Taller regional sobre marcos para la ciberseguridad y la protección de la infraestructura básica de la información (PIBI)

Documento RWBA/2007/01-S
1 de noviembre de 2007
Original: English

Proyecto de Informe de la reunión : Taller regional sobre marcos para la ciberseguridad y la PIBI Buenos Aires, Argentina, 16-18 de octubre de 2007

Sírvanse enviar las observaciones que consideren oportunas sobre este proyecto de Informe de la reunión a cybmail(at)itu.int

Objecto del presente Informe

1. El Taller regional de la UIT sobre marcos para la ciberseguridad y la protección de la infraestructura básica de la información (PIBI) se celebró en Buenos Aires, Argentina, del 16 al 18 de octubre de 2007[1]. Este Taller forma parte de una serie de eventos regionales para la sensibilización y creación de capacidad en materia de ciberseguridad y ha sido organizado conjuntamente por el Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) y el Sector de Normalización de las Telecomunicationes de la UIT (UIT-T). El Taller tenía por objeto identificar los retos principales a los que tienen que enfrentarse los países de la Región de las Américas para desarrollar marcos y estrategias nacionales de ciberseguridad y de PIBI, estudiar las practices óptimas, compartir información sobre las normas técnicas y las actividades de desarrollo emprendidas por la UIT, así como por otras entidades, y examinar la función de los diversos protagonistas del fomento de la cultura de la ciberseguridad.

2. En este evento tomaron parte 60 personas aproximadamente procedentes de los países de la Región de las Américas y de otras partes del mundo. La documentación completa del Taller, en particular el orden del día definitivo y todas las presentaciones, se puede consultar en el sitio web de este evento www.itu.int/itu-d/cyb/events/2007/buenos-aires/. En el presente Informe se resumen los debates sostenidos durante estos tres días, se ofrece una visión general de alto nivel de las sesiones y de las ponencias presentadas, y se recogen algunos de los acuerdos y posturas communes alcanzadas en este evento.

Taller regional sobre marcos para la ciberseguridad y la protección de la infraestructura básica de la información celebrado en Buenos Aires, Argentina, del 16 al 18 de octubre de 2007

3. Pueden considerarse como antecedentes la dependencia cada vez mayor de la sociedad moderna con respecto a las tecnologías de la información y las comunicaciones (TIC), su interconexión a nivel mundial y el hecho de que los países sean cada vez más conscientes de la interdependencia que esto supone y de los riesgos que se afrontan y que deben controlarse a nivel nacional, regional e internacional. Por siguiente, la mejora de la ciberseguridad y la protección de la infraestructura básica de la información son indispensables para el bienestar económico y social y la seguridad de cada país. A nivel nacional, esto constituye una responsabilidad compartida que exige la coordinación de las medidas encaminadas a la prevención, preparación, respuesta y recuperación tras los incidentes, por parte de las autoridades estatales, el sector privado y los ciudadanos. A nivel regional e internacional, es necesaria la cooperación y coordinación con los socios pertinentes. La formulación y puesta en práctica de un marco nacional de ciberseguridad y de protección de la infraestructura básica de la información exige un planteamiento integral. En este evento se debatieron algunos de los elementos clave para el desarrollo de estos marcos.

Apertura de la reunion y bienvenida

4. El Taller regional sobre marcos para la ciberseguridad y la protección de la infraestructura básica de la información se inauguró con un discurso de bienvenida por parte del Sr. D. Gonzalo Heredia, Coordinador de los Programas Nacionales de la Sociedad de la Información, en representación del Sr. D. Carlos Lisandro Salas, Secretario de Comunicaciones, de la Secretaría de Comunicaciones, Argentina. En su discurso inaugural, el Sr. Heredia afirmó que la ciberseguridad y la protección de la infraestructura básica de la información constituyen

[1] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/

retos de la mayor importancia para la sociedad de la información a los que no es posible responder si no es con medidas concretas. Subrayó que, en Argentina, las TIC se están utilizando cada vez más y que por consiguiente hay que prestar cada vez más atención a las cuestiones relacionadas con la seguridad de Internet. Tanto los expertos en seguridad como los usuarios necesitan ser más conscientes de lo que está en juego y de lo que puede hacerse al respecto. Por ello, invitó a los participantes en el Taller a entablar debates, que esperaba fueran fructíferos y acertados, durante los tres días de duración del evento.

5. Tras el discurso de bienvenida a cargo del representante de la Secretaría de Comunicaciones, tuvo lugar el discurso de apertura[2] [3] a cargo del Sr. D. Mario Maniewicz, Jefe a.i. del Departamento de Políticas y Estrategias, Oficina de Desarrollo de las Telecomunicaciones, en representación del Director del UIT-D, Sr. Sami Al-Basheer, y del Director del UIT-T, Sr. Malcolm Johnson. En su discurso de apertura el Sr. Maniewicz señaló que este Taller constituye una excelente oportunidad para compartir experiencias y prácticas óptimas de respuesta a los desafiós a los que se enfrentan los países latinoamericanos y otras regiones cuando desarrollan marcos y estrategias en esta materia. Subrayó además que el Taller ofrecía la oportunidad de dar a conocer las Recomendaciones pertinentes del UIT-T y las actividades que, en materia de ciberseguridad, están realizando el Sector de Desarrollo de las Telecomunicaciones y el de Normalización de las Telecomunicaciones de la UIT. El Sr. Maniewicz agradeció el vivo interés de Argentina en las actividades de la UIT sobre ciberseguridad, y declaró que fue Argentina el primer país que se ofreció voluntario, sin dilación alguna, como anfitrión de este evento en la Región latinoamericana, cuando se anunciaron por primera vez los planes de celebración del mismo.

6. El Sr. Maniewicz destacó la calidad del sobresaliente plantel de expertos y oradores presentes en el Taller e invitó a todos los participantes a que se aprovecharan de la presencia de los mismos así como de la de sus homólogos de los países de las Américas y de otras regiones, mediante la participación activa en las sesiones del Taller compartiendo opiniones y experiencias y planteando las cuestiones o problemas que pudieran suscitarse durante los debates. Señaló asimismo que la participación y contribución activa de los asistentes al Taller constituía en última instancia la base del éxito del evento.

Sesión 1: ¿Qué es un marco para la ciberseguridad y la protección de la infraestructura básica de la información?

7. La necesidad de generar confianza y seguridad en la utilización de las TIC, fomentar la ciberseguridad y proteger las infraestructuras básicas en el plano nacional goza de un reconocimiento general. A medida que los actores de los sectores público y privado dan su propia visión con respecto a la importancia que tienen las distintas cuestiones, para contar con un enfoque coherente, algunos países han establecido estructuras en forma de marcos institucionales para la ciberseguridad y la PIBI mientras que otros han empleado un enfoque más liviano y no institucional. En esta sesión se debatieron el concepto de marco nacional para la ciberseguridad y la PIBI y los trabajos de la UIT en curso para desarrollar este marco de prácticas óptimas.

8. El Sr. Robert Shaw, de la División de Aplicaciones de las TIC y Ciberseguridad, Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT -D), actuó de moderador en esta sesión en la que se pretendía examinar, desde una perspectiva abierta, distintos planteamientos de los marcos de la ciberseguridad, de la PIBI y de sus componentes, a menudo semejantes, a fin de ofrecer a los asistentes a la reunión una visión de las cuestiones y retos implicados. El Sr. Shaw ofreció una visión general de las "actividades del UIT-D en el ámbito de la ciberseguridad y la PIBI"[4] y comentó diversos detalles del Programa de Trabajos del UIT-D en materia de ciberseguridad para ayudar a los países en desarrollo (2007-2009)[5]. Entre las iniciativas de la UIT en materia de ciberseguridad, en curso y proyectadas, a las que aludió se encuentran: las actividades encaminadas a la identificación de prácticas óptimas para la creación de marcos nacionales para la ciberseguridad y la PIBI, una herramienta de autoevaluación de la preparación nacional en materia de ciberseguridad/PIBI, una herramienta para combatir los virus del tipo *botnet*, publicaciones con directrices sobre ciberseguridad para los países en desarrollo, un estudio internacional sobre capacidades nacionales en materia de ciberseguridad/CSIRT, una herramienta con un modelo de legislación contra la ciberdelincuencia destinada a los países en desarrollo, una herramienta de promoción de la cultura de la ciberseguridad así como varios Talleres regionales en proyecto para la creación de capacidades y la sensibilización sobre los marcos para la ciberseguridad y la PIBI.

9. El Sr. Shaw afirmó que en la mayor parte de los países aún no se han formulado, ni puesto en práctica, estrategias nacionales de ciberseguridad y protección de la infraestructura básica de la información y que la disponibilidad limitada de recursos humanos, institucionales y financieros en los países en desarrollo constituía un obstáculo especialmente difícil para la elaboración y aplicación de estas políticas. Indicó asimismo que en el Sector de Desarrollo de las Telecomunicaciones de la UIT existe actualmente una Comisión de Estudio que está elaborando un documento de prácticas óptimas con una propuesta de marco par alas actividades nacionales en materia de ciberseguridad vinculada estrechamente con el *Programa de Trabajos del UIT-D en materia de ciberseguridad para ayudar a los países en desarrollo.* En este *Programa de Trabajos* se expon los planes de la UIT para ayudar a los países a desarrollar su capacidad en materia de ciberseguridad/PIBI, ofreciendo a los Estados Miembros, entre otras cosas, recursos y herramientas de interés sobre temas afines. Cuando estas herramientas hayan alcanzado el grado de madurez suficiente, el UIT-D las hará llegar, por diversos medios, a

[2] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/opening-remarks-itu-buenos-aires-16-oct-07.pdf
[3] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/opening-remarks-itu-buenos-aires-16-oct-07-s.pdf (Español)
[4] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/shaw-itu-d-cybersecurity-overview-buenos-aires-oct-07.pdf
[5] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

los 191 Estados Miembros de la UIT. El Sr. Shaw indicó que una de las dificultades para el progreso de los debates en materia de ciberseguridad era la búsqueda de los mecanismos adecuados que facilitaran la comunicación entre los diferentes actors, debido a que cada grupo de ellos tenía necesidades diferentes y específicas en cuanto a los niveles de confianza necesarios para compartir determinadas informaciones.

