SECRETARIA DE COMUNICACIONES

REPUBLICA ARGENTINA

# Taller Regional sobre Marcos para la Ciberseguridad y la Protección de la Infraestructura básica de la Información

16-18 de octubre de 2007
Buenos Aires, Argentina

## Proyecto de orden del día de la reunión

*Descripción*: En los albores del siglo XXI, las sociedades modernas dependen cada vez más de las tecnologías de la información y la comunicación (TIC), interconectadas a nivel mundial. Ahora bien, esta interconectividad también genera interdependencias y riesgos que deben gestionarse a nivel nacional, regional e internacional. La mejora de la ciberseguridad y la protección de las infraestructuras básicas de la información son fundamentales para la seguridad y el bienestar económico de todos los países. En el plano nacional, se trata de una responsabilidad compartida que exige adoptar medidas coordinadas relacionadas con la prevención, la preparación, la respuesta y la recuperación en caso de incidentes por parte de las autoridades estatales, el sector privado y los ciudadanos. En los planos regional e internacional, ello exige una cooperación y coordinación con los asociados pertinentes. La formulación y aplicación de un marco para la ciberseguridad y la protección de la infraestructura básica de la información exige un enfoque global.

Este taller forma parte de una serie de eventos regionales organizados conjuntamente por el Sector de Desarrollo de las Telecomunicaciones y el Sector de Normalización de las Telecomunicaciones de la UIT, en colaboración con la Secretaría de Comunicaciones de Argentina. La finalidad del taller es identificar los principales desafíos a los que se enfrentan los países en la región de las Américas al desarrollar marcos para la ciberseguridad y la protección de la infraestructura básica de la información, examinar las prácticas óptimas, intercambiar información sobre las normas técnicas y las actividades de desarrollo emprendidas por la UIT, así como por otras entidades, y examinar la función de varios actores en la promoción de una cultura de ciberseguridad.

| MARTES 16 DE OCTUBRE DE 2007 | |
|---|---|
| **08:00–09:00** | **Inscripción en la reunión** |
| **09:00–09:30** | **Apertura de la reunión y bienvenida** |
| | ***Bienvenida a los participantes***: Secretario de Comunicaciones, Secretaría de Comunicaciones, Argentina<br>***Discurso de apertura***: Un representante del UIT-D<br>***Discurso de apertura***: Un representante del UIT-T |
| **09:30–10:45** | **1ª sesión: ¿Qué es un marco para la ciberseguridad y la protección de la infraestructura básica de la información?** |
| | ***Descripción de la sesión***: La necesidad de generar confianza y seguridad en la utilización de las TIC, promover 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 protección de la infraestructura básica de la información, mientras que otros han empleado un enfoque más liviano y no institucional. En esta sesión se examinarán distintos enfoques adoptados en relación con estos marcos, así como sus componentes, a menudo similares, con el fin de ofrecer a los participantes de la reunión una visión general de las cuestiones y los desafíos que éstos plantean. |
| **10:45–11:00** | **Pausa para el café/té** |
| **11:00–12:30** | **2ª sesión: Desarrollo de una estrategia nacional** |
| | ***Descripción de la sesión***: Las redes electrónicas 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 se tratará 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 región de las Américas a crear estrategias nacionales para la ciberseguridad y la protección de la infraestructura básica de la información. |
| **12:30–14:00** | **Almuerzo** |
| **14:00–15:30** | **3ª sesión: Normas técnicas en materia de ciberseguridad** |
| | ***Descripción de la sesión***: Los organismos de normalización son un actor importante a la hora de abordar la vulnerabilidad de la seguridad en el sector de las TIC. En esta sesión se presentarán algunas de las principales actividades de las organizaciones de normalización, centrándose en el UIT-T y examinando temas tales como la arquitectura de la seguridad, la ciberseguridad, la gestión de la seguridad, la gestión de identidades, el establecimiento de una base de referencia en materia de seguridad para los operadores de redes, y el Plan de Normalización de la Seguridad en las TIC iniciado por la Comisión de Estudio 17 del UIT-T. |
| **15:30–15:45** | **Pausa para el café/té** |
| **15:45–17:00** | **Intercambios de información en forma de mesa redonda sobre un marco para la ciberseguridad y la protección de la infraestructura básica de la información, el desarrollo de una estrategia nacional y las normas técnicas** |
| | • Un moderador para los intercambios de información<br>• Un ponente para el intercambio de información sobre marcos para la ciberseguridad y la protección de la infraestructura básica de la información<br>• Un ponente para el intercambio de información sobre estrategias nacionales<br>• Un ponente para las normas técnicas |
| **17:00–17:15** | **Conclusiones diarias y anuncios** |
| | Un moderador de la reunión para presentar las conclusiones de los debates y anuncios |

