Proyecto Número:	
Título del Proyecto:	Difusión de la cultura de ciberseguridad y el combate a las ciberamenazas en América Latina
Fecha estimada de inicio:	Julio 2012
Fecha estimada de finalización:	Junio 2014
Agencias de Cooperación:	ASETA, CITEL, COMTELCA, REGULATEL
Otros Socios Cooperantes:	Agencias del Sistema de Naciones Unidas e IMPACT
Organismo de ejecución:	Unión Internacional de Telecomunicaciones (UIT)
Países beneficiarios:	Países de América Latina de la Región Américas
Gerente de Proyecto de la UIT:	Oficina Regional para las Américas, Brasil

RESUMEN DE LAS CONTRIBUCIONES

A) Presupuesto del Proyecto

Descripción	**US$**
Gastos de Personal	
Consultor Externo (SSA)	90,000
Misiones (Consultor Externo y UIT)	79,000
Servicios externos	36,000
Misceláneo y otros Gastos	36,875
Total:	**241,875**

B) Costos compartidos: US$ 241,875

C) Contribuciones de los países beneficiarios:

En especie: todas aquellas especificadas en este Documento de Proyecto, incluyendo la disponibilidad de instalaciones logísticas

En efectivo: para garantizar la contratación de expertos en caso de que no se identifique otros socios de financiamiento

Breve Descripción:

En términos generales, el objetivo del Proyecto es la planificación, desarrollo y ejecución de programas de creación de capacidades en materia de ciberseguridad, dirigido a los responsables de tomar decisiones en los Gobiernos de países de América Latina, incluidas las agencias a nivel ministerial y los reguladores encauzados principalmente en la necesidad de desarrollar una cultura sostenible y proactiva de ciberseguridad, la sensibilización de aspectos legales para la futura armonización de leyes sobre ciberseguridad, el desarrollo de estrategias nacionales y normas de seguridad. Este Proyecto, tiene como objetivo promover e impulsar a través de programas de capacitación en línea y/o presenciales, la implementación y puesta en práctica de las capacidades de ciberseguridad hacia la consolidación de la Agenda sobre Ciberseguridad Global de la UIT. (ACG).

Para	**Firma**	**Fecha**	**Nombre/Título**
UIT:	_____	___/___/_____	
Socio:	_____	___/___/_____	

1. ANTECEDENTES Y CONTEXTO

1.1 ANTECEDENTES

Las Tecnologías de la Información y la Comunicación (TIC) están transformando constantemente estilos de vida, ya que se han convertido en parte integral de las sociedades modernas, impulsando al usuario final a la vanguardia de las comunicaciones. Las TIC proporcionan comunicaciones en tiempo real, acceso sin fronteras y a una casi ilimitada gama de servicios innovadores y de entretenimiento. Hay un entendimiento común entre los miembros de la comunidad internacional, que las TIC ofrecen oportunidades sin precedentes para acelerar el desarrollo económico y social, al mismo tiempo que el uso indebido y sus vulnerabilidades también han creado nuevas amenazas y desafíos cada vez más allá de las fronteras nacionales para todos los países.

Todo tipo de información está disponible a través de Internet en todos los diferentes formatos, diversos temas y puntos de vista. Cada persona que se encuentra en internet es vulnerable a las Ciberamenazas tales como "software"malicioso (malaware) y ataques cibernéticos, que se están volviendo extremadamente sofisticados. La UIT reconoce que la seguridad de la información y las tecnologías es prioridad crítica para la comunidad internacional. La Ciberseguridad es generalmente del interés de todos y ésta sólo puede lograrse a través de un esfuerzo colaborativo.

En este sentido, La UIT lanzó en el año 2007 la **Agenda sobre Ciberseguridad Global (ACG)**, que es un marco para la cooperación internacional con el objetivo de aumentar la confianza y seguridad en la sociedad de la información. La ACG está diseñada para lograr una mayor cooperación y eficacia, promoviendo la colaboración entre todos los interesados y basándose en las iniciativas en curso para evitar la duplicación de esfuerzos. La ACG se esmera para involucrar a todas las partes interesadas en un esfuerzo concertado para construir confianza y seguridad en la sociedad de la información. La ACG se basa en cinco pilares estratégicos, también conocidos como áreas de trabajo, como siguen: (a) medidas legales, (b) medidas técnicas y de procedimiento, (c) Estructuras organizacionales, d) creación de capacidades y (e) cooperación internacional.

