CERTuy: Hacia un CSIRT Nacional

Eduardo Carozo Carlos Martínez Leonardo Vidal

CSIRT - ANTEL[1]

Gustavo Betarte Alejandro Blanco Eduardo Cota Julio Pérez

Grupo de Seguridad Informática, Facultad de Ingeniería, Universidad de la República

***Resumen*—Este documento describe la actividad que está desarrollando, en el contexto de un proyecto focalizado en el área de la seguridad informática, un equipo integrado por personal de ANTEL y de la Facultad de Ingeniería de la Universidad de la República. El proyecto tiene como objetivos principales la elaboración y definición de metodologías y procedimientos que contribuyan a la formación de equipos de manejo de incidentes de seguridad informática y la consolidación de un grupo de trabajo, integrado por docentes y profesionales, cuya actividad central sea la formación e investigación en el área de seguridad informática.**

***Palabras claves*—Seguridad Informática, Manejo de Incidentes, CERT, CSIRT.**

I. Introducción

SON amplia y consensualmente reconocidas las ventajas que proveen los sistemas de información interconectados a través de redes de datos y comunicación para mejorar las comunicaciones, proveer control, proteger la información e incentivar la competencia entre pares. Es así, que una cantidad significativa de gobiernos, empresas de negocios, instituciones académicas e individuos están haciendo uso intensivo de esas ventajas. El bajo costo de las comunicaciones a través de Internet justifica el reemplazo de formas tradicionales de comunicación (como las basadas en papel, teléfono, o fax). Las computadoras se han transformado en una parte tan integral y esencial de los negocios y gobiernos que actualmente los riesgos relacionados con el uso indebido de recursos computacionales no pueden ser separados de los riesgos más tradicionales concernientes a negocios en general, salud y privacidad de la información. En la actualidad, activos básicos y valiosos tanto de los gobiernos como de las empresas están expuestos en Internet a amenazas de acciones que ponen en riesgo y/o degradan su valor. Por ejemplo, es frecuente que información de clientes sea publicada sin autorización como consecuencia de un ataque que atente contra la confidencialidad de esa información.

Manuscrito enviado el 10 de julio de 2006. Este trabajo ha sido realizado en el marco de un proyecto desarrollado por la empresa nacional uruguaya de telecomunicaciones, ANTEL y la Facultad de Ingeniería de la Universidad de la República.

[1] CSIRT ANTEL es el equipo de respuesta a incidentes informáticos de ANTEL.

La Internet, en consecuencia, se ha convertido en una infraestructura crítica que debe ser protegida. Entendemos por infraestructura crítica aquellos servicios esenciales y funciones de soporte que son necesarios para asegurar la operación de un gobierno o economía: telecomunicaciones, sistemas de información críticos del gobierno, transporte, suministros alimenticios y acuíferos, generación de energía, producción de gas y petróleo, sistemas bancarios y financieros, y servicios de salud y emergencias. La constante expansión de Internet conlleva un crecimiento de configuraciones distribuidas. Así como la tecnología tiende a distribuirse también lo hace la gestión de la misma. Desafortunadamente el carácter dinámico, distribuido e interconectado de este sistema hace que los ataques puedan ser montados y propagados rápidamente en forma global, traspasando límites geográficos y jurisdicciones nacionales. Es muy fácil explotar la gran cantidad de problemas de seguridad que existen en Internet y en los sistemas usados para interactuar con ésta, con el agravante que es también relativamente sencillo ocultar la verdadera identidad u origen de la persona responsable de un ataque. Se hace imperioso entonces contar con la posibilidad de comunicarse, coordinar, analizar y responder a ataques informáticos a través de sectores de negocios y fronteras nacionales.

A nivel nacional nos encontramos también con que la industria del software ha sido uno de los rubros no tradicionales de mayor crecimiento en los últimos años, siendo incluso objeto de iniciativas a nivel gubernamental. El creciente grado de exposición tanto de las empresas de software nacional como de los productos creados por ellas hace que el riesgo de ataques y de descubrimiento y explotación de vulnerabilidades sea cada vez mayor.

