Proyecto AMPARO

Fortalecimiento de la Capacidad Regional de atención de incidentes de Seguridad en América Latina y el Caribe

Número de Donación de IDRC: 105237

Institución Investigadora: LACNIC

Países: América Latina y el Caribe

Integrantes del equipo:

Director: Msc. Ing. Eduardo Carozo, CIS

Steering Committee: Jeimy Cano (CO), Pablo Carretino (AR), José Luis Chavez (GT), Alejandro Hevia (CL), Cristine Hoepers (BR), Patricia Prandini (AR), Indira Moreno (MX)

Coordinación, administración y logística: Raúl Echeverría, Ernesto Majó, Alexandra Dans.

Lapso de tiempo cubierto por el informe: Un año.

Fecha de presentación: 30 de junio de 2010

Tabla de Contenido:

PROYECTO AMPARO

I. Síntesis

El Proyecto AMPARO se hace realidad en Junio del 2009, en Montevideo Uruguay, con la misión de fortalecer la capacidad regional de atención de incidentes de seguridad en América Latina y el Caribe, tanto en el ámbito privado como en organizaciones sociales.

Es una iniciativa de LACNIC (Registro de Direcciones de Internet para América Latina y del Caribe - www.lacnic.net -) con sede en Montevideo Uruguay que cuenta con el apoyo del Centro Internacional de Investigaciones para el Desarrollo (IDRC - International Development Research Center -) de Canadá. El presupuesto inicial del Proyecto AMPARO cubre la operación del primer año y medio.

Su enfoque principal es el de promover la difusión y capacitación de la metodología de Centros de Respuesta a Incidentes de Seguridad Informática o CSIRTs (Computer Security Incident Response Teams). Así mismo desarrollar contenidos públicos originales para el entrenamiento de expertos de la región.

Tiene como Objetivo General: Fortalecer la capacidad de prevención y de respuesta a incidentes de seguridad informática en la región de América Latina y el Caribe.

Al momento se han creado los materiales necesarios para la capacitación de expertos en Creación y Operación de CSIRT, y se han realizado tres talleres.

Un Taller de Expertos e Instructores para finalizar y validar el contenido a brindar en Montevideo, en Marzo de 2010, y dos Talleres para técnicos en Quito, Ecuador y México DF, México, que han obtenido una altísima calificación por parte de los participantes.

Adicionalmente se han seleccionado e iniciado el desarrollo de cinco proyectos de investigación sobre problemáticas de seguridad, asignándose expertos para su seguimiento y control.

Se ha conformado una comunidad de al menos 100 técnicos de la región que están intercomunicados por correo electrónico, para lograr una mejor respuesta y comprensión sobre los incidentes en curso, y se ha identificado y solicitado por ellos la constitución de un sitio seguro compartido para intercambiar opiniones, buenas prácticas y experiencias.

Varias Universidades y organizaciones estatales han solicitado permisos para reproducir partes o la totalidad de los talleres en la región, destacándose la próxima inauguración del primer CSIRT de Ecuador en la Universidad Técnica Particular de Loja, entre otros.

Están programados tres talleres más en el curso del año, en Santo Domingo, República Dominicana, Santiado de Chile, Chile y Bogotá, Colombia.

Finalmente se destaca que las tareas se vienen desarrollando con normalidad según lo esperado, sin la aparición de dificultades de ningún tipo.

II. Problemas objeto de la investigación

La red global y el ciberespacio hoy en día nos han dado facilidades sumamente provechosas para la humanidad. La facilidad con que hoy accedemos al conocimiento universal, a la realización de transferencias financieras, a la comunicación entre personas lejanas, a la realización eficiente de negocios, al intercambio de información en línea, son entre otros avances relevantes en el proceso de mejoramiento de las condiciones de vida de las personas y del desarrollo de las naciones.

Sin embargo, al igual que con cualquier otro medio de comunicación, la red global está siendo crecientemente utilizada para fines delictivos, algunos de ellos verdaderamente perversos y, en todo caso indeseables.

Así es como los diversos incidentes de seguridad informática se han convertido en toda una problemática que tiene que ser atendida, es por ello que no podemos permitir que el avance tecnológico sea libremente atacado por grupos de intrusos que amenazan nuestras infraestructuras y por ende parte de nuestro modo de vida.

Muchas operaciones son realizadas a través de Internet de forma bastante trivial y casi automática, tales como pagar cuentas, hacer compras, reservar viajes, etc. Es también una importante herramienta para la comunicación de las personas, disminuyendo las distancias.

Dentro de los problemas a atender, se puede mencionar el problema de los mensajes con propaganda no solicitada (spam), que por su volumen implican para los usuarios un tiempo más que razonable para eliminarlos y poder atender los mensajes que realmente importan. Esto también genera costos adicionales en los recursos, ancho de banda, filtros, etc. Al igual que en el mundo físico, hay también problemas de robo mediante el aprovechamiento de las debilidades de los sistemas electrónicos, aunado al desconocimiento de los usuarios, causando grandes perjuicios financieros para las personas y organizaciones. Y hay también la combinación de los dos, donde por ejemplo se envían mensajes en forma masiva con el objetivo de atraer el usuario a un sitio falso de un banco o buscando que el usuario brinde información privada. O que lo haga instalar en su computadora programas que le robarán contraseñas y datos confidenciales.