10. El Sr. Daniel Hurley, del Ministerio de Comercio, Administración Nacional de Telecomunicaciones e Información (NTIA, *National Telecommunications and Information Administration (NTIA), United States of America*), Estados Unidos de América, tomó la palabra acto seguido presentado el trabajo *Framework for National Cybersecurity Efforts* (Marco para los trabajos en materia de seguridad nacional) que está siendo elaborado actualmente en el seno de la Comisión de Estudio 1, Cuestión 22, del UIT-D con su presentación sobre "Creación de capacidades en materia de ciberseguridad : Presentación de las prácticas óptimas en materia de ciberseguridad"[6]. Este marco es uno de los componentes del trabajo llevado a cabo por la Comisión de Estudio que fue propuesto en un Informe sobre *Prácticas óptimas para la organización de las actividades en materia de ciberseguridad nacional* y que pueden usar los gobiernos como directrices para la aplicación de estrategias nacionales en materia de ciberseguridad y PIBI. En el *Marco para las actividades en materia de ciberseguridad nacional* se contemplan cinco componentes principales par alas prácticas óptimas en materia de ciberseguridad, a saber: el desarrollo de una estrategia nacional de ciberseguridad, la colaboración entre la administración y la industria, la represión de la ciberdelincuencia, el desarrollo de capacidades de resolución de incidentes a nivel nacional y una cultura nacional de la ciberseguridad. En el proyecto de Informe figura una declaración de política para cada uno de los componentes del marco, se identifican metas y pasos específicos para alcanzarlas, así como referencias y documentación adicional relacionada con cada paso específico. El Informe *Prácticas óptimas para la organización de las actividades nacionales en materia de ciberseguridad*, y especialmente el marco, constituye un documento vivo que evolucionará con el tiempo. El Sr. Hurley hizo hincapié en la importancia de coordinar globalmente todos los programas nacionales de ciberseguridad al máximo nivel de las administraciones de cada país para asegurar su efectividad. El Sr. Hurley cerró su discurso citando los apéndices y anexos de intéres de la *Cuestión 22/1 de la Comisión de Estudio 1 del UIT-D Proyecto de Informe sobre prácticas óptimas recomendadas en material de ciberseguridad*[7] que está disponible en el sitio web del UIT-D.

11. El Sr. Phil Sodoma, del Trustworthy Computing Group, Microsoft Corporation, efectuó a continuación una presentación titulada "Reglas de resistencia: 7 pasos para dotar de resistencia a la protección de la infraestructura básica"[8]. El objeto del planteamiento de las reglas de resistencia presentadas es ofrecer un conjunto de elementos de prácticas óptimas de diversas regiones del mundo, adoptadas por lo gobiernos. Inspirados en estos principios orientadores, los gobiernos, los propietarios de las infraestructuras y sus operadores pueden colaborar en la búsqueda de un conjunto de activadores básicos de resistencia y potenciadores de la infraestructura.

12. Los siete pasos son los siguientes: 1) Definir metas y funciones. La definición de metas claras es esencial para obtener al apoyo para la ciberseguridad por parte de los diversos grupos interesados, mientras que la comprensión de las diversas funciones de las partes interesadas fomenta la coordinación, la eficacia y la confianza. 2) Identificar y priorizar las funciones básicas. Es necesario colaborar estrechamente para entender las interdependencias implicadas. El Sr. Sodoma animó a los países a que establecieran un diálogo abierto para comprender las funciones básicas, los elementos de la infraestructura y los recursos clave necesarios para la prestación de los servicios esenciales, manteniendo al mismo tiempo las operaciones regulares de la economía y contribuyendo a afianzar la seguridad pública. 3) Evaluar y gestionar continuamente los riesgos, ya que la protección consiste en la aplicación continua de la gestión de riesgos. 4) Establecer y ejecutar planes de emergencia y mejorar la coordinación operacional. Los planes de respuesta ante emergencias pueden reducir los daños y fomentar la resistencia. 5) Crear asociaciones públicas-privadas. El Sr. Sodoma expuso las rezones por las que no se debe subestimar la importancia de las asociaciones públicas-privadas. La creación de relaciones de confianza es indispensable para la compartición de información y el desarrollo de soluciones para problemas difíciles mientras que la potenciación de las aptitudes exclusivas de la administración y de las organizaciones del sector privado es necesaria para hacer frente al entorno de amenazas dinámicas existente hoy en día. 6) Integrar la seguridad/resistencia en las operaciones, ya que la seguridad debe ser un proceso continuo. 7) Actualizar e innovar las tecnologías/procesos. Aunque las amenazas de índole informática estén en permanente evolución, los encargados de la formulación de políticas, los propietarios de las empresas y los operadores de las infraestructuras están aún a tiempo de prepararse para estas amenazas y reducirlas manteniendo actualizadas las tecnologías que utilizan.

13. El Sr. Sodoma expusó asimismo a los participantes su visión de los posibles obstáculos para la implementación de un programa y estrategia nacional de ciberseguridad/PIBI. Entre ésto citó los obstáculos de índole económica, el tiempo de transición lógicamente necesario para asegurar las infraestructuras y mencionó el ejemplo de los aviones y el control de tráfico aéreo donde la experiencia acumulada hacía posible evitar en última instancia la caída de los aviones en pleno vuelo. Subrayó la necesidad de montar en algunas ocasiones lo que podría denominarse "un teatro de la seguridad" para despertar la conciencia política sobre los riesgos y la necesidad de adoptar medidas para reducirlos. El Sr. Sodoma señaló asimismo que la falta de cooperación entre

[6] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/hurley-building-cybersecurity-capacity-buenos-aires-oct-07.pdf
[7] http://www.itu.int/md/D06-SG01-C-0130/en
[8] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/sodoma-resiliency-rules-buenos-aires-oct-07.pdf

países, e incluso dentro de un propio país, constituye un obstáculo de la mayor importancia, si no el más importante, para implementar con éxito un programa y estrategia nacional de ciberseguridad/PIBI. Hizo hincapié asimismo en que la única manera de conseguir un progreso eficaz para mejorar la seguridad consistía en allanar estos obstáculos y fomentar la comunicación entre los propios órganos de la administración.

14. El Sr. Sodoma mencionó asimismo que en muchos países carecen de los conocimientos necesarios para saber qué hacer y qué dirección tomar a partir de su propia situación específica, y destacó que la herramienta de la UIT para la autoevaluación de la ciberseguridad/PIBI nacional constituía un medio excelente de abordar este problema. Indicó además que una de las misiones de los gobiernos es la evaluación de los riesgos y que la función de las asociaciones públicas-privadas es definir los puntos básicos mientras que la de los operadores de infraestructuras consiste en priorizar los riesgos. El Sr. Sodoma puso fin a su presentación señalando que, anteriormente, la seguridad de las empresas se consideraba una cuestión tecnológica pero que en los últimos años se ha producido una evolución, y ahora se acepta con carácter general la necesidad de un planteamiento de la seguridad en varias capas y más amplio. También apuntó que los programas informáticos desarrollados hace 10 años no se diseñaron para el entorno de amenazas actual, por lo que es de vital importancia utilizar siempre la última versión disponible del software y del hardware.

Sesión 2: Desarrollo de una estrategia nacional

15. Las redes electronicás se utilizan cada vez más con fines delictivos, o para objetivos que pueden dañar la integridad de las infraestructuras básicas y crear obstáculos que impidan la extensión de los beneficios de las TIC. Para hacer frente a estas amenazas y proteger las infraestructuras, cada país precisa un *plan de acción global* en el que se aborden las cuestiones técnicas, jurídicas y de política, junto con una cooperación regional e internacional. ¿Qué cuestiones habría que examinar en el marco de una estrategia nacional para la ciberseguridad y la protección de la infraestructura básica de la información? ¿A qué actores se debería implicar? ¿Existen ejemplos de marcos que puedan adoptarse? En esta sesión, moderada por el Sr. D. Gonzalo Heredia, Coordinator de los Programas Nacionales de la Sociedad de la Información, Secretaria de Comunicaciones, Argentina, se trato de examinar con más detenimiento varios enfoques, de establecer las prácticas óptimas, y de identificar los elementos fundamentales que podrían ayudar a los países de la region de las Américas a crear estrategias nacionales para la ciberseguridad y la protección de la infraestructura básica de la información.

16. En la primera presentación de la Sesión 2, el Sr. D. Carlos Achiary, Director de la Oficina Nacional de Tecnologías de Información (ONTI), Subsecretaría de la Gestión Pública, Argentina, en su ponencia titulada "Desarrollo de una Estrategia Nacional",[9] expuso ciertas ideas sobre los retos que comporta el desarrollo de una estrategia nacional para la ciberseguridad y la PIBI, citando ejemplos específicos de Argentina y de la region. Manifestó que hoy en día el ciberespacio es un nuevo campo de acción en el que algunas de las actuaciones son legales y otras no, y donde los ciudadanos, las empresas privadas, las organizaciones y los gobiernos buscan por igual nuevas maneras de potenciar las TIC. Debido a ello, el papel que los gobiernos tienen que desempeñar para que el ciberespacio sea un lugar más seguro y fiable, adquiere cada vez más importancia. El Sr. Achiary destacó algunos de los ámbitos en los que Argentina está desarrollando sus esfuerzos para desarrollar una estrategia nacional integral para la ciberseguridad. Reconoció la importancia de la buena cooperación y coordinación entre los organismos nacionales implicados, y la importancia, una vez organizado el país internamente a nivel nacional, del aspecto internacional de la cooperación frente a las amenazas para la creación de capacidad de respuesta, est. que no deben subestimarse. Debe considerarse además la comunicación entre los actores de los sectores público y privado y los ciudadanos dentro de cada país, sin menoscabo de la indispensable función coordinadora que los gobiernos deben asumir.

17. En su Informe sobre la situación actual en Argentina, señaló que el país se encuentra aún en una etapa inicial e inmerso en el studio de las medidas que habría que adoptar tanto a corto como a largo plazo. Antes o después deberá introducirse un cambio en la legislación, lo que compete exclusivamente al gobierno. Muchas veces también el gobierno es el principal representante del país en los foros internacionales. Señaló que la Oficina Nacional de Tecnologías de la Información (ONTI), que es el órgano administrativo responsible de las TIC, es la encargada de coordinar estos trabajos. Asimismo indicó que ArCERT es el único equipo de respuesta ante incidentes de seguridad informática (CSIRT, *computer security incident response team)* y el único equipo de respuesta ante emergencias informáticas (CERT, *computer emergency response team)* de Argentina, y que lleva funcionado desde 1999. ArCERT está encargado del sector público federal, aunque se le pide que ayude a otros sectores de la administración y al sector privado. No obstante, señaló, ArCERT no es formalmente un CERT nacional. Además de sus actividades en material de cooperación internacional en el marco de la OEA y de asumir la representación en las actividades de ciberseguridad de la UIT, se han establecido otros contactos regionales. Declaró asimismo que Argentina ha desarrollado una política modélica de ciberseguridad y que actualmente se está debatiendo en el Congreso un proyecto de ley sobre ciberdelincuencia que, en caso de aprobarse, provocaría la modificación del código penal argentino. Afirmó que Argentina deseaba incrementar la colaboración en materia de ciberseguridad en todos los aspectos así como desempeñar un papel activo en el Taller de ciberseguridad de la UIT.