Asimismo, la UIT colabora con la **Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT,** por sus siglas en inglés**)**, una iniciativa internacional público-privada dedicada a mejorar la capacidad de la comunidad mundial para prevenir las Ciberamenazas, defenderse contra ellas y responder a las mismas. La modernísima sede mundial de IMPACT en Cyberjaya, Malasia, se ha convertido en la sede física de la ACG. Esta histórica colaboración proporciona acceso a los 193 Estados Miembros de la UIT a la experiencia, instalaciones y recursos para abordar de manera eficaz las ciberamenazas más graves del mundo. La estrecha sinergia entre las cinco áreas de trabajo de la ACG, los servicios y la infraestructura proporcionada por IMPACT hicieron de esta asociación un paso lógico en la lucha mundial contra las ciberamenazas, la ciberdelincuencia y otros usos indebidos de las TIC .

La colaboración entre la UIT e IMPACT pretende construir sinergias para proporcionar un número de servicios y actividades. Estos incluyen: análisis en tiempo real, recopilación y difusión de información sobre las ciberamenazas globales; un sistema de alerta temprana y de respuesta de emergencia para las ciberamenazas globales; capacitación y desarrollo de habilidades sobre los aspectos técnicos, legales y políticos de la Ciberseguridad. Muchos Estados miembros de la UIT a nivel mundial, incluyendo veintiuno(21) de la región Américas[1] están recibiendo los servicios de ciberseguridad de IMPACT permitiéndoles tener acceso a su Centro de Respuesta Global (CRG, por sus siglas en inglés), propiedad intelectual, servicios de consultoría, informes y mucho más.

---

[1] Antigua y Barbuda, Belice, Brasil, Costa Rica, Cuba, República Dominicana, Ecuador, Granada, Guatemala, Guyana, Honduras, Panamá, Paraguay, Perú, San Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, Surinam, Trinidad y Tobago, Uruguay y Venezuela.

Las iniciativas de IMPACT, tales como el CRG, así como la capacitación y el desarrollo de habilidades, garantía de la seguridad, investigación y cooperación internacional, se llevarán a cabo bajo los auspicios de la ACG.

El Centro de Respuesta Global (CRG) juega un papel fundamental para lograr el objetivo de la Agenda sobre Ciberseguridad Global (ACG) de la UIT de implantar las medidas técnicas para combatir las ciberamenazas nuevas y cambiantes. Los dos principales puntos de interés del CRG son NEWS (sistema de alerta temprana en red) y ESCAPE (La Plataforma de aplicación colaborativa y electrónicamente segura para expertos). El CRG está concebido para ser el centro de recursos sobre ciberamenazas más avanzado del mundo. Al trabajar con los principales socios, incluyendo gobiernos y academia, el Centro ofrecerá a la comunidad mundial un sistema total de alerta temprana en tiempo real. NEWS ayudará a los países Miembros a identificar de forma temprana las ciberamenazas y les orientará sobre las medidas que pueden tomar para mitigar sus efectos.

El CRG también tiene como objetivo proporcionar a los Estados miembros de la UIT acceso a herramientas y sistemas especializados, incluyendo la antes mencionada plataforma ESCAPE, que es una herramienta electrónica que permite a los expertos autorizados de varios países aunar recursos y colaborar entre sí en forma remota, aún dentro de un entorno seguro y fiable. Al juntar recursos y conocimiento de diferentes países en poco tiempo, ESCAPE permitirá que a las naciones individualmente y a la comunidad mundial responder inmediatamente a las ciberamenazas, especialmente durante situaciones de crisis.

IMPACT está listo para ayudar a sus Estados miembros socios[2] a identificar y superar las inminentes ciberamenazas, por medio del CRG. A través de IMPACT y su CRG, los países socios, pueden mejorar su conocimiento y conciencia del entorno de las ciberamenazas que les afecta, mientras se aprende sobre posibles soluciones para superar estos ataques malintencionados. Con la puesta en marcha de la ACG de la UIT, los actuales Estados miembros de la UIT son elegibles para convertirse en países socios de IMPACT.

En el marco de la ACG y en consonancia con el mandato de la UIT para ayudar a los Estados Miembros en el desarrollo de capacidades de ciberseguridad, entre otras cosas, la UIT trabaja para facilitar el despliegue de recursos de ciberseguridad necesarios para combatir las ciberamenazas. Como tal, la Oficina de Desarrollo de las Telecomunicaciones de la UIT (BDT) está jugando un papel clave en la implementación de los objetivos principales de la ACG y está respondiendo a las necesidades de los Estados Miembros.