Estamos entonces frente a la ineludible necesidad de desarrollar una comunidad de usuarios, educada, entrenada y con conocimientos adecuados, que entienda realmente los riegos y problemas relacionados tanto con incidentes de seguridad informática como las amenazas y ataques que se pueden montar usando las vulnerabilidades de sus sistemas.

A mediados del año 2005, ANTEL y la Facultad de Ingeniería iniciaron una ronda de discusión en torno a la definición de una actividad a desarrollar en el contexto del convenio marco acordado entre las dos instituciones y con la seguridad informática como eje temático. El proyecto que se

planteó tiene como objetivo fundamental desarrollar actividades que contribuyan con sus resultados al complejo proceso de planificar, organizar, instalar y desarrollar un Computer Security Incidents Response Team (CSIRT) nacional. Un CSIRT es una organización responsable de la recepción, análisis y respuesta de reportes e incidentes de seguridad informática. Uno de los objetivos fundamentales es desarrollar infraestructura y capacidades tecnológicas y sociales para la prevención de este tipo de incidentes.

El resto del documento está estructurado como sigue. En la sección II se describe en mayor detalle antecedentes y las motivaciones para el desarrollo de la actividad CERTuy. La sección III discute los objetivos y beneficios de contar con un CSIRT nacional y presenta en detalle los procedimientos y recursos que son necesarios para la creación de un equipo tal. En particular se introducen y discuten las etapas de *Concientización* y *Planificación*, como definidas en [2]. La sección IV describe la actividad que se está desarrollando en el marco de la actividad específica CERTuy. Finalmente la sección V concluye.

II. Contexto y Motivación

A fines de los años 80 la agencia estadounidense DARPA (Defense Advanced Research Projects Agency) creó el Computer Emergency Response Team Coordination Center (CERT/CC) a cargo del Software Engineering Institute (SEI) de la reconocida Carnegie Mellon University. Con el objetivo fundamental de proveer respuestas a incidentes de seguridad en Internet, el CERT/CC ha sido definido para servir como modelo operacional y como promotor de la creación de otros equipos u organismos de respuesta a incidentes de seguridad informática. Desde el inicio de la actividad de este centro, era claro para sus promotores que la diversidad de tecnologías y servicios que podrían ser demandados por las distintas organizaciones consumidoras de esos servicios no podrían ser provistos por una única organización. Ningún equipo será capaz de suministrar respuestas efectivas y eficaces a todos los posibles ataques montados contra redes de computadores o sistemas conectados a estas redes.

En la actualidad existen varios cientos de CSIRTs en operación, sirviendo a una enorme gama de organizaciones comerciales, académicas, gubernamentales y militares. La mayoría de estos equipos focalizan su actividad en proveer a su comunidad objetivo servicios y soporte para la prevención, manejo y respuesta a incidentes de seguridad informática (usualmente denominados en la literatura *cybersecurity incidents*). La mayoría de estos equipos están focalizados en los aspectos técnicos de *cybersecurity* y la coordinación de iniciativas transversales de sectores interesados en resolver esos incidentes. Los beneficios de desarrollar un CSIRT a nivel nacional son muchos y variados. Ante la ocurrencia generalizada de incidentes de seguridad es muy importante contar con mecanismos que permitan:

- detectar e identificar efectivamente la existencia de incidentes de seguridad informática, analizando la actividad derivada de los mismos en los sistemas afectados
- desarrollar estrategias de mitigación y respuesta
- establecer canales de comunicación confiables
- proveer advertencias en forma temprana a los afectados por los incidentes
- notificar actores dentro de la comunidad de Internet de problemas potenciales
- coordinar respuestas efectivas frente a los incidentes detectados
- compartir datos e información sobre los mismos y/o de las correspondientes respuestas de solución
- registrar y monitorear esta información para determinar posibles líneas de acción y estrategias que permitan construir soluciones a largo plazo

Un CSIRT desarrolla tanto funciones reactivas como proactivas para proteger y asegurar los activos críticos de las organizaciones integrantes de su comunidad objetivo. Los objetivos de un CSIRT deben estar necesariamente basados en los objetivos de negocios de dichas organizaciones. Un CSIRT actúa reactivamente cuando, ante un incidente reportado o detectado, ayuda a la comunidad objetivo a contener o recuperarse de ataques a sus activos. Lo hace proactivamente al desarrollar educación y entrenamiento en áreas como detección de intrusión, testeo de penetración, documentación y aún desarrollo de programas.