[9] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/achiary-argentina-national-cybersecurity-strategy-buenos-aires-oct-07.pdf

18. El Sr. Bradford Willke, CERT/CC, del Software Engineering Institute (SEI), Estados Unidos de América, comenzó su presentación sobre el "Diseño de la ciberseguridad nacional y de la protección de la infraestructura básica de la información"[10] considerando algunos de los impedimentos nacionales y multinacionales para la ciberseguridad. Señaló que, cuando se trata de la orientación a objetivos, la ciberseguridad, la continuidad de la actividad de los negocios y las operaciones de las TIC soportan la protección de la infraestructura básica de la información (es decir, proporcionan elementos de resistencia), aunque a menudo se ejecutan independientemente unos de otros. Por otra parte, cuando se considera el aspecto del reconocimiento del problema, el campo de la ciberseguridad y la PIBI tiende a centrarse en soluciones técnicas con preferencia a las de gestión y, por consiguiente, se difumina el planteamiento auténticamente orientado al proceso. Así pues, en su opinion, las naciones tienen una convicción de preparación sin fundamento y esta preparación solo se pone a prueba realmente cuando se produce un evento perturbador. Por ortra parte, a pesar de la abundancia de códigos de prácticas, rara vez se mide la efectividad de éstas. En conjunto, afirmó el Sr. Willke, hay pocas referencias fiables que permitan determiner la capacidad de una nación para proteger la infraestructura básica de la información.

19. Un buen punto de partida para los países que se disponen a desarrollar una estrategia nacional y un programa para la cibeseguridad y la PIBI es la autoevaluación con respecto a un marco común. En esta fase, las preguntas básicas que cabe plantearse tienen por objeto profundizar en la comprensión de los siguientes aspectos: "¿Cuál es el camino? (¿Hay un marco al que ajustarse?)", "¿Cuál es el destino? (¿Hasta qué punto debe implementarse dicho marco?)" y "¿Dónde estamos? (¿Cuánto ha avanzado el país en la implementación de este marco?)". El Sr. Willke subrayó que el "destino" viene determinado por las capacidades y la madurez del proceso que un país debe poner en marcha para gestionar los riesgos inadmisibles. Por otra parte, para que el proceso pueda mejorar realmente es necesario establecer procedimientos claros par las comunidades expertas en este ámbito. A este respecto, es necesario que los países conozcan major su possible respuesta cuando se encuentran en dificultades o ante un ataque, así como la madurez de la misma y de su cultura en este ámbito. También es importante que en el país se pueda aplicar un proceso repetidas veces, y que se disponga de herramientas de medición de la calidad de sur respuesta en cuanto a gestión del riesgo. El Sr. Willke subrayó que el planteamiento de cada país sería distinto, debido a sus diferentes metas, objetivos y sectores que se consideran básicos. Indicó que "aprender de los errores" no es el major método de aprendizaje pero que, a falta de otro remedio, puede constituir una buena experiencia de aprendizaje tanto desde un punto de vista de política como de gestión. En particular, es necesario estudiar "lo que se necesitará la próxima vez". Finalizó su presentación diciendo que hay marcos de diversos tamaños y formas y que la major manera de comenzar consiste en identificar el marco que major responde a las necesidades específicas del país.

20. Fred Clark, de la Superintendencia de Telecomunicaciones, Guatemala, presentó a continuación un estudio de caso práctico de su país sobre "la ciberpreparación en Guatemala"[11]. En esta presentación informó a los delegados de la situación actual de Guatemala y de la transformación que está experimentando la sociedad gracias a la introducción de las TIC en todos los aspectos cotidianos de la vida de los ciudadanos. El Sr. Clark presentó varios ejemplos extraídos de un estudio realizado en 2007 sobre la penetración y la adopción de Internet y de las tecnologías de información y comunicaciones en la República de Guatemala. Estos ejemplos demostraban la necesidad de concienciar a los usurios y a las empresas conectadas a Internet de las amenazas que son cada vez mayors debido a la creciente inseguridad del ciberespacio.

21. Abundando en los contenidos de las exposiciones realizadas en las dos sesiones del taller en la que se presentaban marcos para la ciberseguridad y la PIBI y diversas estrategias y planteamientos nacionales, el Sr. Joseph Richardson, de los Estados Unidos de América, en su presentación sobre "Marco de gestión para organizar los trabajos de ciberseguridad nacional: Herramienta de autoevaluación"[12] describió los elementos de los trabajos en curso de la UIT destinados a desarrollar una "herramienta integral de autoevaluación de la preparación para la ciberseguridad/PIBI nacional[13]. La herramienta de autoevaluación de la cyberseguridad/PIBI nacional de la UIT consituye una de las sinergias clave entre los trabajos de la Cuestión 22/1 de la Comisión de Estudio 1 del UIT-D sobre "Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad "[14] y las actividades del Programa de trabajos en materia de ciberseguridad de la UIT para ayudar a los países en desarrollo (2007-2009)[15] y aplica el marco que está desarrollándose en la Comisión de Estudio como herramienta eminentemente práctica para su utilización a nivel nacional. Esta herramienta puede ayudar a los gobiernos a examinar las políticas, procedimientos, normas, instituciones y demás elementos nacionales necesarios para la formulación de las estrategias de seguridad en el entorno permanentemente dinámico de las TIC. Asimismo puede ayudar a los gobiernos a conocer los sistemas existentes, identificar carencias que requieran especial atención y priorizar las actividades de respuesta del país. En esta herramienta se contemplan el nivel de gestión y el de política para cada uno de los cinco elementos del marco de prácticas óptimas presentado por el Sr. Hurley en la Sesión 1 del Taller, a saber: 1) estrategia nacional,

[10] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/willke-ciip-buenos-aires-oct-07.pdf
[11] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/clark-e-Readiness-guatemala-buenos-aires-oct-07.pdf
[12] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/richardson-national-cybersecurity-ciip-self-assessment-buenos-aires-oct-07.pdf
[13] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
[14] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html
[15] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

2) represión de la ciberdelincuencia, 3) capacidades de gestión de los incidentes a nivel nacional, 4) colaboración entre la administración y el sector privado, y 5) una cultura de la ciberseguridad, las instituciones necesarias, así como las relaciones entre administración, la industria y otras entidades del sector privado.

22. El Sr. Richardson subrayó en esta presentación que, en lo que se refiere a las iniciativas en materia de ciberseguridad y protección de la infraestructura básica de la información, no hay ningun país que empiece de cero. Además, no existe una única respuesta correcta ni un único planteamiento correcto ya que todos los países tienen sus necesidades peculiars y sus conveniencias exclusivas. Es necesario examinar y revisar continuamente el planteamiento adoptado, independientemente de cuál sea éste. Además es importante implicar a todos los interesados, en función de sus cometidos, en el desarrollo de una estrategia nacional para la ciberseguridad y la PIBI. El Sr. Richardson indicó que en el sitio web del UIT-D sobre ciberseguridad (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html) hay actualizaciones de la herramienta y recursos relacionados, y que se están desarrollando proyectos pilotos en alguno países para probar y evaluar la herramienta y, además, la UIT va a organizar una serie de talleres regionales sobre creación de capacidad que se impartirán en 2007, 2008 y 2009.

23. Al concluir el primer día del Taller, los participantes en el mismo y los organizadores locales fueron invitados a un cóctel ofrecido por CISCO.

Sesión 3: Normas técnicas en materia de ciberseguridad

24. Las organizaciones de normalización cumplen una función importante cuando se hace frente a las vulnerabilidades de las TIC. En la sesión 3 del Taller, moderada por el Sr. Paolo Rosa de la División de Seminarios y Promoción, Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T), se presentaron algunas de las principales actividades de las organizaciones de normalización (SDO), con especial énfasis en el UIT-T, y se examinaron aspectos como arquitectura de la seguridad, ciberseguridad, gestión de seguridad, gestión de identidades, seguridad básica para operadores de red y la Guía de normas de seguridad de las TIC, a creada por una Comisión de Estudio del UIT-T.

25. El Sr. Rosa abrió el debate sobre normas con la presentación "UIT-T: Ciberseguridad y Normas"[16], que ofrece una visión general de la estructura del UIT-T y de las actividades pertinentes en materia de seguridad. El Sr. Rosa explicó la importancia de los trabajos realizado en el seno de las Comisiones de Estudio del UIT-T y la forma en que estos se integran en los trabajos de la UIT y destacó algunas de las actividades de la comisión de Estudio 17 del UIT-T, que es la principal Comisión de Estudio del UIT-T encargada de la seguridad. También se explicaron los componentes de la seguridad en el UIT-T, entre los que se encuentran las Recomendaciones de la serie X.800 (marco de la arquitectura de seguridad), la Recomendación X.805, las Recomendaciones de la serie X.1000 (seguridad de las telecomunicaciones), las Recomendaciones de la serie Y.2700 (seguridad de las NGN), etc. El Sr. Rosa también mencionó algunas actividades relacionadas con la seguridad y la gestión de identidades emprendidas por el Grupo temático sobre gestión de identidades (IdM)[17] del UIT-T. Hasta la fecha, este Grupo ha elaborado cuatro informes principales: un informe que identifica requisitos a partir de base en casos hipotéticos, otro informe que identifica componentes genéricos del marco de la IdM; un análisis de las carencias en materia de normalización para identificar nuevos campos de trabajo en el ámbito de la normalización que deben ser cubiertos por las Comisiones de Estudio del UIT-T y otras SDO, y una lista permanentemente actualizada de los organismos … en materia de IdM.

26. El Sr. Mike Harrop, Relator del Proyecto sobre seguridad de las comunicaciones de la Comisión de Estudio 17, presentó a los participantes en el Taller una visión más profunda sobre las "Iniciativas del UIT-T en materia de seguridad de redes"[18]. El Sr. Harrop mostró cómo las actividades del UIT-T en materia de normas de seguridad se encuadran en el campo global de las normas sobre seguridad, destacando algunos de los temas clave de trabajo del Grupo de Trabajo 2 de la CE 17 y de la Cuestión 15 de la CE 13 e informó de los resultados alcanzados mediante proyectos concretos de la CE 17 sobre seguridad y otras actividades de divulgación. Por ejemplo, el Manual del UIT-T sobre seguridad en las tecnologías de las telecomunicaciones y la información[19] ofrece una visión general de las actuales Recomendaciones del UIT-T para comunicaciones seguras. El Compendio sobre seguridad[20] es un catálogo de Recomendaciones del UIT-T aprobadas', que versan sobre la seguridad de las telecomunicaciones. La recientemente publicada Guía de normas de seguridad[21] (v.2, 2007) es un recurso en línea sobre normas de seguridad elaborado por la UIT con la colaboración del Organismo Europeo de Seguridad de las Redes y la Información (ENISA) y el Grupo Rector de Seguridad de las Redes y de la Información (NISSG). La Guía consta de cinco partes: La 1ª partecontiene información sobre organizaciones que trabajan en normas de seguridad de las TIC, la 2ª parte es una base de datos con las normas de seguridad existentes, en la 3ª parte se enumeran proyectos actualmente en ejecución (o enlaces a los mismos) y normas que se están elaborando, la 4ª parte identifica las necesidades futuras y las nuevas normas propuestas y la 5ª parte enumera las prácticas óptimas en materia de seguridad. El Sr. Harrop mencionó también que la Comisión

[16] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rosa-itu-t-cybersecurity-and-standards-buenos-aires-oct-07.pdf
[17] http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html
[18] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/harrop-itu-t-network-security-buenos-aires-oct-07.pdf
[19] http://www.itu.int/pub/T-HDB-SEC.03-2006/en
[20] http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090001MSWE.doc
[21] http://www.itu.int/ITU-T/studygroups/com17/ict/

de Estudio 17 está creando una Red para el intercambio de normas de seguridad (SSEN, *Security Standards Exchange Network*) a fin de mantener un diálogo permanente sobre los principales temas de normalización de la seguridad.