La diferencia es que, al tener acceso a sistemas de información en línea, el cibercriminal opera con varias ventajas diferenciales sobre el mundo físico:

- **Productividad más alta.** Los sistemas vulnerables contienen información sobre miles de víctimas
- **Menor resistencia del blanco**. Cuando son atacados, los sistemas muchas veces no conservan registro de lo que pasó
- **Menor sensibilidad del blanco**. Los dueños del sistema suelen tomar semanas y hasta meses para darse cuenta que han sido infiltrados
- **Escape más fácil.** Cuando se descubre el hecho, el cibercriminal escapa y desaparece más fácilmente.

La mayoría de las veces, estos usuarios mal intencionados hacen uso de computadoras comprometidas anteriormente para practicar las actividades maliciosas y así esconden su verdadera identidad.

Este no es un listado exhaustivo de los problemas que trae consigo el uso de Internet, solo se enumeran algunos a modo de información.

Es también importante subrayar que el cibercriminal ataca en igual medida a grandes empresas y a individuos. No importa el "tamaño" de la víctima. El ataque se efectuará ahí donde hay información que puede ser convertida fácilmente en dinero.

Los ataques provienen en mayor medida de fuentes externas: hackers, grupos criminales, etc. (73%). Sin embargo, los ataques internos: ejecutivos de la compañía, empleados, etc. (18%) son los que producen mayor daño. Otras fuentes de ataques pueden también provenir de los socios de la organización.

Es por todo ello que resulta muy importante para las organizaciones y también para los proveedores de acceso Internet, contar con mecanismos para evitar y contener actividades abusivas que permiten generar los problemas referidos.

Para contrarrestar estos problemas, uno de los mecanismos utilizados cada vez con mayor frecuencia, es el de contar con un grupo que a su nivel (empresa, servicio, país) tenga la capacidad de tratar los incidentes de seguridad de red. Estos grupos son comúnmente denominados Equipos de Respuestas a Incidentes de Seguridad de Computadores, o del Inglés Computer Security Incident Response Team (CSIRT).

Los Grupos de Coordinación de Respuesta a Incidentes de Seguridad (CSIRT por su sigla en Inglés) son organizaciones cuyo rol es el de proveer información en relación con el tratamiento de eventos de seguridad informática. Estas entidades, deben ser capaces de brindar información oportuna sobre cómo responder a los distintos tipos de incidentes, determinar su impacto, alcance y naturaleza, comprender las causas técnicas, investigar soluciones, realizar recomendaciones, coordinar y dar apoyo para la implementación de las estrategias de respuesta con las partes involucradas, difundir información sobre los tipos de incidentes mas frecuentes y toda información relevante que permita estar preparado para dar respuesta a los mismos y mitigar sus efectos, coordinar y colaborar con otros actores, tales como proveedores de Internet (ISP), otros grupos de seguridad, etc.

La existencia de estos grupos de tratamiento de incidentes puede permitir una más rápida y más eficiente dilucidación del origen del problema y con eso evitar prejuicios aún mayores para la organización, usuarios o terceros que sean afectados.

Estos grupos deben recibir avisos, quejas e informes de incidentes de seguridad de la red de la organización o del proveedor de acceso. Deben inmediatamente dar el debido tratamiento al problema, identificando el tipo de incidente, contactar con los responsables de la organización y dar seguimiento y asistencia hasta su solución. Deben también tomar las providencias para corregir las posibles fallas de sus sistemas y así evitar que nuevos incidentes ocurran o reincidan.

El hecho de que haya un equipo asignado específicamente para esa función permite sistematizar la información y los tipos de problemas y las respuestas recomendables, evitando que en cada incidente se pierda tiempo identificando el tipo del problema, como resolverlo, como ubicar los responsables, etc. Esto es precisamente lo que pasa en muchas organizaciones o proveedores, donde los informes de incidentes son tratados por los operadores de la red o por los responsables por el área de TI (Tecnología de Información), sin ese respaldo de sistematización de experiencias y consolidación de puntos de contacto.

Existen CSIRTs nacionales que, entre otras funciones, sirven de punto de referencia para incidentes con origen en las redes de un país. Estos CSIRTs a su vez son los responsables de comunicar los incidentes a los responsables dentro del país. Lo que para ellos es más fácil debido a su mayor conocimiento de las entidades o proveedores y sus responsables en el país.

Además de esa categoría de CSIRTs nacionales, han surgido muchos otros que tienen responsabilidad dentro de una organización o servicio, ya sean universidades, bancos, gobiernos y proveedores de acceso y servicio Internet, buscando dar una respuesta correcta y eficaz a los numerosos incidentes de seguridad.