La actividad de investigación y desarrollo que se describe en este documento, está orientada a satisfacer requerimientos en la mayoría de los aspectos arriba descriptos.

III. Definición e Implantación de un CSIRT nacional

Resumiendo los conceptos y explicaciones de las secciones anteriores, un CSIRT es una organización o equipo que provee servicios y soporte a una comunidad objetivo con el fin de prevenir, manejar y responder a incidentes de seguridad informática. En esta sección se describirá en mayor detalle cuales son usualmente los objetivos y beneficios de contar con un CSIRT, para luego pasar a discutir las actividades y procedimientos requeridos para poder definir y poner en funcionamiento un CSIRT nacional.

Gran parte de esta sección está fuertemente basada en el documento [2] donde se posicionan los conceptos básicos y procedimientos a seguir en el proceso de creación de un CSIRT.

A. Objetivos

Los objetivos fundamentales de un CSIRT son, por un lado, controlar el daño provocado por incidentes informáticos a los sistemas de información de las organizaciones pertenecientes a la comunidad objetivo, proveyendo respuesta y soporte para la recuperación de los mismos, y, por otro lado, desarrollar actividades que permitan prevenir la ocurrencia de incidentes similares.

Es necesario aclarar que el manejo de incidentes implica

mucho más que la sola actividad de implementar soluciones tecnológicas que permitan responder. Es necesario además tener la capacidad de formalizar y estandarizar procesos que permitan comunicar y coordinar las acciones de respuesta y recuperación ante la ocurrencia de eventos maliciosos.

Un CSIRT persigue objetivos diferentes a los de un equipo de seguridad de, por ejemplo, el departamento de TI de una organización o empresa. Un equipo de seguridad usualmente restringe su actividad a ejecutar procedimientos diarios de monitoreo de la red y sistemas de la organización. El equipo es el responsable de mantener los sistemas actualizados ya sea mediante la instalación de *patches* y o implementando *workarounds* que permitan mitigar los incidentes de seguridad. Un CSIRT puede naturalmente ejecutar todos estos procedimientos como parte de su función, pero además también sirve como repositorio de información de incidentes, como centro al que se puede reportar incidentes y análisis de los mismos, y principalmente como coordinador para la respuesta de incidentes transversalmente a toda su comunidad objetivo. Esta coordinación puede asimismo extenderse más allá de su comunidad para incluir colaboración con otros equipos y agencias. En secciones posteriores de este documento se discutirán distintos enfoques que pueden ser seguidos para la elección de modelos organizacionales, estructuras y servicios que puede brindar un CSIRT.

B. Beneficios

El beneficio principal a destacar de contar con un CSIRT es la capacidad que éste proveerá para instrumentar y conducir una rápida respuesta que permita contener un incidente de seguridad informático así como posibilitar la recuperación del daño causado por el mismo. La relación que un CSIRT tiene con sus organizaciones pares, ya sean otros CSIRTs o equipos de seguridad, puede facilitar el acceso compartido a estrategias de respuesta y a alertas tempranas de problemas potenciales, haciendo más efectivo y eficiente su accionar.

Los CSIRTs han evolucionado de ser concebidos como organizaciones orientadas a proveer respuestas, a ser organizaciones que trabajan proactivamente en la defensa y protección de los activos críticos de las organizaciones y de la comunidad Internet en general. Este trabajo proactivo incluye, por ejemplo, actividad de concientización y servicios de educación en seguridad, apoyo en el diseño de políticas de Seguridad de la Información y Seguridad Informática y coordinación de seminarios y de intercambio de información

Un CSIRT contribuirá asimismo a asegurar la calidad, desde la óptica de la seguridad, de los sistemas desarrollados dentro de la comunidad.. También puede ayudar a identificar áreas vulnerables de la cultura de la comunidad y en algunos casos desarrollar análisis y evaluación de vulnerabilidades e incluso detección de incidentes.

