Definición e Implementación de un Centro de Atención de Incidentes (CERT) para un Ámbito Universitario

Mauricio Foster[1], Einar Lanfranco[2], Nicolás Macia[2], Paula Venosa[2], Lía Molinari[2], Javier Díaz[2]

[1] CesPI, Centro Superior del Procesamiento de la Información, Universidad Nacional de La Plata, calle 50 y 115, La Plata, Buenos Aires, Argentina
{mfoster, nmacia}@cespi.unlp.edu.ar
[2]LINTI, Laboratorio de Investigación en Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad Nacional de La Plata, calle 50 y 120, La Plata, Buenos Aires, Argentina
{pvenosa, lmolinari, javierd}@info.unlp.edu.ar

Abstract. En el presente artículo se describe la experiencia adquirida en la implementación de un CERT[1] académico en el ámbito de la Universidad Nacional de La Plata, proyecto que se define a partir de la necesidad de dar respuesta a los incidentes de seguridad que aumentan día a día, teniendo en cuenta la naturaleza de nuestro entorno de trabajo. En la etapa inicial del proyecto se realizaron diversas tareas relacionadas con la definición de objetivo y alcance de nuestro CERT, el establecimiento de procedimientos básicos de trabajo, el armado del equipo de trabajo, la evaluación de las herramientas de apoyo a utilizar y los mecanismos para difundir el nacimiento de este equipo de trabajo, haciendo uso de las mejores prácticas y estándares recomendados.

Keywords: CERT, CSIRT, administración de incidentes, administración de problemas, ITIL

1 Introducción

Un CERT, también conocido como CSIRT[2], es una organización que provee servicios y soporte para prevenir, manejar y dar respuesta a los incidentes de seguridad de la información que ocurren en el ámbito en el cual el CERT trabaja[1]. Presta los servicios necesarios para ocuparse de estos incidentes y ayudar a los damnificados a recuperarse después de sufrir uno de ellos.

Con la aparición de Morris, el primer gusano importante a fines de los ’80 que se propagó rápidamente y logró infectar gran cantidad de equipos a lo largo de todo el mundo, los administradores de sistemas, y gestores de la tecnología de la información, vieron la necesidad de cooperar entre sí, y coordinarse de manera de poder enfrentarse

[1] CERT: Computer Emergency Response Team
[2] CSIRT: Computer Security Incident Response Team

a este tipo de casos. Sin duda, éste fue un paso decisivo para establecer un enfoque común y más organizado en el tratamiento de los incidentes relacionados a la seguridad de la información.

Poco después de este incidente, se crea el primer CSIRT: el CERT Coordination Center (CERT/CC), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania). Poco después el modelo se adoptó en Europa, y en 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnet-CERT. Desde entonces el número de equipos de similares características, ha ido en paulatino aumento, y su distribución ya incluye a muchos países del mundo.

UNLP CERT tiene como misión ser un Centro de Respuestas de Incidentes de Seguridad Académico en el ámbito de la Universidad Nacional de La Plata.

1.1 Ambito de aplicación

El ámbito de operación de CERT-UNLP es el CeSPI[3] que administra la intranet de la Universidad Nacional de La Plata [2]. La Universidad cuenta con 18 facultades donde estudian alrededor de 90000 alumnos. De ella dependen cinco Colegios Preuniversitarios con una matrícula aproximada de 5000 alumnos[4].

En el ámbito universitario se hace uso tanto de servicios internos como de servicios externos. A las actividades de docencia e investigación antes citadas, se suman las pertinentes a las tareas técnicas y administrativas que realiza el personal no docente; las propias de los alumnos, que también son usuarios de los servicios de la UNLP, y las de mantenimiento y administración de la red misma para acceder a recursos de Internet.

El personal asociado a tareas de docencia es de más de 10000, gran parte de los cuales 3500 conducen tareas de investigación en 141 centros ó laboratorios. Debe tenerse en cuenta también, que se realiza un uso masivo de la tecnología, ya sea estableciendo comunicación por mail, videoconferencia, aplicaciones distribuidas o utilizando entornos virtuales de aprendizaje que demandan un servicio de calidad en cuanto a tecnología informática y comunicaciones. [3]

La red informática de la UNLP desde la cual se desarrollan las actividades hasta aquí descriptas, es cada vez más extensa. En la actualidad, se estima que la misma cuenta con más de 5000 equipos (computadoras de usuarios, servidores, equipos de red, impresoras, entre otros) distribuidos entre las dependencias.