1.2 CONTEXTO

Con el importante papel que las TIC desempeñan hoy en la prestación de servicios en sectores tan variados como la salud, la educación, las finanzas y el comercio; es vital crear conciencia de las oportunidades ofrecidas por un entorno cibernético seguro y de las amenazas inherentes al ciberespacio. Como las amenazas se pueden originar en cualquier parte del mundo, los retos son intrínsecamente internacionales en su alcance y requieren la cooperación internacional, la asistencia en la investigación y las provisiones comunes, sustantivas y de procedimiento.

La Internet y las TIC han permitido la interconexión entre países y éstos ni pueden cerrar fácilmente sus fronteras a las ciberamenazas entrantes ni pueden contener aquellas procedentes de su interior. La ciberseguridad es mundial y de gran alcance como lo es la Internet y las soluciones deben ser armonizadas en a través de todas las fronteras. Esto conlleva necesariamente la cooperación internacional, no sólo a nivel de Gobierno, sino también la industria, organizaciones internacionales y no gubernamentales. La ciberseguridad involucra todo tipo de medidas, por esta razón, la ACG busca aprovechar el poder de colaboración de las diferentes partes interesadas para llegar a estrategias globales con el fin de mejorar la ciberseguridad.

[2] http://www.impact-alliance.org/countries/alphabetical-list.html

Desde su lanzamiento, la ACG se ha granjeado el apoyo y reconocimiento de líderes y expertos en ciberseguridad de todo el mundo[3]. La ACG ha promovido iniciativas como la Protección de la Infancia en Línea (PIeL) y a través de su asociación con IMPACT y con el apoyo de los más importantes líderes mundiales, está desplegando en la actualidad soluciones de ciberseguridad en países alrededor del mundo.

Es importante desarrollar Programas encaminados a crear igualdad de condiciones para concientizar y crear capacidades a todo nivel. Estos Programas también se deben desarrollar en el campo internacional.

Junto con las medidas legales, la cooperación internacional y otras áreas de trabajo, la creación de capacidades es un pilar importante para el establecimiento de sistemas jurídicos armonizados y desarrolla una cultura sostenible y proactiva de ciberseguridad. La comunidad internacional identificó varios retos en el campo de la ciberseguridad y algunos de ellos concierne a la eficacia con que se educa al usuario final tomando en cuenta que la comprensión y la conciencia de los peligros potenciales son cruciales. Además, también es importante comprender los aspectos jurídicos de la ciberseguridad a fin de avanzar hacia la armonización de los marcos legales. Las amenazas pueden originarse en cualquier parte del mundo y es importante que los países armonicen sus marcos jurídicos para combatir los ciberdelitos y facilitar la cooperación internacional. Los países también necesitan desarrollar sus estrategias nacionales examinando sus recursos existentes para hacer frente a los retos de la ciberseguridad, identificando sus requerimientos y esbozando un plan de respuesta nacional. Todos estos temas le conciernen a las partes interesadas de los gobiernos.

La Conferencia Mundial de Desarrollo de las Telecomunicaciones 2010 (CMDT-10) diseñó y adoptó el Plan de Acción de Hyderabad (HAP) para ayudar a los países en desarrollo a promover el desarrollo equitativo y sostenible de las redes y servicios de las Tecnologías de la Información y la Comunicación (TIC). El HAP es un paquete completo de cuatro años de actividades, que incluye cinco Programas. Entre estos Programas, el Programa 2[4] fue diseñado para enfocarse en la Ciberseguridad como una de las áreas prioritarias. En este marco, el objetivo de la UIT/BDT es apoyar a los Estados Miembros de la UIT en el desarrollo de sus estrategias nacionales y/o regionales de ciberseguridad, como un paso esencial hacia la creación de capacidades nacionales para afrontar las ciberamenazas. En consonancia con la Cumbre Mundial sobre la sociedad de la Información (CMSI) Línea de Acción C5, "crear confianza y seguridad en el uso de las TIC", la UIT está trabajando para asumir los retos emergentes de la Sociedad de la Información.