A continuación se enumeran los beneficios que en particular un CSIRT nacional puede proveer:

- servir como punto confiable de contacto
- desarrollar una infraestructura para coordinar la respuesta a incidentes de seguridad informática dentro del país, protegiendo los procesos productivos principales, y la economía nacional
- desarrollar la capacidad de proveer soporte para el reporte de incidentes dentro de las fronteras de nuestro país
- conducir análisis de incidentes, vulnerabilidades y *artifacts*[1]
    - difundiendo información sobre vulnerabilidades que han sido reportadas así como las correspondientes estrategias de respuesta
    - compartir el conocimiento y las estrategias relevantes de mitigación con los miembros de la comunidad, *partners* y colaboradores
- participar en actividades de "guardia" tecnológica, promoviendo una comunidad de equipos nacionales y regionales que compartan datos, investigación, estrategias de respuesta, y notificaciones
- ayudar a organizaciones e instituciones nacionales a desarrollar capacidades propias de manejo de incidentes, proveyendo, por ejemplo, guías e información para contribuir a la planificación e implementación de equipos de seguridad, consolidar relaciones y estimular discusiones entre diferentes agencias del gobierno, empresas públicas/privadas y organizaciones académicas
- proveer servicios de traducción y difusión en español, de información relacionada con la seguridad informática proveniente de entidades externas
- publicar, sea a través de sitios web o utilizando métodos eficaces de comunicación, mejores prácticas y guías generales de seguridad. Este tipo de información puede incluir, por ejemplo, guías técnicas para la configuración segura de *hosts* y redes, *links* a otras fuentes confiables de información para la implementación de sistemas de comunicación seguros
- promover y desarrollar materiales de educación, concientización y entrenamiento orientados a diversos tipos de audiencia. El público objetivo puede variar desde administradores de sistemas y redes, otros CSIRTs organizacionales dentro del país, representantes legales, *policy makers*, hasta público en general
- identificar y mantener una lista de CSIRTs y puntos de contacto dentro de las fronteras de nuestro país

Un CSIRT nacional se interesará en mejorar los programas existentes de educación y entrenamiento para desarrollar, consolidar y profundizar las habilidades y conocimientos tecnológicos de los miembros de su equipo y así como de otros CSIRTs y miembros del equipo de TI de las organizaciones pertenecientes a la comunidad objetivo.

Actividades como las mencionadas anteriormente deben ser

[1] Código malicioso

discutidas y resueltas entre varios equipos, y no sólo dentro de una organización o empresa, sino a nivel nacional e inclusive regional. En nuestro país, la mayoría de las organizaciones no cuentan con CSIRTs, equipos responsables, ni siquiera al menos un conjunto mínimo de procedimientos repetibles para el manejo de incidentes de seguridad. En forma similar, pero a nivel nacional, se observa la total ausencia de procesos de respuesta, gestión y coordinación de incidentes que indica el nivel de riesgo al que esta expuesto el país.

En la próxima sección, con el objetivo de contribuir al entendimiento de esta problemática, se describirán los conceptos y procedimientos requeridos para crear un CSIRT.

C. Creación de un CSIRT

Esta sección reproduce en gran medida parte del contenido del documento [2] donde se describe en detalle las distintas etapas a seguir en el proceso de creación de un CSIRT con alcance nacional.

Etapas

En [2] Killcrece introduce y discute, basándose en la experiencia de su propio y otros equipos, un conjunto de etapas básicas que permiten describir estructuradamente el desarrollo de un CSIRT desde el momento de su concepción intelectual hasta el punto de la consolidación de su capacidad operacional integral.

El documento define 5 (cinco) etapas de alto nivel: Capacitación, Planificación, Implementación, Operación y Colaboración. Estas etapas proveen una forma clara de caracterizar la actividad involucrada en la creación de un CSIRT desde la planificación del mismo hasta la creación y mantenimiento de la capacidad de manejo de incidentes. Los procedimientos definidos en estas etapas incluyen: la identificación de los actores involucrados en el proceso de creación del equipo, el desarrollo de un plan estratégico y la visión que determinará la organización, estructura, equipo y financiación del CSIRT, el entrenamiento del staff del CSIRT para operar el mismo, y la incorporación de mecanismos que permitan la evaluación y mejora continua del CSIRT