En cada una de estas dependencias la administración de los recursos informáticos se lleva a cabo de manera descentralizada, es decir que cada una de ellas es responsable de velar por sus recursos como ser servicios, servidores, seguridad perimetral, PCs de usuario final, análisis de vulnerabilidades, etc. Esta actividad implica una enorme cantidad de consideraciones a tener en cuenta de manera tal de poder proveer continuidad de servicios, integridad de la información, entre otros.

A modo gráfico, lo antes descripto puede visualizarse en la siguiente figura:

---

[3] CeSPI: Centro Superior de Procesamiento de la Información de la Universidad Nacional de La Plata

[4] Anuario estadístico 2008-UNLP

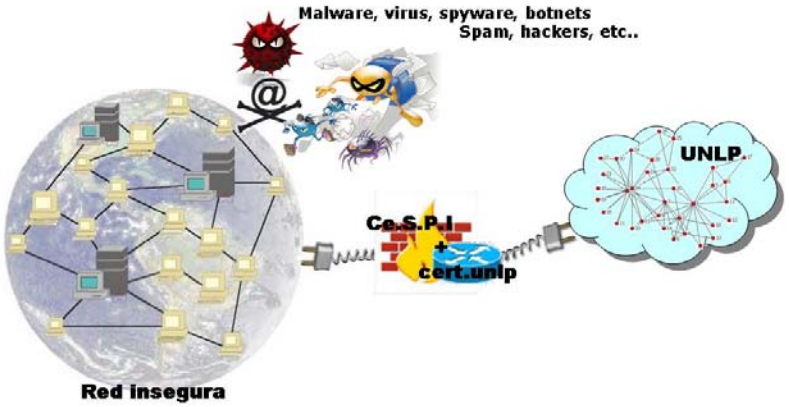

Fig. 1. Cert.unlp en la Red

En la UNLP, el servicio de conexión a la red pública (“Internet”) es brindado históricamente por el CeSPI.

Cada red cuenta con personas encargadas de realizar las tareas de administración de los recursos informáticos. Estas tareas implican tanto la funcionalidad, como la seguridad. Teniendo en cuenta la diversidad de tamaños, tecnologías, disponibilidad de recursos, necesidades, la cooperación entre todas estas redes, las tareas que tienen que ver con la cooperación de los distintos administradores, se convierte en una cuestión por demás complicada.

Considerando además, a la UNLP como un único organismo que debe responder ante cualquier inconveniente ó incidente provocado desde ó hacia cualquier equipo ubicado en cualquiera de las redes que la componen, se hacía cada vez más necesaria la existencia de un grupo referente en temas relacionados a seguridad informática en el cual, los distintos equipos puedan sustentarse, buscar apoyo técnico, una base de conocimientos, intercambiar experiencias. Como una necesidad de colaboración entre los administradores de las distintas dependencias de la UNLP, se ha creado una lista de administradores de red y servicios en donde varias de las personas encargadas de los servicios de infraestructura y comunicaciones de las dependencias de la UNLP pueden hacer algún tipo de intercambio de conocimientos, dudas, experiencia, etc.

Otra pauta de la necesidad de colaboración e intercambio de información y experiencias, es la creación de un repositorio de archivos en el cual, cualquier persona puede encontrar versiones de sistemas operativos del tipo OpenSource, parches o actualizaciones de productos de software entre otros tantos recursos de interés para los administradores de redes.

Todo ésto, sumado al creciente número de incidentes que se reportan, sugiere la necesidad de tomar cartas en el asunto, y de empezar a tomar medidas proactivas. Se estima que los incidentes serán mayores con el pasar del tiempo acorde con la evolución de la tecnología de las comunicaciones y la creciente disponibilidad de herramientas destinadas a fines dañinos.

Teniendo en cuenta lo expuesto, se decide la creación de un grupo especializado en temas relacionados a la seguridad de la información.