Este proyecto está directamente relacionado con las **Iniciativas Regionales 3 y 5 para la Región Américas** basado en la necesidad de concienciar la ciberseguridad para apoyar la promoción sana y segura de las TIC y el acceso a la banda ancha en zonas urbanas/rurales (Iniciativa Regional 3), al mismo tiempo, desarrollar recurso humano sobre las TIC para los encargados de tomar decisiones (Iniciativa Regional 5). Los gobiernos deberían difundir ampliamente la cultura y el conocimiento sobre la Ciberseguridad fomentando la inclusión digital en un entorno electrónico protegido y seguro, promocionando la accesibilidad y el uso de las telecomunicaciones y las TIC para el desarrollo económico y social, incluidas las personas con necesidades especiales. También, como se indica en la Iniciativa Regional 5, se espera promover la cooperación técnica entre las instituciones de capacitación en telecomunicaciones/TIC para la prestación sostenible de programas especiales.

Tomando en cuenta que las computadoras personales, teléfonos móviles y otros dispositivos son cada vez más potentes, que las tecnologías están convergiendo, que el uso de las TIC es cada vez más generalizado, y que las conexiones a través de las fronteras nacionales van en aumento, todos los entes involucrados que desarrollan, poseen, proporcionan, administran, brindan servicio y mantienen redes de información deben entender las cuestiones de ciberseguridad y adoptar medidas adecuadas a sus funciones para

[3] Su Excelencia Dr. Óscar Arias Sánchez, Presidente de la República de Costa Rica y Premio Nobel de la Paz y Su Excelencia Blaise Compaoré, Presidente de Burkina Faso , ambos son defensores de la Agenda de la UIT sobre Ciberseguridad Global (ACG).

[4] Programa 2: Ciberseguridad, Aplicaciones TIC y Cuestiones relacionadas con las Redes IP.

proteger las redes. Los gobiernos desempeñan un papel clave tomando el liderazgo en la promoción de una cultura de ciberseguridad y haciendo frente a sus retos.

2. DESCRIPCIÓN DEL PROYECTO

En términos generales, el objetivo del Proyecto es la planificación, desarrollo y ejecución de programas de creación de capacidades en materia de ciberseguridad dirigido a los encargados de tomar decisiones en el Gobierno de países de América Latina, incluidos los organismos ministeriales y reguladores encauzados principalmente en la necesidad de desarrollar una cultura sostenible y proactiva de ciberseguridad, la sensibilización de aspectos legales para la futura armonización de leyes sobre ciberseguridad, el desarrollo de estrategias nacionales y normas de seguridad. Este Proyecto, tiene como objetivo promover e impulsar a través de programas de capacitación en línea y/o presenciales, la implementación y puesta en práctica de las capacidades de ciberseguridad hacia la consolidación de la Agenda sobre Ciberseguridad Global (ACG) de la UIT.

3. RESULTADOS ESPERADOS

Se prevén los siguientes productos:

3.1 Desarrollo de servicios de asesoría sobre las “Perspectivas y Retos de la Ciberseguridad en América Latina". .

3.2 Planificación, desarrollo y ejecución de las actividades de capacitación en línea y/ o presencial basadas en los recursos legales de la UIT, es decir el “Conjunto de herramientas de la UIT para la Legislación del Ciberdelito”, " y El Ciberdelito: una guía para los países en desarrollo". Esta actividad tomará también en cuenta los instrumentos internacionales ya existentes y se realizará en el marco general de colaboración entre la UIT y la Oficina de las Naciones Unidas contra las Drogas y el Delito (ONUDD), donde los dos órganos de las Naciones Unidas acordaron cooperar a nivel mundial en la prestación de asistencia técnica. Por lo tanto, algunas actividades específicas se realizarán conjuntamente por la UIT y la ONUDD.

3.3 Planificación, desarrollo y ejecución de las actividades de capacitación en línea o presencial basadas en la "Guía de la UIT para la Estrategia Nacional de Ciberseguridad ".

3.4 Organización de Talleres de evaluación, presenciales, regionales y subregionales sobre el establecimiento de estructuras organizativas sólidas con responsabilidades nacionales, como el Equipo Nacional de Respuesta ante Incidentes Informáticos (CIRT), adaptados a la implementación del Centro de Respuesta Global de la UIT-IMPACT.

Los programas de capacitación se ejecutarán con el apoyo del Centro de Excelencia de la UIT para la región Américas.

4. INDICADORES

Se utilizarán los siguientes indicadores para medir el éxito del Proyecto:

4.1 Elaboración de un (1) informe/evaluación sobre " Retos y Perspectivas de la Ciberseguridad en América Latina".

4.2 Al menos una (1) actividad de capacitación ya sea en línea y/o presencial sobre el establecimiento y armonización de la legislación del Ciberdelito, utilizando herramientas de la UIT y otras herramientas existentes y dentro del marco de colaboración de la UIT/ONUDD.