Sesión 4: Vigilancia, alerta y respuesta en caso de incidente

27. Una actividad clave cuando se contempla la ciberseguridad a nivel nacional consiste en prepararse para los incidentes, detectarlos, gestionarlos y responder en caso de que ocurran, mediante la creación de capacidades de vigilancia, alerta y respuesta ante incidentes. Para una gestión eficaz de incidentes es necesario considerar la financiación, los recursos humanos, la formación, la capacidad tecnológica, las relaciones entre la administración y el sector privado y los requisitos jurídicos. Es necesario que en todos los niveles de la administración se colabore con el sector privado, la universidad y las organizaciones regionales e internacionales a fin de despertar la conciencia sobre los posibles ataques y los pasos que se deben seguir para contrarrestarlos. El Sr. Rómulo Dantas del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos actuó como moderador de esta primera sesión del segundo día del Taller, en la que se debatieron las prácticas óptimas y normas afines sobre los aspectos técnicos, de gestión y financieros de la creación de capacidades nacionales o regionales de vigilancia, alerta y respuesta ante incidentes.

28. El Sr. Jason Rafail del CERT/CC, del Software Engineering Institute (SEI), Universidad Carnegie Mellon de Estados Unidos de América, inauguró la sesión con una presentación que ofrecía una "Visión panorámica de la Comunidad CERT/CC y CSIRT"[22]. El Sr. Rafail recalcó que los países necesitan garantizar el acceso a la infraestructura nacional y el funcionamiento de ésta durante los ataques y que los CSIRT deben cumplir una función importante a este respecto. La anticipación y el establecimiento de una cultura de la seguridad son fundamentales para la protección de la infraestructura nacional de la información. Fomentar la creación de CSIRT nacionales forma parte de la solución a nivel nacional. Los CSIRT nacionales proporcionan un canal para las comunicaciones y la coordinación, y una meta sería crear al menos un CSIRT coordinador en cada país. En el mundo existen actualmente cerca de 40 CSIRT nacionales. Entre los servicios que proporcionan los CSIRT nacionales se cuentan los servicios técnicos (como coordinación, servicios de alerta, publicaciones técnicas, análisis de incidentes, análisis de vulnerabilidad, análisis documental, análisis forenses, formación, etc.) y los servicios no técnicos (como servicios de alerta, publicaciones destinadas a los usuarios e información general sobre seguridad e informática). El Sr. Rafail explicó porqué es necesario crear asociaciones para evitar incidentes y responder acertadamente a éstos.

29. Todos los participantes y partes interesadas implicada necesitan comprender mejor la forma en que el empleo de las tecnologías de la información y la comunicación afecta sus actividades empresariales cotidianas. Al tiempo que ponía de relieve que las personas necesitan conocer las herramientas de seguridad existentes y buen acceso a las mismas, el Sr. Rafail mencionó algunos recursos y herramientas de formación en línea sobre seguridad que los participantes podrían llevarse a sus países. Entre estos recursos se cuentan: El Virtual Training Environment (entorno de formación virtual) (VTE)[23], que es una biblioteca prácticas óptimas sobre informática judicial y la seguridad de la información y el Secure Coding Training (formación sobre codificación segura)[24], que es un recurso que tiene por objeto mejorar las aptitudes y capacidades de los progamadores.

30. En su presentación "Honduras – Una visión general"[25], el Sr. Ricardo Woolery, de CONATEL, Honduras, informó a grandes rasgos del desarrollo de las TIC en Honduras así como de la situación actual de la seguridad en tres sectores diferentes de la economía: la administración, las instituciones académicas y centros de enseñanza y las entidades financieras. El Sr. Woolery declaró que, en su calidad de regulador de las telecomunicaciones, CONATEL, la Comisión nacional de telecomunicaciones, exige que cada operador dote a sus redes de mecanismos de seguridad. Además, órgano de la Administración formula su propia estrategia de TI para proteger sus redes y en lo que respecta a las instituciones académicas del país, se percibe que las universidades han creado sus propias redes para ofrecer servicios (como portales universitario, bibliotecas electrónicas, servicios administrativos, puntos de acceso, etc.), y la seguridad es un elemento fundamental de la mayor parte de ellas, si no de todas. En cuanto a las entidades financieras, algunos bancos han certificado sus redes y se están aplicando medidas para proteger las cuentas bancarias de los clientes. Sin embargo, el Sr. Woolery señaló que en términos generales aún hace falta establecer en el país una estrategia integradora en materia de ciberseguridad o un marco general que permita alcanzar un consenso respecto a las políticas a nivel nacional y sectorial.

31. La siguiente presentación corrió a cargo del Sr. D. Gastón Franco de ArCERT, Oficina Nacional de Tecnologías de Información (ONTI), Argentina, quien informó del mandato y las actividades de "ArCERT"[26], primer y único CSIRT de Argentina. El Sr. Franco también mencionó que se había designado a ArCERT ante el CICTE como punto de contacto nacional en materia de ciberseguridad y que ArCERT se intersaba vivamente en la creación de otros CSIRT en Argentina y en otros países de la región. El equipo también participa activamente en

[22] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rafail-buenos-aires-oct-07.pdf

[23] http://www.vte.cert.org/
[24] http://www.cert.org/secure-coding/
[25] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/woolery-honduras-overview-buenos-aires-oct-07.pdf
[26] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/franco-arCERT-buenos-aires-oct-07.pdf

foros internacionales afines sobre gestión y respuesta ante incidentes. Entre las principales actividades preventivas del ArCERT se encuentran la oferta de formación, asesoría en políticas, alertas y divulgación de información, así como otros servicios y productos relacionados con la seguridad. El Sr. Franco describió algunos casos de phishing (suplantación de identidad) en Argentina que ha resuelto ArCERT, para que los participantes pudieran comprender mejor sus actividades. Por ejemplo, a partir de la información recopilada de un sitio de phishing, el CSIRT puede saber cuántos PSI y usuarios han accedido al sitio.

Sesión 5: Vigilancia, alerta y respuesta en caso de incidente

32. Las deliberaciones en torno a la vigilancia, alerta y respuesta en caso de incidente prosiguieron en la 5ª sesión con la presentación del Sr. D. Marcelo HP Caetano Chaves, de CERT-br, Brasil sobre "Utilización de señuelos (honeypots) para supervisar las tendencias del correo basura y de los ataques"[27], en la que informó sobre la investigación y los proyectos de CERT-br. Como ejemplo, mostró lo que su equipo había hecho para comprobar si en Brasil se generaba en realidad se generaba tanta cantidad de correo basura como lo afirman los medios o si tan solo se estaba utilizando Brasil como plataforma de lanzamiento de los ataques. El Sr. Chaves presentó algunos detalles del Proyecto de señuelos distribuidos de la Brazilian Honeypots Alliance[28] cuyos objetivos son: mejorar la capacidad de detección de incidentes y realizar correlaciones de eventos y análisis de tendencias en la red de Internet de Brasil. También expuso algunos detalles del proyecto brasileño SpamPots que utiliza señuelos (honeypots) para medir la utilización malintencionada de máquinas de usuarios finales para enviar correo basura. Entre las actividades previstas de CERT-BR están el análisis de correo basura mediante técnicas de minería de datos, la determinación de patrones en el lenguaje, en URL integradas, etc. y un proyecto para plantear las prácticas óptimas para los PSI. Entre ellas la administración del puerto 25 y la supervisión de la utilización indebida de proxys (servidores intermediarios). El Sr. Chaves manifestó que CERT-br atribuye gran importancia a la cooperación internacional.

33. El Sr. Fred Clark, de la Superintendencia de Telecomunicaciones de Guatemala, hizo una exposición sobre el CSIRT-gt, el CSIRT de Guatemala: "CSIRT-gt: El Equipo de Respuesta a Incidentes de Seguridad Informática de Guatemala"[29]. Guatemala se encuentra en el proceso de establecer un CSIRT nacional y el Sr. Clark desconfió sobre los motivos por los que Guatemala necesita también contar urgentemente con un CSIRT. El papel del CSIRT consiste en entrenar y preparar a los guatemaltecos para proteger el patrimonio de su país. Los desafíos a los que se enfrenta hoy el CSIRT-gt incluyen establecer una disponibilidad 24/7 y lograr de que el equipo esté debidamente entrenado y equipado para ayudar a garantizar la seguridad de las redes nacionales.

34. El Sr. Clark mencionó que la iniciativa de crear el CSIRT-gt surgió de una recomendación del CICTE. En el CSIRT trabajan actualmente cuatro personas y el equipo está buscando otros mecanismos para financiar sus operaciones. En última instancia, el CSIRT podría llegar a ser autosuficiente, pero se necesitan propuestas creativas para encontrar mecanismos que permitan al CSIRT generar ingresos a partir de las actividades y servicios prestados. Es interesante señalar que las personas que actualmente administran el CSIRT se formaron principalmente en el CERT-br de Brasil, lo que demuestra la importancia de la cooperación internacional en todos los campos relacionados con la ciberseguridad.

35. El Sr.Suresh Ramasubramanian, de Outblaze, India, informó sobre el "Proyecto de herramienta de la UIT para reducir los efectos de los Botnet". En su presentación, el Sr. Ramasubramanian explicó las posibilidades de los botnet (programas autónomos), además del envío de correo basura ya mencionado en otras presentaciones. Entre los ejemplos se encuentran el ataque a la infraestructura de internet del país, extorsiónes tales como la amenazas de lanzar ataques de denegación de servicio para inutilizar las páginas web de comercio electrónico; suplantación de identidad y espionaje industrial, robo de información de tarjetas de crédito, contraseñas, etc. almacenada en ordenadores personales (PC) infectados; y/o fraudes de compraventa de acciones. Habló sobre la economía sumergida que han propiciado los *botnet* y que reporta pingües beneficios a los creadores de los virus informáticos, los controladores de los botnet y los delincuentes que llevan a cabo esta actividad ilegal alquilando los *botnet*. Señaló que la amenaza que suponen los botnet aumenta rápidamente. La generación más reciente de *botnet* (como el gusano Zhelatin/Storm) utiliza técnicas particularmente agresivas como las redes de rápida fluctuación (fast-flux) y los ataques de DDoS contra los fabricantes de soluciones de de seguridad que intentan reducir sus efectos.