Los responsables por la creación y gestión de los CSIRTs pasan por entrenamientos estandarizados y por ello actúan de forma parecida permitiendo una interacción eficiente entre ellos y con otras organizaciones. Existen organizaciones extrarregionales quienes han desarrollado programas de capacitación y certificación de profesionales en la operación de CSIRTs, pero su acceso es restringido en costo y en posibilidad de uso de los materiales, estando debidamente protegidos sus derechos de uso (copyright).

Es común que los CSIRTs también se encuentren en foros para discusión de sus actividades y actualización de información. Un foro muy conocido es el FIRST del ingles Forum of Incident Response and Security Teams, el que centraliza un conjunto de materiales de divulgación muy amplio, de utilidad limitada para quien no cuenta con una formación básica en la materia.

A nivel regional la creación de CSIRTs, cuenta con algunos ejemplos relevantes, pero no es una metodología generalizada. En ese sentido se destaca claramente, el trabajo del CERT.br, quien desde el año 1997 viene desarrollando una labor fundamental en Brasil, de coordinación y entrenamiento, pero también de apoyo y colaboración en toda la región, participando en diversas actividades de divulgación y capacitación a lo largo de la región. Argentina (1999), Chile (2001) y Venezuela cuentan también con CERT oficiales, aunque existen otras iniciativas muy relevantes en los distintos países (CSIRT Antel, Uruguay).

Si bien se ha logrado en las actividades reseñadas, identificar un conjunto de expertos de relevancia internacional en la región, no se ha logrado avanzar en el desarrollo de materiales de capacitación y entrenamiento de acceso libre que pueda ser utilizado para promover cursos que permitan difundir las mejores prácticas de seguridad informática.

El contenido académico de libre acceso disponible es casi inexistente, así como la mayoría del material que se encuentra en Internet está orientado a promover ofertas comerciales de empresas proveedoras de Seguridad Informática.

Es importante consignar que el desarrollo de nuevas estrategias y metodologías de seguridad debe ser tan rápido, comprehensivo y complejo como la habilidad de los “hackers o crackers” de explotar los nuevos servicios que se ofrezcan a través de la red, por lo que la investigación y desarrollo de las mismas es permanente y muy exigente.

Debe tenerse en cuenta que esta necesidad de investigación se fundamenta en dos situaciones altamente dinámicas:

1. El desarrollo explosivo de las diferentes tecnologías de la información y telecomunicaciones y su altísima aceptación por las comunidades de los países de menor desarrollo (destacándose la tecnología celular y su nueva capacidad de transmisión de datos de alta velocidad e interacción con Internet)

2. Los cibercriminales gestionan su accionar basándose en comunicaciones tempranas de las debilidades de las nuevas plataformas (dado que son las más rentables y menos probadas) donde justamente los países en desarrollo son compradores pasivos de tecnologías y no tienen capacidades, ni de investigación, ni de desarrollo de estrategias defensivas especializadas.

Es fundamental entonces que los profesionales que sean responsables de brindar la respuesta a los incidentes obtengan acceso también temprano a las nuevas tecnologías, así como desarrollar una metodología adecuada a la idiosincrasia de la región, que posibilite dicho acceso en forma continuada y sistémica.

La investigación y desarrollo y la difusión de las mejores prácticas del sector es uno de los principales cometidos de estos equipos y deben realizarlo basándose en estructura metodológicas que aún no han sido desarrolladas, ni siquiera estudiadas, y mucho menos implantadas en la gran mayoría de los países integrantes de la comunidad atendida por LACNIC. Actualmente la mayoría de los incidentes se resuelven en base a esfuerzos individuales de técnicos, que toman medidas tardías y frecuentemente desproporcionadas, aumentando significativamente el impacto del incidente original y generando grandes costos económicos y sociales a las comunidades de la región.

Si bien existe buena bibliografía en temáticas puntuales de Seguridad Informática, la misma está enfocada a resolver problemas en sistemas de cómputo individuales, o de alcance acotado a eventos informáticos de bajo impacto. No existe bibliografía aceptada que describa los procesos asociados a incidentes masivos en Internet, así como no existe ninguna base documental, ni metodológica, de acceso libre, que difunda las actividades que debe llevar a cabo el profesional de seguridad de un CSIRT que deba gestionar los incidentes de este tipo.

Finalmente, la falta de capacitación disponible provoca que los profesionales en el tema estén sobre-demandados, sean escasos, y no se puedan constituir equipos estables de respuesta en muchas de las comunidades atendidas por LACNIC.

En forma complementaria con las actividades desarrolladas por otros actores de la región, LACNIC viene impulsando desde sus inicios la atención sobre la problemática de Seguridad en Internet, con sus diversas vertientes, en el entendido que la problemática de seguridad es crítica para el desarrollo de Internet en la región.