4.3 Al menos una (1) actividad de capacitación ya sea en línea y/o presencial sobre la "Guía de la UIT para la Estrategia Nacional de Ciberseguridad"

4.4 Al menos un (1) Taller presencial, regional/subregional para el establecimiento de Equipos Nacionales de Respuesta ante Incidentes Informáticos (CIRT).

4.5 Al menos un 70% de la audiencia a la que está orientada las actividades y talleres de capacitación sean especialistas y encargados de tomar decisiones de las Instituciones de Gobierno.

4.6 Al menos un 10% de la audiencia a la que está orientada las actividades de capacitación y talleres sean representantes de Instituciones académicas y de investigación.

5. PRINCIPALES ACTIVIDADES

De conformidad con la Agenda sobre Ciberseguridad Global (ACG) de la UIT, se han previsto llevar a cabo las siguientes actividades en el marco de este Proyecto:

5.1 Desarrollo de servicios de consultoría para realizar una evaluación de los retos y perspectivas de la ciberseguridad en América Latina.

5.2 Planificación, desarrollo y ejecución de las actividades de capacitación ya sea en línea y/o presenciales basadas en los **Recursos Jurídicos de la UIT**:

Los recursos jurídicos de la UIT sobre ciberdelitos[5] actualmente constan de dos entregables principales: 1) la publicación de la UIT titulada **"El Ciberdelito: Guía para los países en desarrollo"** que tiene como objetivo ayudar a los países en desarrollo a entender mejor las implicaciones nacionales e internacionales de las ciberamenazas en constante crecimiento, evaluar los requisitos de los actuales instrumentos nacionales, regionales e internacionales y colaborar con los países para establecer unas bases jurídicas sólidas; 2) "**Conjunto de herramientas de la UIT para la Legislación del Ciberdelito"** , un instrumento práctico que los países pueden utilizar para la elaboración de un marco jurídico sobre ciberseguridad y leyes relacionadas. Este instrumento pretende servir de guía a los países deseosos de desarrollar, formular o modificar sus propias leyes de ciberdelitos y avanzar en la armonización mundial de estas leyes , sirviendo como un recurso central para ayudar a los legisladores, abogados, funcionarios de gobierno, expertos en políticas y representantes de la industria a nivel mundial a movilizar sus países hacia un marco jurídico consistente que proteja contra el uso inadecuado de las TIC. Esta actividad se llevará a cabo en el marco de colaboración entre la UIT y ONUDD.

[5] *Los recursos jurídicos de la UIT están disponibles en: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html*

5.3 Organización de Talleres de evaluación presenciales, regionales y subregionales sobre el establecimiento de estructuras organizativas sólidas con responsabilidades nacionales, es decir el Equipo Nacional de Respuesta ante Incidentes Informáticos (CIRT), adaptado a la implementación del Centro de Respuesta Global de la UIT-IMPACT :

El objetivo primario de esta actividad es ayudar a los Estados miembros a evaluar su grado de preparación para implementar un CIRT nacional. El CIRT nacional proporcionará recursos para identificar, responder y gestionar ciberamenazas y al mismo tiempo mejorará la postura de la ciberseguridad del país. El establecimiento del CIRT nacional, aunado a los recursos ya implementados de la UIT IMPACT, como es el CRG y considerando las mejores prácticas internacionales (por ejemplo, FIRST- Foro Global de Equipos de Respuesta y Seguridad frente a Incidentes Informáticos) puede jugar un papel clave en el mantenimiento de una vigilancia continua para defender la infraestructura y/o activos nacionales contra los ataques cibernéticos, y servir también como un centro importante de control cibernético para el análisis de información sobre amenazas. Las actividades específicas pueden incluir:

a. Estudiar el estado de preparación de las necesidades actuales de los países.
b. Estudiar y sugerir los requisitos institucionales y organizacionales y los procedimientos para establecer los CIRTs nacionales.
c. Crear capacidades para los CIRTs.
d. Llevar a cabo entrenamientos de desarrollo de recurso humano con el propósito de impartir conocimientos y habilidades para la operación, mantenimiento y coordinación de los CIRTs con los organismos pertinentes, tanto locales como internacionales.
e. Diseñar las especificaciones de hardware y software para los CIRTs.