2 Objetivos

Según los lineamientos que aporta ITIL[5], la operación de un servicio es parte del ciclo de vida del servicio: es responsable por permitir que se ejecuten procesos optimizando el costo y la calidad de dichos servicios. Es, por lo tanto, responsable por el funcionamiento efectivo y para definir esa efectividad debe conocerse cuáles son los objetivos que tiene la organización en el uso de la tecnología.
De acuerdo a las actividades que se realizan en la UNLP, vemos que los 7 criterios que enuncia COBIT6 (efectividad, eficiencia, confidencialidad, cumplimiento, disponibilidad, integridad, confiabilidad) se deben respetar ya sea demanda primaria o secundaria.

Por ejemplo, la administración de los entornos de aprendizaje virtuales tendrá una fuerte exigencia en cuanto a disponibilidad, efectividad y confiabilidad. Si tenemos en cuenta que allí se publican resultados de exámenes, la confidencialidad es un criterio que también debe respetarse.

Otras actividades pueden no tener una demanda de disponibilidad primaria, pero si la exigencia por alguno de los otros criterios.

La administración de servicios trata sobre mantener y mejorar los servicios de tecnología informática (de ahora en más TI) definiendo, negociando y administrando los niveles de servicio. La administración de la disponibilidad asegura que los servicios sean provistos según acuerdos de servicio establecidos. La mayoría de las veces estos acuerdos no existen formalmente, y queda sujeto a lo que el proveedor cree que es el valor del servicio.

Al ser el proveedor del servicio un equipo perteneciente a la UNLP, se conoce el valor del activo que se está manejando.

Este equipo, que cuenta con experiencia académica en el área de seguridad (son docentes e investigadores en el área, ver [4] y [5]), conoce los objetivos de la organización y que el buen uso de las TICs es estratégico.

UNLP CERT tiene como principal objetivo brindar servicios de atención, manejo y respuesta de incidentes de seguridad en las siguientes áreas de la red de la Universidad Nacional de La Plata:

- Monitoreo de seguridad del Backbone de la red.
- Monitoreo de uso de la red según políticas de uso razonable.
- Deployment de red de sensores de seguridad y tecnologías de Honeypots en distintos segmentos de red de la UNLP.
- Continuidad de los servicios de red de las distintas unidades académicas de la UNLP, definidos en el registro de servidores.
- Servicios propios:
    - Infraestructura PKI de la UNLP: http://www.pkigrid.unlp.edu.ar

[5] InformationTechnology Infrastructure Library
[6] Control Objectives for Information and related Technology

    - Sistema de gestión de Alumnos (SIU Guaraní): http://www.guarani.unlp.edu.ar
- Diagnósticos de seguridad proactivos, según pautas acordadas con cada dependencia.
- Entrega en forma oportuna y sistemática de información sobre vulnerabilidades de seguridad, amenazas, prevención y resolución de incidentes de seguridad.
- Capacitación sobre temas de seguridad y uso seguro de la tecnología..

El análisis para el armado de un Centro de Respuesta de incidentes, conjuga una serie de variables por demás importantes las cuales deben ser tenidas en cuenta de manera de tomar las decisiones correctas, y no llevar el proyecto a un fracaso. Toda esta información, se describe con detalle en el gran número de documentos existentes que se refieren a los mecanismos, pasos necesarios y decisiones a ser tomadas al momento de crear un CSIRT.

Definiciones

A los efectos de acordar el alcance de este proyecto se hizo necesario establecer una serie de definiciones. A modo de ejemplo se citan algunas de ellas.

Vale aclarar que las definiciones se han extraído de estándares, lineamientos y buenas prácticas internacionales.

Amenaza: Cualquier actividad relacionada con alguna variación o forma de participación en las siguientes cuestiones:

- Botnets
- Malware: Virus / Troyano / Spyware / Gusano
- Denegación de Servicios
- Scanning
- Phishing
- SPAM
- Ataques: Exploit / Brute force / Sql injection / etc
- Violaciones de Copyright
- Alteraciones en el uso normal de protocolos y servicios (ej: spoofing, poisoning)

Incidente: cualquier evento que no forma parte de la operación acordada de un servicio de TI y causa o puede causar, una interrupción del mismo o una reducción de su nivel de calidad.