III. Hallazgos de la investigación.

En el transcurso de las actividades se ha detectado una fuerte tendencia a mantener la información de los incidentes en la interna de las organizaciones, por temor a afectar la reputación de la organización afectada, que está provocando una importante barrera a la hora de mitigar y acotar el impacto de los incidentes. Esta compartimentación de la información es aún mas notoria en la interna de los países visitados, en los cuales existen altos grados de desconocimiento de las habilidades de otros equipos, impidiendo utilizar el potencial de acción de entidades de gobierno, universidades o empresas privadas.
El tipo de taller diseñado, es especialmente adecuado para demostrar **qué** información, **cuando** debe comunicarse y a **quién** debe comunicarse por su rol dentro de la sociedad. Esto ha sorprendido a los participantes, y ha sido de los resultados mas valorados en la interna de cada país.
Se valora también la existencia de una comunidad multinacional de contactos y relaciones de confianza y se visualiza a Proyecto AMPARO, como un posible actor en esta tarea.

A nivel de la investigación se constata el bajo desarrollo de la región en actividades vinculadas a investigación en seguridad informática y se detectan pocas universidades y/o entidades de investigación en la región.
La comunidad de participantes adicionalmente está solicitando la existencia de un foro de compartición de experiencias y buenas prácticas, así como una segunda versión de talleres más especializados.
Desde la Dirección del Proyecto se constata un alto grado de compromiso de los participantes y un fuerte relacionamiento posterior, que permite a los participantes consultar a otros sobre ataques que están sufriendo y formas de mitigarlos.

IV. Implementación y gestión del Proyecto.

Inicialmente, el Director del Proyecto AMPARO realiza una convocatoria a expertos involucrados en la problemática de Seguridad Informática de la región, para conformar el Steering Committee, a los siguientes profesionales:

- Dr. Ing. Cristine Hoeppers, Brasil.
- Ing. Patricia Prandini, Argentina.
- Ing. Indira Moreno, México.
- Dr. Ing. Alejandro Hevia, Chile.
- Ing. Pablo Carretino, Argentina.
- Dr. Jeimy Cano, Colombia.
- Ing. José Luis Chávez Cortéz, Guatemala.

Todos los expertos aprobaron su inclusión en el mencionado comité y apoyaron la propuesta, reconociéndola como pertinente y oportuna.
El Steering Committee ha brindado lineamientos que le brinden un marco de referencia regional al Proyecto AMPARO, así como han contribuido eficazmente a su difusión y comunicación hacia la comunidad.

Luego ha podido crearse en tiempo record y con una calidad excepcional los siguientes materiales: ***"*Manual Gestión de Incidentes de Seguridad Informática para América Latina y el Caribe"** y cuatro diferentes **Talleres de Gestión de Incidentes: Caso de Phishing; Caso de DDoS por Botnet; Caso de desarrollo de una HoneyNet; Caso de Análisis Forense Informático.**

Para la creación del Manual, se envió una invitación para participar como autores en la creación del mismo, así como cuatro Talleres "Hands On", que trataran los tipos de incidentes más frecuentes. Los contenidos iniciales del manual fueron ideados por el Director del Proyecto AMPARO y distribuidos entre los autores en función de su experiencia. Los Autores designados fueron:

Autores del "Manual de Gestión de Incidentes de Seguridad Informática"
- Ec. Araí Alvez Bou, Uruguay.
- Lorena Ferreyro, Argentina.
- Ing. Rubén Aquino Luna, México.
- Ing. Leonardo Vidal, Uruguay.
- Ing. José Luis Chávez Cortéz, Guatemala.
- Msc. Ing. Eduardo Carozo, Uruguay.

Autores de los "Talleres de Gestión de Incidentes"
- Ing. Gastón Franco, Argentina.

- Ing. Carlos Martinez, Uruguay.
- Ing. Alejandro Hevia, Chile.
- Ing. Felipe Troncoso, Chile.
- Dr. Jeimy Cano, Colombia.
- Ing. Andres Almanza, Colombia.

Estos materiales se desarrollaron entre Septiembre y Diciembre de 2009, conformando así la primera versión de cada uno. Esta primera versión fue integrada por el Director del Proyecto AMPARO, el Ing. Eduardo Carozo.

Simultáneamente se realizar una convocatoria a Proyectos de investigación, el 14 de Octubre de 2009.

El 12 de Noviembre de 2009, se cerró la convocatoria; recabándose 9 proyectos de diferentes países, a continuación el listado:

No.	Título de Proyecto	Organización	País
1	Implementación de IPv6- SEND para IP4JVM	Instituto de Computación / Facultad de Ingeniería / Universidad de la República	Uruguay
2	Planificación de Seguridad VoIP	Universidad Nacional de Río Cuarto – Departamento de Telecomunicaciones	Argentina
3	Detección de actividad maliciosa dentro de una red	LNXnetwork / HOLA PARAGUAY S.A.	Paraguay
4	Seguridad en Redes Oportunistas (SeRO)	Facultad de Ingeniería – Universidad de la República	Uruguay
5	Creación e Implementación de un CSIRT Académico para la Universidad Técnica Particular de Loja	UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	Ecuador
6	FACTOIDS: Modelos y Herramientas para el Análisis e Intercambio Seguro de Datos Colectados por Sensores	Universidad de la República, Facultad de Ingeniería, Instituto de Computación (INCO)	Uruguay
7	Desarrollo de un estándar para intercambio de información sobre incidentes	CABASE	Argentina
8	Diseño e Implementación de una Darknet para monitoreo de la red en Chile	CLCERT	Chile
9	Sistema de Autentificación en redes inalámbricas de la Universidad de los Andes	IDTIC, CA	Venezuela