36. Como respuesta a ello, la UIT está ejecutando un proyecto para crear una *herramienta para reducir los efectos de los Botnet*[30] con el que se pretende hacer frente al problema cada vez mayor de los botnet. La herramienta para reducir los efectos de los Botnet es una estrategia polivalente de múltiples partes interesadas para rastrear los botnet y reducir sus efectos, que hace especial hincapié en los problemas particulares de las economías emergentes de Internet. La herramienta aprovecha los recursos existentes, identifica las partes interesadas, pertinentes, locales e internacionales y tiene en cuenta las limitaciones concretas de las economías en desarrollo. Esta herramienta pretende sensibilizar a los Estados Miembros sobre las amenazas cada vez de los botnet y su relación con las actividades delictivas e incorpora los aspectos técnicos, sociales y de políticas relacionados con la reducción de los efectos de los *botnet*. La primera versión de la herramienta estará

[27] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/chaves-certbr-buenos-aires-oct-07.pdf
[28] http://www.honeypots-alliance.org.br/
[29] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/clark-CSIRT-guatemala-buenos-aires-oct-07.pdf
[30] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

disponible en diciembre de 2007 y está previsto realizar pruebas piloto en varios Estados Miembros de la UIT en 2008.

Sesión 6: Fomento de una cultura de ciberseguridad y la función de los CSIRT

37. Al considerar que los ordenadores personales y los teléfonos móviles utilizan tecnologías cada vez más poderosas y convergentes, que la utilización de las TIC está cada vez más y más difundida y que son cada vez más las conexiones transfronterizas, se hace evidente que todos los participantes que crean redes de información, las posean, las gestionen, las atiendan y las mantienen deben conocer los temas relacionados con la ciberseguridad y adoptar las medidas oportunas que corresponda a su función protectora. En esta sesión se exploró el concepto de fomento de una cultura de ciberseguridad y se examinaron detenidamente las funciones de las diversas partes interesadas, en particular la función que deben cumplir los CSIRT para convertir esta cultura en una realidad.

38. La Sra.Christine Sund, de la División de Aplicaciones de las TIC y ciberseguridad, Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D), ofreció, en su presentación sobre "fomento de una cultura de la ciberseguridad"[31], una visión general del significado de una cultura de la ciberseguridad y de las posibles funciones que las diversas partes interesadas de la sociedad de la información para crear dicha cultura a nivel mundial. La Sra. Sund hizo hincapié en los nueve elementos de la creación de una cultura de la ciberseguridad mencionados en la Resolución 57/239 (2002) de las Naciones Unidas, "Creación de una cultura mundial de seguridad cibernética" y en la Resolución 58/199 (2004) de las Naciones Unidas, "Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales". Estos elementos son: conciencia, responsabilidad, respuesta, ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación. A los Estados Miembros y a todas las organizaciones internacionales pertinentes se les había solicitado que consideraran estos elementos y los tuvieran en cuenta durante las preparaciones de las dos fases de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[32] que se celebraron en 2003 y en 2005. En los documentos que resultaron de las dos fases de la CMSI se recalca aún más la importancia de crear confianza y seguridad en la utilización de las TIC y se pone de manifiesto el compromiso de los países de fomentar la cultura de la ciberseguridad.

39. En la presentación de la Sra. Sund se mencionaron varias funciones que podrían desempeñar los gobiernos en el fomento de una cultura de la ciberseguridad, a saber: garantizar la protección de los habitantes del país, desempeñar un papel central en la coordinación y puesta en marcha de una estrategia nacional de ciberseguridad, asegurarse de que las políticas nacionales, sean flexibles y adaptables, coordinar las responsabilidades asignadas a las autoridades y órgano de la Administración, crear nuevas leyes (o adaptar las existentes) para penalizar el uso indebido de las TIC, poner freno a los abusos y proteger los derechos del consumidor y liderar las actividades nacionales, regionales e internacionales en materia de ciberseguridad. La Sra. Sund recalcó que las infraestructuras de las TIC pertenecen en gran parte al sector privado y son explotadas por éste, por lo que la participación de este sector en el fomento de una cultura mundial de la ciberseguridad es de primordial importancia. Para que la ciberseguridad sea eficaz es necesario comprender a fondo todos los aspectos de las redes de las TIC, y por ende es vital contar con la experiencia y la participación del sector privado para poder formular y poner en práctica las estrategias de ciberseguridad. Además, la Sra. Sund destacó que los gobiernos y las empresas necesitan ayudar a los ciudadanos a informarse de cómo protegerse cuando están conectados. Disponiendo de las herramientas adecuadas, cada participante en la sociedad de la información tiene la responsabilidad de estar alerta y de protegerse, sin olvidar, por otra parte, que la ciberseguridad es fundamentalmente una responsabilidad compartida.

40. Dos participantes, el Sr. Bradford Willke, del CERT/CC Software Engineering Institute (SEI), Estados Unidos de América y la Sra. Patricia Prandini, del ArCERT, Argentina, expusieron a continuación algunas reflexiones respecto al tema. En su presentación sobre "Contribuciones del CSIRT a los esfuerzos nacionales para proteger la infraestructura básica de la información"[33], el Sr. Willke examinó algunas prácticas idóneas aplicables a marcos de la PIBI relacionados con los CSIRT, algunas actividades comunes de los CSIRT en la PIBI, las ventajas de planificar o dar alcance a las actividades de los CSIRT en la PIBI y la coordinación multinacional de eventos en el marco de la PIBI. El Sr. Willke mencionó algunas de las actividades de los CSIRT que él considera están relacionadas con la protección de la infraestructura básica de la información nacional. Entre estas responsabilidades están crear y mantener el conocimiento del entorno de la ciberseguridad, es decir, las amenazas, vulnerabilidades, riesgos, capacidades e intereses existentes, crear indicadores para cuantificar estas amenazas, hacer un seguimiento de la evolución de la situación de la ciberseguridad, ayudar a los proveedores de infraestructuras básicas de la información y a los organismos oficiales de reglamentación a identificar y hacer frente a las vulnerabilidades y amenazas de la seguridad de la información, divulgar los "errores cometidos" a partir del análisis del entorno cibernético y de la información obtenida de los diversos sectores para así ampliar y mejorar el nivel general de ciberseguridad de la nación y coordinarse con las autoridades, los reguladores, los expertos en la materia, etc. sobre soluciones e implicaciones técnicas. El Sr. Willke también resaltó que la intervención de los CSIRT o la efectuada a través de ellos contribuiría al cumplimiento de las metas

[31] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/sund-promoting-a-culture-of-cybersecurity-buenos-aires-oct-07.pdf
[32] http://www.itu.int/wsis/
[33] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/willke-role-of-csirts-buenos-aires-oct-07.pdf

internacionales en materia de ciberseguridad. Entre las actividades que podrían abarcar también los CSIRT se encuentran: la identificación de los expertos y recursos necesarios; la coordinación de las comunidades de fabricantes y proveedores de servicios sobre soluciones y medidas correctivas técnicas y de procedimiento; coordinar programas, planes nacionales de respuesta ante situaciones de emergencia, etc. dentro de marcos de gestión (como los programas para la protección de infraestructuras esenciales (CIP)), planes de respuesta ante emergencias, etc.; Asesorar al gobierno y a la industria sobre lo que se debe o no se debe hacer y tal vez participar con los asociados en los procesos de planificación, diseño, puesta en marcha, explotación y reconstitución.

41. La Sra. Patricia Prandini, de ArCERT[34], Argentina abordó la función concreta de los CSIRT en su presentación, "RoI de los CSIRTs"[35]. Expuso inicialmente las tareas que deberían realizar los CSIRT, entre las que mencionó: producir material técnico e iniciar programas de formación sobre el uso responsable de las TIC, contribuir a la formulación de normas y prácticas óptimas en seguridad informática, prestar servicios especiales como la posibilidad de identificar grupos prioritarios y temáticas de interés y fomentar la toma de conciencia de los grupos que prestan los servicios necesarios. Mencionó, además, que los CSIRT contribuyen a mejorar las operaciones cotidianas y a minimizar el número de incidentes cibernéticos. La Sra. Prandini también habló sobre algunas iniciativas de toma de sensibilización en materia de ciberseguridad que se están ejecutando en la región, como COLARIS (Conferencia Latino Americana de Respuesta a Incidentes de Seguridad) que organiza cursos de formación en TRANSITS, talleres sobre seguridad y reuniones de FIRST-TC., Mencionó asimismo que el CICTE (Comité Interamericano contra el Terrorismo) y la OEA han propuesto iniciativas que incorporan la seguridad de las TI en el orden del día de las reuniones y eventos regionales, y para la coordinación de algunas actividades regionales de los CSIRT. Por ejemplo, LACNIC ha impartido formación para el fortalecimiento de las capacidades de los funcionarios del CSIRT, además de otras actividades de coordinación. La Sra. Prandini también informó de algunas de las iniciativas argentinas desensibilización en marcha y de otras proyectadas para el futuro.

Sesión 7: Fundamento jurídico, desarrollo reglamentario y aplicación

42. La legislación adecuada, la coordinación jurídica internacional y su aplicación son elementos importantes para prevenir, detectar y dar respuesta a la ciberdelincuencia y el uso indebido de las TIC. Ello requiere actualizar el derecho penal, los procedimientos jurídicos y las políticas para que contemplen los incidentes de ciberseguridad y den respuesta a la ciberdelincuencia. Por ello, muchos países han modificado o están enmendando sus códigos penales con arreglo a los convenios y recomendaciones internacionales. En las sesiones 7 y 8 del Taller se examinaron estrategias jurídicas de diversos países y posibles campos en las que podrían existir una coordinación jurídica internacional y realizar trabajo de aplicación. El moderador de la sesión 7, el Sr. Marco Gercke, de Alemania, inauguró la sesión exponiendo lo que se está haciendo en la Unión Europea para revisar las leyes existentes y elaborar nuevas leyes que tengan en cuenta la utilización cada vez mayor de las tecnologías de la información y la comunicación por parte de los ciudadanos.