Este proceso no debe entenderse como secuencial, en las experiencias que este equipo ha llevado a cabo, muchas de las tareas se han llevando a cabo simultáneamente. Existirán iteraciones que exigirán refinar los componentes de algunas etapas previas al tratar de definir otros de una etapa posterior. En las dos próximas secciones se describirá en mayor detalle las etapas de Capacitación y Planificación. Esto nos permitirá fijar los elementos y procedimientos referencia que han sido considerados en el proceso de discusión y definición del CERTuy.

a) Etapa 1: Capacitación

Esta es básicamente una etapa de concientización, donde aquellos que participan y promocionan el desarrollo de una capacidad de respuesta a incidentes nacional comprenden lo que es requerido para el desarrollo y establecimiento de un CSIRT. En esta etapa se analiza el rol que se espera ocupará el CSIRT así como las cuestiones clave que deben ser resueltas (por ejemplo, gestión y reclutamiento, desarrollo de comunicaciones y coordinación confiables, procesos efectivos)

Una actividad central de esta etapa, además de la actividad de mejorar el entrenamiento disponible para el desarrollo de CSIRTs organizacionales, es la de organizar reuniones y promover discusiones que permitan identificar y precisar las cuestiones fundamentales relacionadas con la definición y desarrollo de un CSIRT nacional y los consecuentes beneficios de contar con un equipo tal. Estas reuniones y discusiones deberán analizar todos los aspectos que implica desarrollar una capacidad de respuesta a incidentes con proyección nacional, incluyendo por ejemplo, los posibles modelos de negocio para un equipo nacional y la necesidad que motiva su creación, así como la misión, objetivos estratégicos y expectativas del mismo. También se deberá identificar los actores a involucrar en la discusión para la creación de un equipo nacional, los promotores y desarrolladores del equipo, los planificadores e implementadores del mismo y los tipos de canales de comunicación que necesitan ser implementados. Asimismo se debe determinar cuáles son los recursos clave y las infraestructuras críticas existentes en la nación, las leyes específicas, reglamentos, y otras políticas que enmarcarán el desarrollo del CSIRT nacional y sus actividades, y la tecnología e infraestructura de red que será necesaria para soportar las operaciones del equipo nacional. Finalmente, es muy importante revisar e investigar lo que otros países están haciendo o han hecho para crear sus equipos nacionales e identificar las mejores prácticas y guías que pueden ser aplicadas en el caso propio.

b) Etapa 2: Planificación

Apoyándose en el conocimiento e información ganados en la etapa de Capacitación, esta próxima etapa se focaliza en el diseño y planificación del CSIRT nacional. Cuestiones discutidas y revisadas durante esta etapa incluyen la articulación de la necesidad y beneficios de contar con un equipo nacional, identificar la comunidad objetivo, los servicios y el rol que el CSIRT tendrá, determinar los costos de creación y operación del mismo, definir el cronograma de trabajo y la gente que será asignada para desarrollar la planificación, implementación y puesta en operación del equipo.

Más específicamente, las actividades de esta etapa requieren:

1. *Establecer los requerimientos e identificar la necesidad de un CSIRT nacional*.
2. *Desarrollar la visión y misión que guiarán el CSIRT*.
3. *Identificar el tipo de respaldo y aprobación (gubernamental) nacional, dirección y* patrocinio *requeridos para el éxito del equipo, y obtener ese respaldo*.
4. *Identificar las habilidades y conocimiento requeridos para operar el equipo*.

5. *Definir los roles y responsabilidades para el CSIRT nacional*.
6. *Especificar los procesos de gestión de incidentes que el equipó llevará adelante*.
7. *Desarrollar un conjunto de criterios estándar y terminología consistente para la categorización y definición de eventos y actividad de incidentes*.
8. *Definir un conjunto de guías para el manejo de incidentes, requerimientos de reporte y formularios para determinar el modo de interacción entre el CSIRT y la comunidad objetivo, otros CSIRTs y partners externos*.
9. *Determinar los procesos requeridos para la integración con otros equipos o planes de gestión de emergencias*.
10. *Determinar los métodos para establecer y consolidar relaciones y colaboraciones confiables con otras infraestructuras críticas*.
11. *Diseñar los procesos y mecanismos de comunicación y coordinación para lograr una eficaz difusión de información a la comunidad objetivo*.
12. *Definir hitos y entregables*.
13. *Crear el plan del CSIRT nacional basándose en los resultados determinados por la actividad de planificación, la visión y el correspondiente marco de referencia, obteniendo feedback y revisión del plan, incorporando revisiones al mismo si es necesario, desarrollando cronogramas para la revisión y modificación del documento de planificación y todo material de soporte del mismo.*

