de URL de accesos

- Protección del Servidor: puertos abiertos innecesarios, protocolos habilitados innecesarios, análisis de servicios y versiones utilizadas, existencia de política de firewall, problemas de DOS.

El responsable mantiene una comunicación adecuada con el soporte y con el usuario requirente, para ir resolviendo las distintas instancias que puedan presentarse en este proceso. Finalmente se confecciona el informe final que se entrega al usuario que solicitó el trabajo, previa firma del comprobante de recepción del pedido.

El trabajo del área incluye, entre otras, la realización de test de seguridad para todas las aplicaciones desarrolladas por el CeSPI, algunas de las cuales han soportado más de 9000 inscripciones a materias en una hora y más de 18000 mil en un día pico, en el caso de sistemas académicos durante el año 2014, sin registro de incidentes de

seguridad. También permitieron la gestión de más de 7000 inscripciones a colegios de la UNLP en un día, para el año 2015.

4 Resultados Obtenidos

En base a la recepción periódica de las evaluaciones de seguridad sobre las redes, servidores y servicios del CeSPI, se pudo atacar inicialmente los problemas más críticos y luego atacar el resto de los problemas que implican algún tipo de riesgo.

Actualmente los reportes resultantes de los testeos muestran que debilidades de seguridad descubiertas tienen un nivel de riesgo aceptable, por lo que se los puede empezar a evaluar en función de los cambios observados respecto del análisis anterior.

La experiencia obtenida en la implementación de servicios de seguridad prestados por CERTunlp en el ámbito académico, es aprovechada en la producción de material y armado de ejercicios prácticos de las materias de grado y postgrado de Seguridad y Privacidad en Redes, así como de distintos cursos de Postgrado que se dictan en la Facultad de Informática de la UNLP, en particular los cursos "Seguridad en Redes" "Conceptos avanzados de Seguridad Informática" impartidos en el marco del Doctorado en Ciencias Informáticas.

La experiencia en detección y prevención de incidentes de seguridad no sólo se aplica al anterior de la UNLP sino también a distintas aplicaciones del consorcio SIU de Universidades Nacionales. Asimismo se ha trabajado en el sistema de voto electrónico del Conicet y otros organismos

Cabe destacar también que el conocimiento adquirido en la participación en los procesos, enriquecerá las capacitaciones a brindar por la UNLP como Centro de Excelencia de la ITU en ciberseguridad para el período 2015-2018.

Conclusiones

La certificación de calidad permitió estandarizar los procesos de atención, y al incorporar servicios de seguridad a los mismos a través del pentesting, se mejoraron los niveles de seguridad de los sistemas que acompañan dichos procesos de atención que brinda el CeSPI a sus usuarios.

Además, los servicios continuos de auditoría de seguridad de la red posibilitan el seguimiento del estado de la seguridad en la misma, de manera tal de disminuir los niveles de riesgo en la organización y permitiendo priorizar los problemas en función del riesgo para su mitigación en tiempo y forma.

Al tener implementado un sistema de gestión de calidad, contando con la certificación ISO 9001:2008 para los procesos: Gestión de Requerimientos de Servicios e Información de Sistemas Académicos y Servicios de Consultoría y Auditoría Tecnológica y contar con un CERT en funcionamiento: CERTunlp, el

CeSPI, ya tiene recorrido gran parte del camino hacia la implementación de un Sistema de Gestión de Seguridad de la Información, en sintonía con la ISO 27001 [19][20].
Asimismo, la integración de aspectos de seguridad a la certificación compromete a incluir la seguridad informática en los planes de capacitación y en los planes de mejora continua de los sistemas.

Agradecimientos

Los autores desean expresar su agradecimiento a la Lic. Dalila Romero y Luján D'Alessandro por su participación en la certificaciones de calidad.

Referencias

1. Anuario Estadístico Secretaría de Políticas Universitarias. Ministerio de Educación de la Nación - 2012 http://informacionpresupuestaria.siu.edu.ar/DocumentosSPU/diu/anuario_2012.pdf
2. Indicadores Estadísticos UNLP. http://www.unlp.edu.ar/indicadores
3. CeSPI UNLP. http://cespi.unlp.edu.ar
4. Díaz, Osorio, Amadeo (2012) Hacia un Sistema de Información Integrado en la Universidad Nacional de La Plata. Argentina Una caso de estudio. Anales de la Conferencia TICAL 2012. http://tical_2012.redclara.net/es/presentaciones.html
5. Díaz, Venosa, Lanfranco, Macia (2009) Definición e Implementación de un Centro de Atención de Incidentes (CERT) para un Ámbito Universitario anales de CACIC 2009, Universidad Nacional de Jujuy, octubre 5 al 9 de 2009 - ISBN 978-897-24068-4-1 .
6. http://www.proyectoamparo.net/files/manual_seguridad/manual_basico_sp.pdf
7. Dova M. Grunfeld C. Monticelli F. Tripiana M. Veiga A. Ambrosi V. Barbieri A. Díaz J. Luengo M. Macia N. Molinari L. Venosa P. Zabaljáuregui M. Progress of Grid Technology in Argentina: Lessons Learned from EELA. Anales de la III conferencia de EELA, Catania, pp.225-232. ISBN: 978-84-7834-565-6 http://www.eu-eela.org/3_conference/index.html
8. TÜV http://www.tuv.com/es/argentina/home.jsp
9. http://www.tenable.com/products/nessus-vulnerability-scanner
10. https://www.us-cert.gov/ncas/alerts/TA14-290A
11. http://heartbleed.com/
12. https://shellshocker.net/
13. http://www.cabase.org.ar/wordpress/nap-la-plata/
14. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
15. https://www.owasp.org/index.php/Cheat_Sheets
16. https://www.owasp.org/index.php/Category:OWASP_Testing_Project
17. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
18. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems – Requirements
19. ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005)