43. La primera presentación correspondió al Sr. Albert Rees, de la Computer Crime and Intellectual Property Section (CCIPS), Ministerio de Justicia, Estados Unidos de América. El Sr. Rees comenzó su presentación sobre "Bases jurídicas"[36] preguntándose cómo podían conseguir los países investigar, procesar y condenar a las personas que utilizan los computadores e Internet con fines delictivos. Señaló que, aún siendo diferentes, las metas de las diversas partes interesadas en ciberseguridad seguía siendo importante trabajar mancomunadamente para combatir la ciberdelincuencia, ya que esta repercute y afecta a todas las personas y a todos los países. Independientemente de su nivel de desarrollo, todos los países se ven afectados de una forma u otra. Un componente crucial de toda acción nacional de respuesta es la comunicación y cooperación, bien sea al interior del gobierno, con el sector privado o a nivel internacional. El Sr. Rees citó tres acciones principales que pueden realizar los países para combatir la ciberdelincuencia: 1. garantizar que existan y estén vigentes leyes apropiadas en materia de ciberdelincuencia y temas afines, 2. establecer y formar órganos competentes especializados en la aplicación de la ley que conozcan la tecnología y las leyes del país y la forma en que éstas se concilian y 3. establecer vínculos con otros países para compartir información.

44. El Sr. Rees puso de manifiesto la necesidad de que en cada país se adapte el marco jurídico establecido contra la ciberdelincuencia para que cumpla los objetivos nacionales, de forma que las leyes y reglamentos se ajusten a las necesidades particulares del país. No obstante, las leyes nacionales en materia de ciberdelincuencia deben, al mismo tiempo, facilitar la cooperación y deben por ende ser en lo posible compatibles con las de otros países, debido al carácter internacional de Internet, ajeno a las fronteras nacionales. El convenio sobre el delito cibernético del Consejo de Europa propone un marco para el tipo de leyes que son necesarias. Por ejemplo, como el sistema jurídico de Estados Unidos es diferente al de Bolivia, el Convenio proporciona un marco que todos los países pueden utilizar para desarrollar su legislación en esta materia. También se cuenta con recursos de diversas fuentes que pueden ayudar a los países a formular leyes en esta esfera. En la región de las Américas, la OEA y la REMJA han ratificado el Convenio sobre el delito cibernético. Inicialmente, el grupo REMJA indicó que era preferible pensar en un marco regional, pero hoy en día el grupo estudia detenidamente la forma de utilizar el convenio y posiblemente se adhiera al mismo. En la región, tanto México como Costa Rica muestran interés por comprender mejor los beneficios del Convenio. El Sr.

[34] http://www.arcert.gov.ar
[35] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/prandini-rol-de-los-CSIRTs-buenos-aires-oct-07.pdf
[36] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rees-legal-foundation-buenos-aires-oct-07.pdf

Rees finalizó su presentación instando a los países a que soliciten asistencia y apoyo para la revisión de la legislación vigente y la formulación de nuevas leyes. Recalcó que el Consejo de Europa cuenta con un programa muy eficaz para revisar la legislación y que el Ministerio de Justicia de Estados Unidos también tiene un programa para el mismo fin.

45. El Sr. Gilberto Martins de Almeida, Brazil, expuso la "estrategia jurídica de Brasil en materia de ciberdelincuencia"[37] así como la situación de los diversos países de la región de las Américas en lo que respecta la actualización de sus códigos. En cuanto a la estrategia de Brasil para combatir la ciberdelincuencia, el Sr. Martins de Almeida indicó que pueden suscitarse incompatibilidades en las políticas nacionales de los países. Un problema vigente en Brasil es que el código penal y el código civil cuentan con 30 artículos. Debido a esto, para Brasil no sería muy práctico establecer una legislación sobre ciberdelincuencia, pues no es muy factible realizar comparaciones directas. El Sr. Martins de Almeida dijo que el país "no debería esforzarse demasiado en probar que se requiere una ley, pero al mismo tiempo es necesario demostrar que es necesaria una ley." El Sr. Martins de Almeida analizó el Convenio sobre el delito cibernético del Consejo de Europa y lo que éste significa para Brasil. Señaló que en términos generales el convenio proporciona unas bases legales jurídicas de forma y de fondo, define las facultades para realizar investigaciones y los límites/salvaguardas pertinentes, ofrece orientación para las relaciones con los proveedores de servicios y orientaciones para la formulación de la legislación nacional, así como bases para la cooperación internacional. Señaló que, en conjunto, el Convenio sobre el delito cibernético había cambiado la forma de pensar de la comunidad brasileña que participa en los asuntos legislativos. Una causa de esto es que el Convenio deja que la legislación nacional establezca el equilibrio entre la seguridad y la privacidad. Señaló que el convenio se puede utilizar como orientación para la formulación de la legislación nacional sobre ciberdelincuencia puesto que presenta un enfoque coherente en lo que respecta la legislación nacional, la armonización y compatibilidad de las disposiciones penales sobre ciberdelincuencia con las de otros países y procedimientos para investigaciones más eficaces. Adicionalmente, el convenio proporciona un cierto número de herramientas para recopilar pruebas electrónicas, entre ellas herramientas para investigar el ciberblanqueo de capitales, el ciberterrorismo y otros delitos graves. Estas herramientas también pueden utilizarse en el contexto de la cooperación internacional.

46. El Sr. D. Fernando Maresca, de la Oficina nacional de tecnologías de información (ONTI), Argentina, expuso su opinión sobre los aspectos legales relacionados con la ciberdelincuencia en su presentación "Aspectos Legales del Cibercrimen"[38] en la que incluyó ejemplos sobre las acciones emprendidas en Argentina para revisar los marcos jurídicos. El Sr. Maresca inició su presentación señalando que uno de los desafíos a los que se enfrentan quienes combaten la ciberdelincuencia se relaciona con la dosolescencia de las descripciones de los tipos de delito que deberían clasificarse como "delitos cibernéticos", al tiempo que las descripciones y definiciones existentes no son suficientes para atajar las actividades que surgen a raíz de la utilización de nuevos métodos delictivos. Señaló además que la ciberdelincuencia se puede analizar desde perspectivas diferentes. Mientras que algunos aseveran que la ciberdelincuencia debería considerarse como un nuevo tipo de delito, otros afirman que la ciberdelincuencia no existe sino que es una extensión de los delitos actuales. Dijo que si ese era el caso, no estaríamos tratando con un nuevo tipo de delito sino con una cuestión semántica.

47. El Sr. Maresca señaló que en el congreso Argentino está debatiendo un proyecto de ley sobre ciberdelincuencia y que era muy posible que se éste aprobara como Ley específica contra la ciberdelincuencia. Señaló que únicamente once países de la región cuentan con algún tipo de legislación contra la ciberdelincuencia. También señaló que las penas por delitos informáticos son muy diferentes en los distintos países que poseen una legislación contra la delincuencia electrónica. Afirmó que es urgente establecer normas para tipificar y penalizar las conductas delictivas, y lograr una armonización de la legislación de todos los países de la regió.

Sesión 8: Base jurídica, desarrollo de la reglamentación y cumplimiento

48. En la 8ª sesión, prosiguieron los debates acerca del establecimiento de las bases jurídicas, el desarrollo de la reglamentación y el cumplimiento.

49. La Sra. Jody Westby, de Global Cyber Risk LLC (Estados Unidos de América), presentó una ponencia sobre las "Cuestiones internacionales en la lucha contra la ciberdelincuencia: una llamamiento a la armonización".[39] La Sra. Westby comenzó comparando la ciberseguridad con un taburete de tres patas; afirmó que la ciberdelincuencia, la privacidad y la ciberseguridad son asuntos de alcance mundial. Además, la ciberdelincuencia, la privacidad y la protección de la infraestructura de la información son muy importantes para preservar los intereses nacionales y económicos, así como para la seguridad pública. Mientras que los países industrializados ponen el mayor empeño en tratar de resolver estos asuntos, los países en desarrollo del mundo están quedando rezagados. Prosiguió su presentación observando que el sistema jurídico mundial muestra muchas discrepancias y que las principales diferencias radican en la legislación en materia de ciberdelincuencia. Ello se debe, en parte, a que los países y organizaciones se han esforzado por reducir la "brecha digital", pero han creado una "brecha jurídica". Por otra parte, planteó la pregunta de por qué la legislación sobre ciberdelincuencia es un asunto también importante para los países en desarrollo. A este respecto, subrayó que la

[37] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/almeida-brazil-legal-approach-buenos-aires-oct-07.pdf
[38] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/maresca-cibercrime-buenos-aires-oct-07.pdf
[39] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/westby-model-law-project-buenos-aires-oct-07.pdf

promulgación de leyes y legislación en materia de ciberdelincuencia contribuirá a garantizar que no exista ningún país en el que puedan refugiarse los ciberdelincuentes y que al final no exista amparo para los delincuentes en ningún rincón del planeta. La Sra. también destacó los principales aspectos que es necesario armonizar, en particular, las definiciones y el alcance, las cláusulas jurisdiccionales, las disposiciones sustantivas, las cláusulas de procedimiento y el ámbito de cooperación internacional.

50. Para ayudar a los países a crear un legislación modelo en materia de cibertelito, la Sra. Westby mencionó la iniciativa en curso de la UIT, "herramienta de la UIT para una legislación modelo en materia de ciberdelincuencia".[40] Esta herramienta constituyen uno de los cinco elementos identificados en el *Marco para la organización de un enfoque nacional de la ciberseguridad* elaborado por la Comisión de Estudio del UIT-D encargada de la Cuestión 22/1. Una parte integrante de la estrategia de ciberseguridad/PIBI es disuadir la ciberdelincuencia, en particular, mediante la adopción de la legislación adecuada contra la utilización indebida de las TIC con fines delictivos y otros fines y actividades que comprometan la integridad de la infraestructura básica nacional. Dado que las amenazas pueden provenir de cualquier lugar del planeta, la problemática tiene una dimensión intrínsecamente internacional, razón por la cual conviene armonizar lo más posible la legislación para facilitar la cooperación a escala regional e internacional. La herramienta mencionada está destinada a proporcionar a los países una legislación modelo que les ayude a establecer un marco legislativo que desaliente la ciberdelincuencia. Un grupo de expertos internacionales y multidisciplinarios, del que forma parte la Sra. Westby, se está encargando de desarrollar esta herramienta y el proyecto preliminar estará disponible el primer trimestre de 2008.

51. El Sr. Marco Gercke (Alemania) presentó una ponencia titulada "El desafío de combatir la ciberdelincuencia en los países en desarrollo y el papel que desempeña la legislación nacional, regional e internacional en materia de ciberdelincuencia"[41], en la que subrayó algunas de las dificultades que han de arrostrar los países en desarrollo al combatir la ciberdelincuencia y facilitó información detallada acerca de la próxima publicación de la UIT en 2007 sobre este particular.[42] También explicó la importancia de la legislación nacional, regional e internacional en materia de ciberdelincuencia para el fomento de una cultura mundial de la ciberseguridad. El Sr. Gercke dijo que uno de los desafíos más importantes para los países en desarrollo es encontrar soluciones adecuadas para responder a la amenaza que representa la ciberdelincuencia. La creación y aplicación de una estrategia nacional sobre ciberseguridad, que incluya la lucha contra la ciberdelincuencia, requiere tiempo y puede tener un coste elevado, factores éstos que pueden impedir a los países la adopción de las medidas necesarias para reforzar la seguridad. El Sr. Gercke insistió también en que es importante destacar los peligros que entraña una escasa protección, por cuanto pueden afectar gravemente al entorno social y empresarial. Por consiguiente, los países en desarrollo corren el riesgo de atraer la actividad ciberdelictiva, lo que tendría consecuencias adversas para el mercado nacional. Añadió que, como parten desde cero, los países en desarrollo tienen una oportunidad sin precedentes de armonizar sus estrategias en materia de ciberdelincuencia desde el principio y de manera normalizada.