El equipo de planificación puede también desarrollar un documento de operaciones que asista en la definición del alcance o límites de las responsabilidades del equipo. Este documento podría constituir la hoja de ruta para el desarrollo de la visión del CSIRT y debería presentar una descripción de alto nivel de todas las actividades enumeradas anteriormente. Debería también incluir información concerniente a los principios guías y consideraciones de reglamentación, los roles de coordinación y las responsabilidades, y discutir la estructura y tipos de relaciones el equipo tendrá con otras organizaciones.

IV. El proyecto CERTuy

Este proyecto está efectivamente operativo desde marzo de 2006. La actividad que se ha desarrollado ha estado orientada a satisfacer requerimientos que surgen de las etapas arriba descriptas. Más específicamente, se han planteado dos ejes de actividad: por un lado se está desarrollando trabajo que contribuye al proceso de formación e instalación de un CSIRT nacional y por otro lado se está trabajando en actividades que permitirán consolidar la creación e instalación de un Laboratorio de Seguridad Informática (LaSI), con base en la Facultad de Ingeniería y sustentado por recursos (tanto humanos como estructurales) de esta institución educativa y de ANTEL. A continuación se describe brevemente estas actividades.

A. Taller CSIRT

Como primera tarea de esta actividad se ha planteado la organización de un taller de trabajo en el que se ponga en común la investigación de material bibliográfico que cubre diferentes aspectos relacionados con la instalación, puesta en marcha y operación de un CSIRT nacional. El objetivo principal de esta actividad es la elaboración de un conjunto de documentos que constituyan una propuesta metodológica y organizacional de un CSIRT nacional. En primer lugar se elaborará un documento que describa el rol que el equipo de respuesta debe jugar y que identifique los componentes operacionales a considerar tanto en la fase de formación del equipo como después de iniciada su actividad. La determinación de cuáles son los servicios esenciales del CSIRT y la definición de las políticas y procedimientos internos del CSIRT, así como la definición y documentación de la visión y alcance de un servicio de respuesta a incidentes serán descriptos en un segundo documento. Otro documento describirá el modelo organizacional a aplicar para implementar las capacidades de respuesta a incidentes de seguridad, incluyendo una comparación con otros modelos alternativos. Finalmente, se elaborará un documento primario sobre el modelo y plan de negocio.

B. LaSI

Este laboratorio ha sido concebido como un centro de actividades de difusión, formación, experimentación e investigación en torno a los múltiples aspectos de la seguridad informática y además como un instrumento fundamental de aporte a la formación e instalación de un CSIRT nacional. El conocimiento y manejo de las distintas herramientas que permiten implementar medidas de protección, detección y prevención de incidentes es una necesidad en el ámbito de la Seguridad Informática y se considera que un enfoque práctico es particularmente enriquecedor.

Los objetivos del LaSI son variados. En primer lugar, contribuirá a consolidar un ámbito aglutinador para las actividades de seguridad informática que posibilite el desarrollo de un grupo de trabajo, integrado por docentes y profesionales, para la formación e investigación en el área de seguridad informática. Otro objetivo importante es poder consolidar una infraestructura tecnológica, aislada de los sistemas en producción, donde poder experimentar. Esta plataforma permitirá la instalación, configuración, funcionamiento y evaluación de herramientas de seguridad informática así como el análisis en condiciones controladas de vulnerabilidades y ataques a los sistemas operativos y servicios. La formación de recursos humanos es otro objetivo fundamental. Para eso se planea desarrollar capacitación en seguridad informática mediante la realización de talleres, cursos, seminarios con importante contenido práctico.