Problema: es la causa subyacente de uno o más incidentes.

Error conocido: incidente o problema para el cual se conoce la causa subyacente que lo produce y se ha identificado una solución transitoria o definitiva.

Uso responsable de la red: El producido por cualquier actividad motivada por la realización de tareas académicas. Debido a la gran diversidad de dicha actividades y a la dificultad de discernir usos correctos e incorrectos en base al monitoreo de red, se entiende por uso correcto a todo aquello que no esta explícitamente ligado a un uso NO responsable de la red.

Uso NO responsable de red: El producido por algún tipo de amenaza que el usuario puede estar siendo víctima o que el usuario pueda estar provocando a terceros, intencionalmente o no.

3 Evaluación de las herramientas de administración

Considerando la magnitud de la organización y los objetivos de servicio, se hace imprescindible contar con una herramienta que permita realizar la administración del servicio en forma automatizada.

3.1 Exigencias del Productos a evaluar

Según se expresa en [6] hay un conjunto de requerimientos que la herramienta debe cumplir:

- Posibilidad de interoperar con programas y herramientas existentes. Tener interfaces flexibles que poder interactuar con aplicaciones y herramientas existentes.
- Ser de código abierto.
- Contar con interfase de usuario web-based.
- Estar orientado a equipo de respuesta a incidentes de pequeña a mediana magnitud (un promedio de 250 incidentes por día.
- Crear rápidamente un registro de incidentes (menos de 30 segundos desde la recepción)
- Contar con documentación de la herramienta.

3.2 Productos probados:

Los productos evaluados fueron: AIRT [7], RTIR [8] y SIRIOS [9]. Teniendo en cuenta los requisitos anteriormente mencionados y las pruebas realizadas en cada herramienta, se muestran en el siguiente cuadro algunos de los resultados obtenidos:

Tabla 1. Cumplimiento de requisitos-Tabla comparativa.

Requerimiento	**RTIR**	**Sirios**	**AIRT**
1.Interoperabilidad con programas y herramientas existentes (integración con el servicio de mail)	X	X	X
2. Estar desarrolladas en código abierto	X	X	X
3. Posee interfaz basada en web	X	X	X
4. Está orientada a un equipo de pequeña a mediana escala	X	X	X
5. Hay documentación disponible	X	X	Documentación disponible en Idioma Alemán

En cuanto a las características de las mismas en lo que se refiere a requisitos deseables en herramientas que manejan incidentes, se encuentra también disponible un análisis pormenorizado realizado por el ArCERT, unidad de respuesta ante incidentes en redes que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública Nacional [10].

Además pudimos observar otras características relevantes de cada producto:

- En cuanto al alta de incidentes: En Airt los incidentes se cargan por el equipo de trabajo desde la interfaz web o se importan de una cola, que puede ser la salida de otras herramientas. En Sirios los incidentes pueden reportarse desde la interfaz web siendo un cliente definido. En RTIR los incidentes pueden reportarse por mail o crearse desde la interfaz web como un caso nuevo.
- En cuanto a la funcionalidad de búsquedas: Airt posee criterios de búsqueda son predefinidos, permitiendo buscar por 4 campos ya prestablecidos. Sirios permite buscar por todos los atributos del ticket y armar búsquedas predefinidas, así como también posibilita buscar por texto libre. RTIR permite realizar búsquedas simples o avanzadas, y buscar por texto libre.
- Otras características interesantes:
    - Airt convierte automáticamente direcciones IP en nombre si WHOIS lo resuelve.
    - Sirios maneja en forma clara y flexible los roles y los permisos sobre los mismos. Además maneja dos niveles de notas asociadas a un incidente: notas externas q pueden ser vistas por el cliente que reportó el incidente y notas internas que no son vistas por el cliente.
    - RTIR ofrece gráficos estadísticos relacionados a los incidentes. También tiene un manejo apropiado de roles y permisos como Sirios, incluso superador de acuerdo a nuestro criterio. Esta herramienta permite también crear relaciones entre diferentes tickets (de mezclar, de referenciar o ser referenciado, de dependencia), lo cual no proveen las otras dos herramientas analizadas.