Luego se realizó el proceso de evaluación de cada uno de los proyectos presentados, mismo que fue realizado por la Ing. Cristine Hoeppers y el Ing. José Luis Chávez Cortéz; presentándose los resultados el 14 de Diciembre de 2009 dónde se anunció los 5 proyectos seleccionados que fueron:

No.	Título de Proyecto	Organización	País

1	Seguridad en Redes Oportunistas (SeRO)	Facultad de Ingeniería – Universidad de la República	Uruguay
2	FACTOIDS: Modelos y Herramientas para el Análisis e Intercambio Seguro de Datos Colectados por Sensores	Universidad de la República, Facultad de Ingeniería, Instituto de Computación (INCO)	Uruguay
3	Diseño e Implementación de una Darknet para monitoreo de la red en Chile	CLCERT	Chile
4	Planificación de Seguridad VoIP	Universidad Nacional de Río Cuarto – Departamento de Telecomunicaciones	Argentina
5	Creación e Implementación de un CSIRT Académico para la Universidad Técnica Particular de Loja	UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	Ecuador

Según cronograma en el año 2010, se lleva a cabo, el:

Primer Taller de Expertos en Gestión de Incidentes de Seguridad Informática Montevideo, Uruguay (23 al 27 de Febrero 2010)

Fue una experiencia catalogada por los participantes como "Excelente y única en su género", dado que se logró un foro de 37 participantes expertos de los países: Argentina, Brasil, Colombia, México, El Salvador, Guatemala, Ecuador, Estados Unidos y Uruguay; que activamente participaron durante 5 días en la recepción y crítica constructiva del material presentado.

También se contó con la participación de Brian Sullivan como representante de OEA CICTE (Organización de Estados Americanos – Comité Interamericano contra el Terrorismo) quién realizó una presentación relevante sobre los esfuerzos que ellos han realizado para la formación de CSIRTs Gubernamentales en la región y así mismo ofreció gestionar para que se pueda apoyar al Proyecto AMPARO dentro de sus esfuerzos.

El material elaborado fue presentado por sus autores, otorgando una especial relevancia al Taller.

También se logró que el Steering Committee se reuniera en pleno por primera vez. Se realizaron tres sesiones de trabajo dónde se discutieron temas a fines del desarrollo del Primer Taller de Expertos, así como de la estrategia que se adoptaría para enfrentar el Taller de Ecuador y la conformación del material elaborado tomando en cuenta todos los comentarios brindados por los participantes. Dentro de los acuerdos relevantes se encuentran los siguientes:

- Hacer un esfuerzo en conjunto con el apoyo de los autores para conformar el Manual de Gestión de Incidentes de Seguridad Informática en una sola pieza y que también integre los comentarios brindados por los participantes del Primer Taller de Expertos que a consideración de los autores sean relevantes de incorporar.
- Realizar las gestiones adecuadas para que el material elaborado cumpla con las características de ser Público (Open Source).

Especial mención merece realizar, la transcripción de un documento que se llamó "**ACUERDO DE MONTEVIDEO**", creado el 27 de Febrero de 2010 y firmado por el

Steering Committee el mismo día, dónde expresa la alta motivación de los profesionales participantes del Primer Taller de Expertos y presenta la necesidad de establecer un foro de intercambio de información, buenas prácticas y experiencias. Reconoce, la necesidad de crear un espacio de trabajo para diseminar rápidamente información acerca de seguridad cibernética y responder más eficazmente a crisis, incidentes y amenazas a la seguridad de las redes de computadoras; el sentido de urgencia en fomentar el continuo incremento de la seguridad de las redes y sistemas de información ante las graves y perjudiciales amenazas que representan aquellos que podrían realizar ataques en el espacio cibernético con fines maliciosos y delictivos; dar continuidad a la promoción y apoyo en las distintas actividades que el Proyecto AMPARO organice.

Por acuerdo del Steering Committee respaldado por los autores del Manual de Gestión de Incidentes de Seguridad Informática y coordinado por el Ing. José Luis Chávez Cortéz se procedió a integrar el material en un solo documento. Se tuvo una ventana de tiempo de tres semanas para realizar la tarea. Se logró que los autores pudieran incorporar la mayoría de cambios/mejoras comentadas en las primeras dos semanas, quedando la última semana para que se integrara en una sola pieza todos los capítulos y quedar listos para presentar el material en una versión 1.1 para el siguiente Taller de Ecuador a realizarse en Marzo.

Taller Regional de Entrenamiento para Técnicos en Seguridad Informática
Quito, Ecuador (23 al 26 de Marzo 2010)

Se organizó en conjunto con AEPROVI (Asociación de Empresas Proveedoras de Servicios de Internet de Ecuador) y la Universidad Técnica Particular de Loja. Se logró la participación de 26 profesionales pertenecientes a los países de: Estados Unidos, Guatemala, Costa Rica, Colombia, Venezuela, Ecuador, Chile y Uruguay.