Asimismo el LaSI contribuirá como ámbito de experimentación para el desarrollo de maestrías y doctorados en el área. Es también vocación del laboratorio el impulsar y fomentar una cultura de Seguridad Informática y de intercambio de información en seguridad.

En lo que va del proyecto ya se ha elaborado el diseño de la arquitectura de la plataforma de experimentación, se han preparado módulos prácticos de aplicación de fundamentos de la seguridad informática y se han identificado casos de prueba y herramientas a utilizar para el desarrollo de los mismos.

C. Taller de formación y experimentación.

La puesta en marcha de un taller de formación, tiene dos objetivos fundamentales. El primero de ellos, nivelar entre los integrantes del grupo de trabajo, los conocimientos existentes en cuanto a seguridad informática. El segundo objetivo consiste en que dicha nivelación sea el primer paso hacia la creación de un diploma de especialización y/o postgrado en seguridad informática, hasta ahora inédito en nuestro país.

Para lograr el primer objetivo, se ha procedido por refinamientos sucesivos: se identificó las grandes áreas temáticas a ser cubiertas por el taller, se definieron los temas específicos a tratar dentro de cada área y se relevó el material bibliográfico que servirá de soporte para el tratamiento de los mismos. Este taller de formación, que se estima tendrá una duración de dos meses aproximadamente, con dos sesiones semanales de una hora y media cada una, incluye actividades teóricas y prácticas. Esta actividad permitirá generar un importante *input* para el LaSI. Con esta primera experiencia se satisface, por un lado, uno de los objetivos fundamentales del proyecto y además se obtendrá una primera versión de un plan de nivelación focalizado en introducir los conceptos básicos y herramientas de las áreas fundamentales de la Seguridad Informática..

Respecto al segundo objetivo, la realización del taller de formación permitirá refinar y validar lo que se ha identificado como el núcleo básico temático de un programa de formación especializada en el área de la seguridad computacional e informática.

V. CONCLUSIONES

El modelo de centro de respuestas a incidentes informáticos (CSIRTs) es reconocido a nivel mundial como una excelente herramienta a la problemática general de la seguridad informática. El proyecto CERTuy tiene como principal objetivo contribuir al desarrollo del área de coordinación en seguridad informática a nivel nacional. En el mismo se ha trabajado en un modelo innovador de colaboración entre la industria y la academia, algo no tradicional en Uruguay.

Este proyecto además de cumplir con los objetivos planificados, ha logrado en sinergia con la actividad del CSIRT de ANTEL importantes reconocimientos nacionales y regionales. En particular ya están establecidos numerosos contactos a nivel internacional, como ser el CERT.BR de Brasil, ARCERT de Argentina, AUSCERT de Australia, y LACNIC que ya han comprometido su apoyo para la inclusión del proyecto (luego de implementado) en el FIRST (Forum of Incident Response and Security Teams), así como a nivel nacional se han establecido contactos con el Ministerio de Defensa Nacional, Ministerio del Interior y Prosecretaría de la Presidencia de la República, quienes han mostrado alto interés por la concreción del mismo. Esta situación es consecuencia directa de la relevancia que el mismo tiene para aquellas organizaciones que tienen alta dependencia de su plataforma tecnológica, y que perciben en el proyecto un aporte significativo a la capacidad de responder a los problemas asociados a la actividad maliciosa en informática y promover un desarrollo de las empresas del país más sostenible.

Por otra parte se está conformando un equipo de expertos en seguridad informática sobre la base de un fuerte entrelazamiento de la actividad profesional y académica.

REFERENCIAS

[1] G. Killcrece et al, *Organizational Models for Computer Security Incident Teams (CSIRTs)*, Handbook CMU/SEI-2003-HB-001, diciembre 2003.

[2] G. Killcrece, *Steps for Creating National CSIRTs*, CERT/CC, SEI, Carnegie Mellon University, agosto 2004.

[3] D. Smith, *Forming an Incident Response Team*, Australian Computer Emergency Team, 1993.

[4] M.J. West-Brown et al, *Handbook for Computer Security Incident Teams (CSIRTs)*, Handbook CMU/SEI-2003-HB-002, segunda edición, abril 2003.