Las 3 herramientas analizadas cumplen con las exigencias planteadas. Sin embargo, a pesar de ser las herramientas más referenciadas en el manejo de incidentes, presentaban complejidad en la comprensión de su manejo y denotaban falta de madurez en su desarrollo. Por ello en esta primer etapa se optó por utilizar una herramienta, de manejo general de tickets, más madura y conocida, y se pensó en adoptar GLPI [11] para la gestión de incidentes de seguridad. GLPI (Gestion Libre de Parc Informatique) es una herramienta open source para la gestión del parque informático y de la mesa de ayuda.

4. Situación actual

4.1 Actividades realizadas

- Definición de una lista de administradores
- Definición de una lista de repositorio de actualizaciones
- Se realizaron visitas a centros de similares características al que se desea montar dentro de la UNLP.
- Análisis de las prestaciones del GLPI, teniendo en cuenta con la integración del formulario creado.
- Se armaron una serie de capacitaciones sobre concientización sobre seguridad de la información. El seminario ha sido dictado en diversos ámbitos. Se tuvo una reunión con autoridades de la UNLP, y se proyecta dictar el mismo curso de manera más masiva para personal docente, no docente y alumnos de la UNLP.
- Análisis de procedimientos y políticas sobre uso razonable de la red, teniendo en cuenta documentos publicados por unidades académicas de la UNLP (por ejemplo las facultades de Cs. Económicas e Ingeniería)
- Desarrollo del sitio web (https://www.cert.unlp.edu.ar). Allí, además de definir misión, objetivos, servicios, se definen un conjunto de procedimientos de manera de determinar las acciones y pasos a seguir en conjunto con el equipo de soporte técnico de los servicios y redes de la UNLP ante acontecimientos particulares como:
    - Denuncia de incidente con equipos propios de la UNLP implicado como causante del mismo
    - Denuncia de incidente con equipos propios de la UNLP implicado como equipo afectado
- Se creó un formulario a través del cual un usuario de la red de la UNLP, o bien cualquier persona que haya sido damnificada por algún equipo perteneciente a la red de la UNLP, puede enviar dar de alta un incidente de manera tal que el mismo sea analizado, y en caso de considerarse necesario, realizar las tareas necesarias para dar solución y seguimiento. El mismo se armó en base a formularios existentes en varios organismos de similares características al que se desea conformar en la UNLP, y teniendo en cuenta la información con la que se desea contar al momento de recibir notificaciones de nuevos incidentes.
- Se analizan los perfiles que deben ser creados en el aplicativo seleccionado para poder llevar a cabo la operatoria del sistema de la mejor manera posible.
- Se llevó a cabo un análisis de requerimientos de manera de poder determinar los recursos tanto humanos como de infraestructura necesarios para sustentar el servicio teniendo en cuenta cantidad de requerimientos que se esperan recibir, entre otras variables.
- Se definió el documento con las especificaciones del equipamiento necesario para el CERT

- Se participó en el evento LACNIC XI desarrollado en la ciudad de Salvador Bahía, Brasil durante los días 26 al 30 de mayo de 2008. En el mismo se brindó un curso en el cual se interiorizó a los participantes en las pautas a tener en cuenta para la creación un de CSIRT **"Creating and Managing Computer Security Incident Response Teams (CSIRTs)".** Dicho curso fue dictado por personal del CERT.br (CERT de Brasil) el cual es "SEI Partner for CERT Courses". Esto significa que son "Software Engineering Institute Partner". Del mencionado evento se obtuvo mucho material de interés, entre el que se destaca un "manual" ó instructivo de seguridad para usuarios finales de recursos informáticos a través del cual intenta introducir los conceptos básicos y a los que los usuarios se ven más frecuentemente enfrentados en su tarea diaria.

4.2 Definición de un decálogo de seguridad informática

Una de las actividades que ha realizado el equipo del CERT en el marco de las tareas de concientización, es la definición del siguiente Decálogo de la Seguridad Informática.