52. Por otra parte, el Sr. Gercke subrayó que Internet es un lugar idóneo para ocultar información sobre asuntos "confidenciales". El inconveniente de los mecanismos que ofrece Internet es que muchos delincuentes saben utilizar muy bien estas técnicas. Los participantes en el taller apreciaron sobremanera las demostraciones en vivo que hizo el Sr. Gercke durante su ponencia, ya que les ayudaron a comprender mejor ciertas técnicas, por ejemplo, la ocultación de conversaciones en imágenes y mensajes de correo electrónico.

Sesión 9: Cooperación regional e internacional

53. La cooperación regional e internacional es sumamente importante para promover una cultura de la seguridad, al igual que la función que desempeñan los foros regionales de facilitar la interacción y el intercambio de información. En esta sesión se examinaron algunas de las actuales iniciativas de cooperación regionales e internacionales con el fin de alentar a los asistentes a la reunión a que participen en otras actividades concretas que podrían llevarse a cabo en la región de las Américas y a nivel internacional.

54. El Sr. Albert Rees, del Departamento de Justicia de Estados Unidos de América, y en representación de las REMJA (Reuniones de Ministros de Justicia o Ministros o Procuradores Generales de las Américas) de la OEA (Organización de los Estados Americanos) y de su Grupo de Expertos Gubernamentales en ciberdelincuencia, abrió los debates de esta sesión con una ponencia sobre "cooperación internacional".[43] Indicó que las REMJA prestan asistencia a los Estados Miembros de la OEA mediante, entre otras cosas, la organización de talleres regionales, la preparación de políticas y legislación, las investigaciones e informes forenses sobre informática y la cooperación internacional. El Sr. Rees también se refirió a la Red 24/7 contra la delincuencia de alta tecnología, originalmente una iniciativa del G8, que consiste en una red de contactos de emergencia para asuntos de delitos en línea. La red está constituida por personal de las fuerzas de seguridad que comparten

[40] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

[41] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/gercke-cybercrime-guide-buenos-aires-oct-07.pdf

[42] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html

[43] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/rees-international-cooperation-buenos-aires-oct-07.pdf

información y prestan asesoramiento acerca de la preservación de datos, la información de contacto con los PSI y sobre cómo iniciar un proceso de asistencia jurídica mutua.

55. Actualmente, la Red 24/7 contra la delincuencia de alta tecnologías dispone de puntos de contacto en 50 países y, en la región de las Américas, cuenta con la participación de Brasil, Canadá, Chile, la República Dominicana, Jamaica, Perú y Estados Unidos. El Sr. Rees dijo que la participación en la red está abierta a todos los países que lo deseen y que es fácil afiliarse a la misma. El único requisito es que el país designe una persona de contacto, que atienda un teléfono y tenga los conocimientos técnicos suficientes para ocuparse de los ciberdelincuencias, dado que uno de los principales problemas relacionados con la ciberdelincuencia es conseguir pruebas forenses digitales. Es igualmente necesario que dicha persona conozca los procedimientos y la legislación nacionales. Por consiguiente, no hay obstáculos especiales para participar en la mencionada red. El Sr. Rees añadió que los países interesados en obtener mayor información sobre el particular pueden dirigirse a la Sección de Propiedad Intelectual y Delincuencia Informática del Departamento de Justicia de los Estados Unidos (CCIPS)[44].

56. El Sr. Romulo Dantas, representante del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), hizo una ponencia titulada "Programa de la OEA de Protección de Infraestructuras Críticas" [45], en la que presentó este programa de la OEA. Indicó que, a raíz del aumento del número de incidentes de seguridad, la OEA está intensificando sus actividades en el campo de la protección de infraestructura. Señaló asimismo que durante el pasado año muchos Estados Miembros de la OEA registraron un progreso considerable en el cumplimiento de los compromisos contraídos con arreglo a la Estrategia Interamericana Integral para combatir las amenazas a la seguridad cibernética.[46] Cabe señalar que todos los países de la OEA firmaron esta estrategia y designaron puntos de contacto nacionales, que pueden consultarse en el sitio web del CICTE. A través de estos puntos de contacto nacionales, los expertos que participan en el programa tienen acceso directo al personal de los gobiernos nacionales que son conscientes de las posibles repercusiones de las amenazas a la ciberseguridad.

57. En la estrategia mencionada se reconoce la necesidad de crear una red interamericana de supervisión, alerta y respuesta, que permita la pronta diseminación de información relativa a la ciberseguridad y la prestación de asistencia a los países para responder y recuperarse de las crisis, incidentes y amenazas en el ámbito de la seguridad informática. Así pues, uno de los compromisos de la estrategia regional es la creación de equipos de respuesta ante incidentes informáticos (CSIRT) en los Estados Miembros de la OEA para reaccionar a incidentes de ciberseguridad. En esta estrategia, que integra las actividades y conocimientos especializados del CICTE, la CITEL y las REMJA, se reconoce la necesidad de que todos los participantes en la redes y los sistemas de información sean conscientes de su función y responsabilidades en lo relativo a la seguridad, con miras a promover una cultura de la ciberseguridad. El Sr. Dantas observó que el CICTE concentra sus actividades en ayudar a los países a aumentar sus capacidades mediante el desarrollo y la formación de personal de los CSIRT en la región. En el marco de una importante estrategia, el CICTE se ha comprometido también a planificar la creación de una red que abarque todo el hemisferio y funcione 24 horas al día los siete días de la semana, y en la que los CSIRT desempeñarán la importante función de distribuir rápidamente información relativa a la seguridad y prestar asesoramiento técnico y asistencia en caso de que se produzca un ciberincidente. Uno de los objetivos es que los puntos de contacto nacionales se transformen en CSIRT plenamente capacitados.

58. El Sr. prosiguió explicando el grado de preparación general de los Estados Miembros de la OEA, considerando los países que han integrado la ciberdelincuencia en su legislación y cuánto han progresado en la aplicación de los aspectos específicos de la Estrategia Interamericana Integral para combatir las amenazas a la seguridad cibernética.

59. El Sr. Wayne Zeuch, de Alcatel-Lucent, en nombre de la Comisión Interamericana de Telecomunicaciones (CITEL) de la Organización de los Estados Americanos, presentó la ponencia titulada "Objetivos de la CITEL en materia de ciberseguridad y protección de la infraestructura básica".[47] El Sr. Zeuch comenzó su ponencia observando que en el mandato de la OEA sobre ciberseguridad y protección de la infraestructura básica, el CICTE, la CITEL y la REMJA son los pilares sobre los que se asienta la Estrategia Interamericana Integral en materia de ciberseguridad, y que las actividades multidisciplinarias de estos organismos tienen por objeto contribuir al crecimiento, el desarrollo y la protección de Internet y los sistemas de la información conexos, así como proteger a los usuarios de esas redes de la información. En la CITEL, las actividades relativas a la ciberseguridad y la infraestructura básica están a cargo del Comité Consultivo Permanente I (CCP.I) de dicha organización. El Sr. Zeuch explicó que el mandato del grupo incluye el estudio de los aspectos de la seguridad relacionados con el desarrollo de redes de comunicaciones (en particular, la función de apoyo a la infraestructura básica, la función del sector privado en la protección de las redes de comunicaciones, y los enfoques nacionales y regionales necesarios en la región de las Américas). También forma parte de dicho mandato la evaluación de la labor en curso en la OEA, la UIT y otros foros sobre cuestiones relativas a la seguridad y la protección de la

[44] http://www.cybercrime.gov
[45] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/dantas-cicte-buenos-aires-oct-07.pdf
[46] http://www.cicte.oas.org/Rev/En/Documents/OAS_GA/AG-RES.%202004%20(XXXIV-O-04)_EN.pdf
[47] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/zeuch-citel-buenos-aires-oct-07.pdf

infraestructura básica, además de la creación de enfoques nacionales y regionales en materia de seguridad de las redes, estrategias de despliegue, intercambio de información y concienciación de los sectores público y privado. El CCP.I también examina los marcos y las directrices relativas a las redes y la ciberseguridad y su posible aplicación a las Américas, y trata de fomentar el diálogo en lo que respecta a los trabajos de la Comisión de Estudio 17 del UIT-T y otros foros pertinentes.

60. El Sr. Zeuch hizo referencia al denominado "cuaderno técnico de la ciberseguridad" del CCP.I, que reúne los resultados de los talleres y las estrategias de ciberseguridad y PIBI adoptadas por los Estados Miembros, e incluye apéndices con experiencias nacionales específicas. Añadió que se está preparando un "cuaderno técnico de la protección de la infraestructura básica", complementario del relativo a la ciberseguridad, y cuya finalidad es facilitar información sobre la protección de la infraestructura básica a las empresas del sector de telecomunicaciones y a los Estados Miembros, documentar las estrategias nacionales de PIBI adoptadas por los Estados Miembros e indicar las recomendaciones pertinentes de la UIT y otro foros, a fin de que los Estados Miembros puedan abordar mejor los problemas técnicos de la PIBI a medida que vayan surgiendo. En la última reunión de la CCP.I celebrada a finales de 2007, se propuso la preparación de un "cuaterno técnico sobre el fraude en la prestación de servicios de telecomunicaciones". El Sr. Zeuch terminó su ponencia explicando la función que desempeña la CITEL en la coordinación de normas, tanto las relativas a la seguridad como las normas más generales en el campo de la telecomunicaciones. Ahora bien, en lo que respecta a las normas de seguridad, la CITEL utiliza documentos normativos coordinados para dar a conocer las normas de seguridad pertinentes y promover la utilización de otras normas pertinentes en la región.

Mesa redonda para el intercambio de información

61. Al final de cada uno de los dos primeros días del taller, los participantes se reunieron en mesas redondas, constituidas por grupos más pequeños y dirigidas por un moderador, para discutir asuntos concretos del programa del día. El moderador veló por que todos los participantes tuvieran la oportunidad de compartir las experiencias específicas de sus países y formuló preguntas de los expertos que participaban en los debates de cada mesa. Durante los tres días del evento, los grupos más pequeños mantuvieron debates acerca de cinco temas distintos:

- Elaboración de una estrategia nacional, moderado por el Sr. Joseph Richardson;
- Normas técnicas de seguridad, moderado por el Sr. Mike Harrop, Comisión de Estudio 17 del UIT-T, Relator para el proyecto de seguridad;
- Supervisión, alerta y respuesta a incidentes, moderado por el Sr. Jason Rafail, CERT/CC SEI, Estados Unidos de América;
- Fomento de una cultura de ciberseguridad y función de los CSIRTS, moderado por la Sra. Patricia Prandini, ArCERT, Argentina;
- Base jurídica, desarrollo de la reglamentación y cumplimiento (1), moderado por el Sr. Albert Rees, Departamento de Justicia de Estados Unidos de América;
- Base jurídica, elaboración de la reglamentación y cumplimiento (2), moderado por la Sra. Jody Westby, GlobalCyber Risk LLC, Estados Unidos de América.