| MIÉRCOLES 17 DE OCTUBRE DE 2007 | |
|---|---|
| **09:00–10:15** | **4ª sesión: Supervisión, alerta y respuesta en caso de incidente** |
| | ***Descripción de la sesión***: Una actividad fundamental a la hora de abordar la ciberseguridad a escala nacional es la necesidad de prepararse para los ciberincidentes, detectarlos, gestionarlos y responder a los mismos mediante el establecimiento de mecanismos de supervisión, alerta y respuesta en caso de incidente. Para que la gestión de los incidentes sea eficaz, es necesario examinar la financiación, los recursos humanos, la formación, la capacidad tecnológica, las relaciones entre el gobierno y el sector privado, y los requisitos legales. Es necesario asimismo colaborar en todas las esferas de gobierno, así como con el sector privado, los círculos académicos y las organizaciones regionales e internacionales, para lograr una mayor concienciación sobre los posibles ataques y las medidas necesarias para corregirlos. En esta sesión se examinarán las prácticas óptimas y las normas conexas en lo que se refiere a los aspectos técnicos, de gestión y financieros del establecimiento de mecanismos nacionales o regionales de supervisión, alerta y respuesta en caso de incidente. |
| **10:15–10:30** | **Pausa para el café/té** |
| **10:30–12:00** | **5ª sesión: Luchar contra el correo no solicitado (spam) y las amenazas conexas** |
| | ***Descripción de la sesión***: Uno de los principales riesgos que ponen en peligro la seguridad de Internet es el correo electrónico no solicitado (spam), que de ser una molestia general ha pasado a convertirse en una amenaza más amplia para la ciberseguridad. El correo no solicitado constituye ahora el principal mecanismo para transmitir virus que pueden introducirse en millones de ordenadores (a través de grupos de ordenadores zombis) o para lanzar ataques de usurpación de identidad (phishing) a fin de conseguir información financiera de los particulares o empresas. La usurpación de identidad se refiere al correo electrónico no solicitado enviado con fines fraudulentos, por ejemplo para conseguir información sobre la tarjeta de crédito o los datos bancarios personales. El correo electrónico no solicitado también actúa como plataforma para muchos otros tipos de scam (captación de personas). Aunque es posible utilizar una serie de contramedidas para luchar contra los autores del correo electrónico no solicitado (técnicas, jurídicas, financieras, formación de los usuarios), existe en general una falta de coordinación global en el plano internacional. En esta sesión se examinarán algunas de las normas, prácticas óptimas e iniciativas instauradas para luchar contra el correo electrónico no solicitado. |
| **12:00–13:30** | **Almuerzo** |
| **13:30–15:00** | **6ª sesión: Colaboración entre el gobierno, la industria y las organizaciones de normalización** |
| | ***Descripción de la sesión***: Las asociaciones constituidas entre la industria y el gobierno se basan en tres pilares, a saber, la confianza, el beneficio mutuo y una clara comprensión de las funciones y responsabilidades. Un elemento fundamental de las asociaciones fructíferas constituidas entre la industria y el gobierno es la confianza, un elemento necesario para el establecimiento, el desarrollo y el mantenimiento de relaciones de intercambio entre el sector privado y el gobierno. La condición para que las asociaciones constituidas entre la industria y el gobierno tengan éxito es que todos los participantes puedan beneficiarse de las mismas. Al permitir una comprensión de las funciones y responsabilidades de las distintas partes en materia de ciberseguridad, así como la participación en un intercambio recíproco de información, las asociaciones constituidas entre la industria y el gobierno pueden disminuir los riesgos y aplicar un enfoque más global a la ciberseguridad. En esta sesión se examinarán las asociaciones constituidas entre la industria y el gobierno y se estudiará el ejemplo concreto de la importante función desempeñada por las organizaciones de normalización. |
| **15:00–15:15** | **Pausa para el café/té** |
| **15:15–17:00** | **Intercambios de información en forma de mesa redonda sobre supervisión, alerta y respuesta en caso de incidente, la lucha contra el correo electrónico no solicitado y las amenazas conexas, y la colaboración entre el gobierno, la industria y las organizaciones de normalización** |