Como instructores del Proyecto AMPARO: Ing. Eduardo Carozo (Uruguay), Ing. Leonardo Vidal (Uruguay) e Ing. José Luis Chávez Cortéz (Guatemala).

La actividad fue dirigida por el Director del Proyecto AMPARO, dónde se presentó la primera versión integrada del Manual de Gestión de Incidentes de Seguridad Informática así como tres talleres Hands On.

Tanto AEPROVI (La Nueva Constitución y las Telecomunicaciones en Ecuador) como OEA CICTE (Presentación Institucional) brindaron presentaciones durante el evento, generando alto interés por parte de los participantes.

Es importante mencionar que la participación del OEA CICTE fue relevante debido a que estuvieron presentes George Soares (Gerente de Programa de Seguridad Cibernética) y Belisario Contreras (Asistente de Proyecto Seguridad Cibernética), los cuales presentaron los esfuerzos que han hecho y dónde ya incorporan dentro de su esfuerzo de conformación de CSIRTs no solo a los Gubernamentales sino también a los de la Iniciativa Privada, enmarcándose en un hecho que suma a los esfuerzos que el Proyecto AMPARO está llevando a cabo.

Se sentía una gran expectativa por parte de los participantes cuando se iniciaron los talleres de gestión de incidentes. Se vivió un clima participativo y de ansiedad de trabajo por parte de cada grupo que se conformó. Se logró con el apoyo de los instructores que los distintos grupos tuvieran la vivencia de los diversos escenarios planteados. Todos los participantes se mostraron muy motivados y satisfechos por los objetivos alcanzados.

Los Talleres Hands On provocaron un impacto fuerte en los participantes debido a la experiencia que se tiene por parte de los instructores ante el montaje de los ambientes colaborativos y la dirección de trabajo donde se involucraron todos los participantes. Sobrepaso largamente las expectativas de los participantes.

La evaluación general sobre la presentación magistral del contenido brindado fue catalogada como “Excelente”.

Los participantes interactuaron constantemente dentro del desarrollo del evento. Tanto que solicitaron crear una comunidad para interactuar en buenas y mejores prácticas donde participen los instructores del Proyecto Amparo y los participantes del evento.

El evento fue muy bien montado en el Ecuador, el apoyo de LACNIC, AEPROVI y La Universidad Técnica Particular de Loja fue particularmente importante, así como la ayuda por parte del Hotel Quito dónde se realizó el evento.

Dada la primera experiencia del Taller en Quito Ecuador se procedió a realizar las gestiones necesarias por parte del Director del Proyecto AMPARO y LACNIC hacia el Ing. Rubén Aquino (Director de UNAM CERT) y la Ing. Indira Moreno (Procuraduría General de la República de México) con la intención de coordinar las actividades necesarias para poder llevar a cabo el evento del 8 al 11 de Junio del 2010.

Es de destacar que en este evento se contaría con dos autores del Manual (Ing. Ruben Aquino e Ing. José Luis Chávez Cortéz), un autor de los Talleres de Gestión de Incidentes (Ing. Carlos Martinez) y tres integrantes del Steering Committe del Proyecto AMPARO (Ing. Indira Moreno, Ing. Eduardo Carozo e Ing. José Luis Chávez Cortéz), brindándole al evento un respaldo de participación alto a nivel de instructores y experiencias.

Taller Regional de Entrenamiento para Técnicos en Seguridad Informática
México DF, México (8 al 11 de Junio 2010)

El evento fue organizado por UNAM CERT y el Ing. Rubén Aquino, Director de UNAM CERT, participó durante toda la duración del evento como uno de los instructores. Se logró la participación de 47 profesionales pertenecientes a los países de: México, Guatemala, Costa Rica, Panamá y Uruguay.

Como instructores del Proyecto AMPARO: Ing. Eduardo Carozo (Uruguay), Ing. Rubén Aquino (México), Ing. Indira Moreno (México), Ing. Carlos Martinez (Uruguay) e Ing. José Luis Chávez Cortéz (Guatemala).

La actividad fue dirigida por el Director del Proyecto AMPARO, dónde se presentó el Manual de Gestión de Incidentes de Seguridad Informática así como tres talleres Hands On.

Juan Carlos Alonso estuvo en representación de LACNIC y realizó una presentación pertinente. También el Ing. Rubén Aquino realizó una presentación sobre el trabajo que viene desempeñando UNAM CERT.

Es de destacar el alto compromiso que presentaron los asistentes y su amplia participación durante el desarrollo del Taller. Se tuvo un clima de intercambio de información entre todos los que participaron en el evento.

Un importante número de participantes fue demostrando que tenían experiencias diversas en manejo de incidentes de seguridad informática, esto representó un plus dentro de las diversas experiencias presentadas durante el Taller.

- Durante la experiencia de los talleres realizados se observó un ambiente colaborativo con mucha motivación para desarrollar las diferentes actividades propuestas. Si bien es cierto para algunos representó un escenario típico del diario trabajo, para otros fue una experiencia de un posible ambiente real bajo gestación de un posible incidente de seguridad informática. Los participantes trabajaron muy comprometidos en la obtención y generación de resultados. Nuevamente se comprueba que esta parte del Taller deja un impacto fuerte en los participantes.