62. Antes de dar por terminado el taller por la tarde, cada grupo informaba a los participantes en la reunión y facilitaba un resumen sucinto sobre los temas tratados y los principales problemas identificados. Las conclusiones y el consenso resultantes de dichos debates se resumieron ulteriormente en la 10ª sesión de la reunión. A continuación figura información detallada sobre el particular.

Sesión 10: Conclusiones, recomendaciones y el camino a seguir

63. En la última sesión de la reunión, moderada por el Sr. Robert Shaw, de la División de aplicaciones TIC y ciberseguridad del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D), se resumieron las diferentes sesiones celebradas durante el taller y se plantearon preguntas acerca de cuáles son las estrategias futuras, las soluciones, las asociaciones y las estructuras necesarias para seguir avanzando estos debates relativos a los marcos para la ciberseguridad y la protección de la infraestructura básica de la información. Los representantes de los cinco esferas principales formularon sus principales conclusiones del evento, en particular las relativas a los debates de la sesión en la que hicieron su ponencia, y explicaron sus puntos de vista sobre las posibles medidas constructivas que podrían adoptarse.

64. Sesiones 1 y 2, marcos para la ciberseguridad y la protección de la infraeSesiones 1 y 2, marcos para la ciberseguridad y la protección de la infraestructura básica de la información (PIBI): Sr. Daniel Hurley, Departamento de Comercio de la Administración Nacional de Telecomunicaciones e Información (NTIA) de Estados Unidos de América. El Sr. Hurley destacó la importancia de la colaboración entre gobierno e industria y observó que resultaría más sencillo si todas las partes trataran de cooperar tal y como describió el orador de Microsoft. Además, señaló a la atención de los participantes en el taller la herramienta de la UIT para la autoevaluación nacional de la ciberseguridad/PIBI, que puede resultar útil a los países en desarrollo para establecer un nivel de referencia de la seguridad y ayudarles a determinar el nivel de seguridad actual y a establecer prioridades en función de sus necesidades específicas. En lo que respecta a las propuestas para el

futuro, el Sr. Hurley insistió en la necesidad de pasar de las actividades de sensibilización a la creación de capacidades sobre temas específicos para aumentar así la ciberseguridad.

65. Sesión 3, Normas técnicas en materia de ciberseguridad: Sr. Mike Harrop, Comisión de Estudio 17 del UIT-T, relator sobre el proyecto de seguridad. El Sr. Harrop observó que es importante lograr sin dilación una mayor participación de los países de América Latina y menos adelantados del mundo en las actividades de normalización de la UIT, para que puedan expresar sus puntos de vista e intereses en lo que concierne a la normalización. Recordó que a lo largo del taller los países preguntaron acerca de qué políticas en materia de ciberseguridad han adoptado otros países y cuán eficaces son, por lo que quizá resulte interesante comenzar a investigar más profundamente la creación de un posible índice de preparación en materia de ciberseguridad/PIBI para ayudar a los países a conocer su grado de preparación a nivel nacional y poder compararse con otros países.

66. Sesiones 4, 5 y 6, Supervisión, alerta y respuesta en caso de incidente y la función de los CSIRT en el fomento de una cultura de ciberseguridad: Sra. Patricia Prandini, ArCERT, Argentina. La Sra. Prandini dijo que se alegraba de haber comprobado durante el taller que ningún país está comenzando desde cero en lo referente a la creación de capacidades para la ciberseguridad y la PIBI, aunque, al mismo tiempo, ninguno está totalmente preparado. Por consiguiente, todos los países tienen trabajo pendiente a este respecto. Dijo que el trabajo en curso es como las cuentas de un collar y señaló con una imagen poética que "tenemos las cuentas pero no sabemos cómo ensartarlas para formar el collar". Puso como ejemplo el caso de Argentina, país en el que existe un CSIRT y que en breve se promulgará una ley contra la ciberdelincuencia, auque aún no cuente con un marco general que integre todos los elementos de una estrategia nacional. Añadió que las herramientas de la UIT mencionada durante el taller, especialmente en la relativa a la preparación nacional en materia de ciberseguridad/PIBI, nos permitiría conocer mejor nuestra situación, en relación con los anteriores logros y respecto a otros países. La Sra. Prandini declaró que aunque queda mucho por hacer, está plenamente convencida de que vamos por el buen camino. En cuanto al futuro, la Sra. Prandini destacó la necesidad de crear un portal web sobre ciberseguridad en el que puedan consultarse todas las reuniones, el material de formación y los programas desde un mismo lugar. Sugirió además que para allanar el camino a la colaboración eficaz, resultaría muy práctico disponer también de un calendario común de eventos. Por último, la Sra. Prandini señaló a la atención de los participantes la posible creación de un CERT regional para América Latina.

67. Sesiones 7 y 8, Base jurídica, desarrollo de la reglamentación y cumplimiento: Sra. Jody Westby, Global CyberRisk LLC, Estados Unidos de América. Los tres puntos más importantes sobre los que insistió la Sra. Westby fueron la necesidad de aumentar la cooperación internacional en materia de legislación y cumplimiento, la necesidad de crear el próximo año una Red 24/7 contra la delincuencia de alta tecnología y la posibilidad de preparar un "recetario de búsqueda e incautación". La Sra. Westby también formuló una petición abierta a CISCO, patrocinador de las pausas para el café/té durante el taller, relativa al establecimiento de centros de telepresencia en la región de las Américas y en otras regiones del mundo, que permitan a los asistentes a talleres y reuniones regionales similares al presente seguir discutiendo estos temas en línea, además de las reuniones presenciales.

68. Sesión 9, Cooperación regional e internacional: Sr. Romulo Dantas, Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos. El Sr. Dantas dijo que al parecer siguen habiendo algunas tensiones fundamentales entre los enfoques nacionales, regionales e internacionales sobre ciberseguridad, pese a que la filosofía de protección es común a todos. Alegó que debería fomentarse y alentarse la cooperación intrarregional, además de la regional, es decir, dentro de una misma región y entre regiones. Por último, insistió en que instaurar la ciberseguridad es una tarea que no puede llevar cabo el gobierno por sí solo, por lo que es muy importante la asociación con la industria y el sector privado, asunto al que debe conferirse la atención necesaria. El Sr. Dantas concluyó sus observaciones señalando que el alcance de las ciberamenazas es muy amplio y que las cosas podrían ser muy distintas con una educación multidisciplinaria.

Clausura de la reunión

69. El Sr. Gonzalo Heredia, Coordinador de programas nacionales sobre la sociedad de la información de la Secretaría de Comunicaciones de Argentina, dirigió las palabras de clausura[48] de este evento de tres días de duración. Dijo que la seguridad ha dejado de ser un problema exclusivo del ámbito de la informática, de una organización en particular, de una industria o de los gobiernos, razón por la cual los países han de garantizar que las amenazas a la ciberseguridad y sus vulnerabilidades se afronten de manera coordinada en todos estos ámbitos. Elogió la reciente iniciativa de la UIT destinada a ayudar a los países a crear estrategias nacionales de ciberseguridad y protección de la infraestructura básica de la información y añadió que Argentina se complace de haber acogido este evento para apoyar tan importante iniciativa. Dió las gracias a los asistentes y oradores por haberse desplazado hasta Buenos Aires y haber sacado tiempo de su apretada agenda para participar en este taller. Para concluir, insistió en que todos y cada uno de nosotros, integrantes de la sociedad de la información, tenemos una función que desempeñar en la creación de una cultura mundial de la ciberseguridad y es nuestra responsabilidad velar por ello. El Sr. Heredia añadió que hay trabajo para todos y mucho por hacer, y espera que este encuentro sea un hito más hacia un mundo mejor.

[48] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/closing-remarks-heredia-buenos-aires-18-oct-07-s.pdf (español)

70. En su discurso de clausura[49] Paolo Rosa, de la División de Talleres y Promoción de la Oficina de normalización de las Telecomunicaciones de la UIT, dió las gracias, en nombre de Sami Al-Basheer Director del UIT-D y Malcolm Johnson Director del UIT-T, al organizador nacional por su extraordinaria labor en este evento regional sobre ciberseguridad, organizado con la colaboración de los Sectores de Normalización y Desarrollo de las Telecomunicaciones de la UIT, que ha resultado ser todo un éxito. Extendió su agradecimiento especial a la Secretaría de Comunicaciones de Argentina y la Comisión Nacional de Comunicaciones (CNC) de este país, por su magnífica acogida del evento y su cooperación en la planificación y organización del mismo; a todos los oradores por haber sacado tiempo de su apretada agenda para compartir sus experiencias y conocimientos especializados con los participantes en la reunión; a los delegados por su atención, participación y contribución activas; a CISCO por haber tenido la cortesía de patrocinar las pausas para el café y el cóctel de bienvenida. En su calidad de entidad principal para facilitar la aplicación de la línea de acción C5 de la CMSI, cuyo objetivo es instaurar la confianza y seguridad en la utilización de las TIC, y en el marco de las actividades de normalización y desarrollo que desempeña desde hace mucho tiempo, se subrayó que la UIT seguirá siendo un foro en el que los gobiernos, el sector privado y otros interesados en la ciberseguridad y la PIBI podran debatir los diversos puntos de vista a través de sus diferentes actividades e iniciativas.

71. Se podrán formular comentarios sobre el presente proyecto de informe de la reunión durante los 30 siguientes a su recepción y publicación en el sitio web del taller. La dirección de correo electrónico a la que habrán de dirigirse los comentarios sobre el presente proyecto de informe y sobre el Programa de trabajo de la UIT relativo a la ciberseguridad para prestar asistencia a los países en desarrollo (2007-2009)[50], es la siguiente: cybmail@itu.int.[51] A los efectos de compartir información, se añadirán todos los participantes en la reunión a los foros/listas de correo sobre asuntos relacionados con las actividades relacionadas con la ciberseguridad del UIT-D. Si usted no ha participado directamente en el taller o no está inscrito en la lista de correo, pero le interesa participar en estos debates a través del foro/lista de correo, escriba un mensaje de correo electrónico a la siguiente dirección cybmail@itu.int.

[49] http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/docs/closing-remarks-itu-buenos-aires-18-oct-07.pdf

[50] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme

[51] Dirija sus comentarios acerca del informe del taller a cybmail@itu.int