| | |
|---|---|
| | • Un moderador para los intercambios de información<br>• Un ponente para la supervisión, alerta y respuesta en caso de incidente<br>• Un ponente para la lucha contra el correo electrónico no solicitado y las amenazas conexas<br>• Un ponente para la colaboración entre el gobierno, la industria y los organismos de normalización |
| **17:00–17:15** | **Conclusiones diarias y anuncios** |
| | Un moderador de la reunión presentará las conclusiones de los debates y anuncios |

| **JUEVES 18 DE OCTUBRE DE 2007** | |
|---|---|
| **09:00–11:00** | **7ª sesión: Base jurídica, desarrollo de la reglamentación y cumplimiento** |
| | ***Descripción de la sesión***: Una legislación apropiada, la coordinación legal internacional y el cumplimiento son elementos importantes para prevenir y detectar la ciberdelincuencia y el uso indebido de las TIC y actuar contra los mismos. Ello exige actualizar el derecho, los procedimientos y las políticas penales para abordar los incidentes en materia de ciberseguridad y actuar contra la ciberdelincuencia. Por ello, muchos países han introducido enmiendas en sus códigos penales, o las están adoptando, de conformidad con lo dispuesto en los convenios y recomendaciones internacionales. En esta sesión se examinarán varios enfoques legales nacionales y las posibles esferas en las que se desplegarán esfuerzos para el cumplimiento y la coordinación legal a nivel internacional. |
| **11:00–11:15** | **Pausa para el café/té** |
| **10:30–12:00** | **8ª sesión: Promover una cultura de ciberseguridad** |
| | ***Descripción de la sesión***: Habida cuenta de que los ordenadores personales y los teléfonos móviles son más potentes que nunca, de la convergencia de las tecnologías, del uso cada vez más generalizado de las TIC y del aumento de las conexiones transfronterizas, todos los participantes que desarrollen, posean, suministren, gestionen, abastezcan y mantengan redes de información deben comprender las cuestiones relacionadas con la ciberseguridad y adoptar las medidas que correspondan a sus funciones para proteger dichas redes. Los gobiernos pueden asumir una función de liderazgo en la promoción de una cultura de ciberseguridad y en la prestación de apoyo a otros actores. En esta sesión se examinará el concepto de la promoción de una cultura de ciberseguridad, se darán ejemplos de iniciativas concretas y se explicarán con mayor detalle las posibles prácticas óptimas. |
| **12:00–13:30** | **Lunch** |
| **13:30–15:00** | **9ª sesión: Cooperación regional e internacional** |
| | ***Descripción de la sesión***: La cooperación regional e internacional es sumamente importante para promover una cultura de seguridad, al igual que la función que desempeñan los foros regionales al facilitar las interacciones y los intercambios. En esta sesión se examinarán algunas de las iniciativas de cooperación en curso en los planos regional e internacional a fin de alentar a los participantes de la reunión a participar en otras medidas concretas que podrían aplicarse en la región de las Américas y a nivel internacional. |
| **15:00–15:15** | **Coffee/Tea Break** |
| **15:15–17:00** | **10ª sesión: Conclusiones, recomendaciones y el camino a seguir** |
| | ***Descripción de la sesión***: En la sesión final de la reunión se informará sobre las principales |

| | |
|---|---|
| | conclusiones del evento, con el objetivo de formular recomendaciones para las actividades futuras y, de este modo, mejorar la ciberseguridad y aumentar la protección de las infraestructuras básicas de la información en la región. |
| **17:00–17:15** | **Clausura de la reunión** |
| | ***Discurso de clausura***: Secretario de Comunicaciones, Secretaría de Comunicaciones, Argentina<br>***Discurso de clausura***: Un representante del UIT-D clausurará la reunión |