Dadas las propuestas que presentaron algunos de los participantes, se espera que algunos se sumen al Proyecto AMPARO, ya sea presentando ideas o iniciativas que enriquezcan el material.

Las instalaciones del Hotel estuvieron adecuadas a las necesidades del evento. El apoyo y compromiso recibido hacia el evento por parte de los representantes de UNAM CERT fue de destacar.

Se sigue demostrando la conveniencia de tener como sede un Hotel que brinde los servicios adecuados al evento del Proyecto AMPARO dado que evita atrasos y garantiza el adecuado desempeño del evento, tanto para los participantes como para los instructores.

Dadas las experiencias de los Talleres en los diferentes países de la región se continúa el trabajo enfocando esfuerzos a las distintas actividades pre-calendarizadas, en las cuales se impartirán por parte de los instructores del Proyecto los materiales elaborados en los países que solicitaron ser los pioneros en la recepción del material, de los cuales restan: República Dominicana y Chile. Dado el éxito obtenido en los tres primeros talleres se ha decidido incorporar un sexto taller en Colombia, en el presente año. Se constata que han quedado solicitudes para realizar nuevos talleres en: Panamá, Costa Rica, México (una segunda edición), Brasil, Perú y Uruguay.

V. Resultados y diseminación del Proyecto

Se ha comunicado a la Dirección del Proyecto, la puesta en marcha de dos CSIRT en Ecuador, como consecuencia de las capacitaciones brindadas:

1. El CSIRT de la Universidad Técnica Particular de Loja, primer Centro de Respuesta de Ecuadro
2. El CSIRT del Ejército Ecuatoriano, dependiente del Gobierno nacional.

Se ha recibido interés de parte de AEPROVI de promover un Centro de Respuesta para Organizaciones privadas.

De Costa Rica, el Instituto Costarricense de Electricidad, está iniciando la implementación de un CSIRT para su organización, como consecuencia de las capacitaciones brindadas.

Desde México, se han recibido algunas solicitudes de apoyo, sobre todo de algunas entidades académicas, y la solicitud de una organización privada de Monterrey para apoyar las iniciativas del Proyecto AMPARO.

Se han formado más de 110 técnicos con altas responsabilidades en gobiernos y/o empresas de más de 12 países y más de 20 organizaciones relevantes.

En relación al cumplimiento de los objetivos se detalla:

Objetivo:	Estado de cumplimiento:
Aumentar la capacidad regional de prevenir la ocurrencia de incidentes de seguridad informática	En trabajo: Tres países de cinco comprometidos, ya han recibido el material)
Desarrollar actividades de investigación aplicada que apoyen las prioridades regionales	En trabajo: Los proyectos han sido seleccionados y están a mitad de desarrollo
Promover la creación de CSIRTs a nivel de grandes organizaciones en los diferentes países de la región	En trabajo: En Ecuador se ha impulsado la creación de dos CSIRT, uno académico y otro del gobierno, En Costa Rica el Instituto Costarricense de Electricidad (ICE) ha decido implementar su CSIRT, En México se esperan novedades…
Desarrollar una plataforma regional de capacitación de expertos en Seguridad Informática	En trabajo, se desarrollará una aplicación web para este fin, se están colectando los técnicos para que exista masa crítica para la creación de los contenidos en el transcurso de los talleres
Contribuir al análisis sobre posibles modelos y posibilidades de constitución de un CSIRT Regional	No iniciado
Llevar adelante un programa regional de capacitación incluyendo el desarrollo de materiales y guías metodológicas	En trabajo, según cronograma establecido, tres talleres realizados de cinco acordados
Formación de formadores. Propiciar la formación de un grupo de profesionales en la región que puedan actuar como instructores	Finalizado, consecuencia del Taller de Expertos en Montevideo
Identificación de líderes y financiamiento para la difusión de buenas prácticas en la región	En curso, varios países están solicitando la visita de Proyecto AMPARO.

VI. Formación de Capacidades

Una de los mayores hallazgos, es la falta de comunicación entre los actores de seguridad dentro de los países visitados. Es sorprendente constatar el aumento de confianza e intercambio de información que se logran luego de los talleres, entre actores del gobierno, por ejemplo, técnicos de la justicia, de la policía, de las entidades financieras, las universidades, las empresas. Se entiende este aumento de comunicación como un

trascendente cambio y aumento de la capacidad de reacción de las organizaciones frente a ataques informáticos.

Tanto en Ecuador, como en México, se han formado personas con cargos relevantes, que entendiendo la problemática a la que se enfrentan, han establecido comunicaciones y relaciones de confianza, han entendido qué información deben colectar e intercambiar y permitirán sin duda mejorar la capacidad de respuesta nacional.

También han comprendido la relevancia de disponer de Centros de Respuesta y han definido dentro de sus prioridades, a través del conocimiento adquirido, recorrer las acciones necesarias para desarrollar proyectos para implementarlos en sus organizaciones.