1. No usaré contraseñas fáciles de adivinar, ni las compartiré con otras personas.
2. Cada día verificaré que el antivirus se encuentre activo, actualizado y libre de errores.
3. No haré caso a mensajes que soliciten mis contraseñas, datos personales u otra información sensible.
4. Solicitaré y usaré los recursos centralizados asignados por la UNLP para resguardar la información importante.
5. No abriré ningún archivo adjunto al correo electrónico, sin verificarlos previamente, aunque provenga de una persona conocida.
6. No descargaré ni instalaré aplicaciones desde Internet, sin verificarlos previamente. Acudiré siempre al personal que corresponda para la instalación de cualquier aplicación.
7. No aceptaré mensajes de correo electrónico sospechosos, de remitentes o asuntos desconocidos. Los borraré sin abrirlos. Tampoco participaré en cadenas empleando la dirección de correo institucional de la UNLP.
8. No divulgaré ningún tipo de información confidencial sin la debida autorización.
9. Alertaré a mis superiores o al responsable del área informática en caso de situaciones anormales relacionadas con la seguridad de la información.
10. Si tengo dudas o necesito asesoramiento respecto a la seguridad de la información, me comunicaré con la oficina correspondiente o a UNLP CERT.

5 Difusión del Proyecto

Cert.unlp tiene entre sus metas principales la capacitación, no sólo de la comunidad educativa de la UNLP sino también de la comunidad en general. Dentro de ese marco y a fin de dar a conocer el proyecto y el equipo de trabajo, se organizaron en primera instancia jornadas de concientización en seguridad de la información. Las primeras charlas estuvieron dirigidas a autoridades de la UNLP, personal del CeSPI, personal de la Biblioteca Pública y direcciones de enseñanza de diversas unidades académicas, y luego se realizaron diversos seminarios en el marco de la "Semana Internacional de la Seguridad Informática".

Estas actividades se difunden a través del sitio www.cert.unlp.edu.ar, carta de presentación de este proyecto. En este sitio se brinda información general en lo que respecta a incidentes de seguridad, como así también se difunden vulnerabilidades existentes. Con el objetivo de formar a la comunidad de la Universidad en el manejo seguro de la información, se publican avisos de phishing que ocurren en la red de la UNLP así como también mensajes falsos que circulan por la misma. Sin dejar de mencionar el decálogo de Seguridad Informática que compendia los principales consejos para manejar la información de manera segura.

6 Conclusiones

Para continuar su alineamiento con los estándares y mejores prácticas internacionales se ha comenzado a trabajar en la definición formal de acuerdos de niveles de servicio (SLA, service level agreements) con los clientes del servicio, para los proveedores externos y con los proveedores internos (OLA, Organizational level agrements)y con eventuales proveedores externos (UC, underpinning contracts).

Está pendiente culminar la definición formal de los catálogos de servicios, como así también completar la definición de las distintas bases de datos (de conocimiento, de errores conocidos, etc.).

7 Referencias

1. "CERT Creating and Managing Computer Security Incident Response Teams (CSIRTs)" Carnegie Mellon University 2007
2. Universidad Nacional de La Plata, http://www.unlp.edu.ar
3. Javier Díaz, Lía Molinari, Marcelo Raimundo. Uso y políticas de TICs en la Educación Superior de Argentina: el caso de la Universidad Nacional de La Plata. EDUTEC 2007.
4. Javier Díaz, Nicolás Macia, Paula Venosa, Miguel Luengo, Lía Molinari, Viviana Ambrosi. Arquitectura de sensores de seguridad para la correlación de eventos de seguridad. IX Workshop de Investigadores en Ciencias de la Computación - WICC 2007"
5. Javier Díaz, Viviana Ambrosi, Miguel Luengo, Nicolás Macia, Lía Molinari, Paula Venosa. "Cuando la seguridad trasciende fronteras, autenticación internacional en recursos distribuidos". VIII Workshop de Investigadores en Ciencias de la Computación - WICC 2006"

6. Kees Leune and Sebastiaan Tesink. Designing and developing an Application for Incident Response Teams. Tilburg University, Infolab. The Netherlands. 2006
7. Sitio web de la herramienta [https://www.airt.nl/]
8. Sitio web de la herramienta [http://bestpractical.com/rtir/]
9. Sitio web de la herramienta [http://www.sirios.org/]
10. Sitio Web del ArCert, http://www.arcert.gov.ar/
11. Sitio Web GLPI, http://www.glpi-project.org/