VII. Impactos

El Equipo de proyecto evalúa que se está consiguiendo un impacto muy positivo en los países visitados, derivados principalmente de la alta capacidad de influencia de los participantes a los talleres. La mayoría de ellos tienen altas responsabilidades asignadas en las organizaciones en las que se desempeñan.

El Taller por su construcción incentiva a los participantes a llevar dichas prácticas a su vida diaria y los orienta a colaborar y apoyarse en sus pares, generando fuertes lazos de relacionamiento dentro del país en el que se desarrolla el mismo. A su vez los participantes internacionales que asisten visualizan ésta interacción e identifican la realización del Taller como una acción de alta trascendencia en su vida profesional.

Esta nueva capacidad de colaboración frente al manejo de incidentes, mejora sustantivamente la capacidad de las comunidades técnicas de hacer frente a las amenazas sobre los servicios que recibe la población a través de las TIC's, por lo que se espera incida muy favorablemente en el aumento de la confianza y accesibilidad por parte de la población a servicios de los gobiernos, empresas, etc.

VIII. Recomendaciones

Recomendaciones sobre el Manual de Gestión de Incidentes:

La evaluación general sobre la presentación magistral del contenido brindado tuvo los siguientes comentarios:

- Cubrió y superó las expectativas.
- Provechoso.
- Felicitan a los autores por la calidad y cantidad en su contenido.
- Contenido interesante y beneficioso.
- Traslado de experiencias que complementan y enriquecen.
- Iniciativa muy buena y excelente.
- Fomenta la cultura de seguridad de la información.

Las propuestas de mejora que se recibieron sobre el manual:

- Insertar más imágenes. Una imagen vale más que mil palabras.
- Fomentar más la pro actividad.

- Crear un Anexo con documentos que se puedan compartir con la comunidad, tales como: procedimientos y modelos.
- Presentar o agregar un directorio de CSIRTs en la región.
- Crear un marco histórico para que dé la importancia en la creación de un CSIRT.
- Incluir más ejemplos/casos de estudio.

Tomando las propuestas, se entiende que el Manual debería ser traducido a otros idiomas de la comunidad (Inglés, Portugués, Francés) e incluidas en una segunda edición más imágenes. El contenido se propone completarlo con dos capítulos adicionales a los ya existentes: Aspectos Legales de la Seguridad Informática y Entendiendo las acciones de un Hacker.

Como se ha dicho anteriormente se han iniciado contactos para la elaboración de dichos capítulos y se espera estén finalizados a fines de Agosto 2010.

Recomendaciones sobre lecciones aprendidas:

Se identifica que debemos de brindar un espacio para que los distintos participantes puedan compartir un artículo dónde transmitan sus experiencias e inquietudes. La intención inicial es de generar un espacio colaborativo, promotor e impulsor del Proyecto.

Proyecto AMPARO se está posicionando como un referente muy importante para el continente en Materia de Seguridad Informática y se hace necesario tomar medidas para canalizar adecuadamente los apoyos que se generen para garantizar la existencia del mismo, siempre siendo consistente con el cumpliendo de los objetivos por los que fue creado y se entiende que esta plataforma de compartición de información será clave para ello.

Recomendaciones sobre siguientes fases:

Se recomienda la necesidad de promover talleres del Proyecto AMPARO, en más países de la región, iniciando por aquellos que han expresado ya interés, como ser el caso de Panamá, Costa Rica, Perú, Argentina y Uruguay.

Se entiende además necesario (en base a solicitudes de los participantes) que se elaboren nuevos talleres adicionales, que incluya otros tipos de ataques maliciosos y técnicas de seguridad, y se informa que los más solicitados al momento son: ataques sobre servidores de DNS y Programación Segura.

Se constata un bajo nivel de desarrollo en las universidades de la región de proyectos de investigación en seguridad informática, por lo que se entiende necesario realizar un nuevo llamado, con más tiempo a proyectos, luego de cerrado el llamado actual.

ANEXO I: Proyectos de investigación en ejecución

#	TITULO	ORGANIZACIÓN	JEFE PROYECTO	PAIS	Monto solicitado
2	Planificación de seguridad VoIP	Universidad Nacional de Río Cuarto – Departamento de Telecomunicaciones	Rodrigo Gastón Prat	Argentina	8000
4	Seguridad en Redes Oportunistas (SeRO)	Facultad de Ingeniería – Universidad de la República	Leonardo Vidal Martínez	Uruguay	8000
5	Creación e Implementación de un CSIRT Académico para la Universidad Técnica Particular de Loja	Universidad Técnica Particular de Loja	María Paula Espinosa Vélez	Ecuador	8000
6	FACTOIDS: Modelos y Herramientas para el Análisis e Intercambio Seguro de Datos Colectados por Sensores	Universidad de la República, Facultad de Ingeniería, Instituto de Computación (INCO)	Carlos Martínez-Cagnazzo	Uruguay	8000
8	Diseño e Implementación de una Darknet para monitoreo de la red en Chile	CLCERT	Alejandro Hevia	Chile	8000