5.4 Planificación, desarrollo y ejecución de las actividades de capacitación en línea y/o presenciales basadas en la **Guía de la UIT para la Estrategia Nacional de Ciberseguridad:**

La **Guía de la UIT para la Estrategia Nacional de Ciberseguridad** se centra en los temas que los países deben considerar al momento de elaborar o revisar las estrategias nacionales de ciberseguridad. Como varían las capacidades nacionales, las necesidades y las amenazas, los países utilizan valores nacionales como la base para las estrategias, por dos razones principales: En primer lugar, los intereses nacionales y la cultura influyen en la percepción del riesgo y el éxito relativo de las defensas contra las ciberamenazas. En segundo lugar, una estrategia basada en los valores nacionales es probable que gane el apoyo de los interesados, como el poder judicial y el sector privado. Considerando que la ciberseguridad es una cuestión de política nacional, la Guía adopta el paradigma de la estrategia fines-formas-medios, debido a su popularidad con los legisladores nacionales. La actividad tendrá el objetivo principal de ayudar a los Estados Miembros en la creación de un plan para el establecimiento de una estrategia nacional de ciberseguridad y crear la capacidad necesaria para ejecutarlo.

6. INSUMOS

6.1 La Unión Internacional de Telecomunicaciones (UIT)

La UIT será el organismo de ejecución. La UIT asumirá la administración de los recursos de personal que serán financiados y contratados a través de este Proyecto. Se ofrecerá información sobre temas relacionados al acceso y uso de las TIC, acceso a materiales existentes de la UIT, incluyendo cursos de capacitación y publicaciones pertinentes. La UIT hará uso de sus capacidades, cuidados y diligencia para

garantizar el éxito del Proyecto, asimismo, designará un Coordinador de Proyecto para supervisar y evaluar su ejecución e identificará y contratará los especialistas para implementar los programas de capacitación.

6.2 Socios:

Es necesario identificar socios interesados en proporcionar apoyo financiero para la ejecución del Proyecto. El Proyecto prevé la contratación de expertos para llevar a cabo las actividades de capacitación, así como la coordinación de los talleres con un costo estimado de **USD 241,875** . El costo de las actividades previstas a realizarse en el marco de este Proyecto puede ser cubierto por los programas y/o iniciativas de las organizaciones que trabajan para el combate de las ciberamenazas.

6.3 Beneficiarios:

Se espera que las organizaciones regionales y los países respectivos apoyen la organización de las actividades de capacitación y los talleres, mediante recursos de personal e instalaciones locales. También, se espera que los países beneficiarios proporcionen información/datos necesarios para llevar a cabo el trabajo, locales seguros para albergar las actividades de capacitación y talleres, arreglos de logística, apoyo y cualquier otro tipo de asistencia al Proyecto que puede ser requerido por el personal del Proyecto.

7. EVALUACIÓN DEL RIESGO

7.1 Las organizaciones regionales, las diferentes instituciones de Gobierno nacionales y socios locales comprometidos con el Proyecto trabajarán en estrecha coordinación, ya que la falta de coordinación y/o colaboración entre las partes interesadas puede representar un riesgo.

7.2 La colaboración de los socios importantes del Gobierno es crucial para el desarrollo del Proyecto a manera de reducir cualquier riesgo de implementación a este nivel.

7.3 El principal riesgo es que las actividades pueden sufrir retrasos debido a eventos y/o circunstancias imprevistas. En este sentido, el Coordinador de Proyecto garantizará la preparación de cada una de las actividades en su debido tiempo.

8. GESTION DEL PROYECTO

8.1 Las funciones y responsabilidades de los diferentes actores se definirán claramente en una reunión entre las partes interesadas al comienzo del Proyecto. La UIT es el organismo de ejecución. Después de identificar el principal organismo de financiamiento y a fin de facilitar la ejecución de este Proyecto, la UIT constituirá un equipo de proyecto financiado por el Proyecto, incluyendo un Coordinador de Proyecto.

8.2 El Coordinador de Proyecto será responsable de la ejecución del mismo, bajo la supervisión del Director Regional de la oficina de la UIT para la región Américas, en estrecha coordinación con las oficinas de Área, así como con los Departamentos correspondientes en la Sede de la UIT.

8.3 El Coordinador del Proyecto trabajará en estrecha coordinación con los Departamentos correspondientes en la Sede de la UIT para la gestión y seguimiento de todos los aspectos administrativos

y financieros involucrados en el Proyecto y proporcionará periódicamente los Informes de Progreso correspondientes.

8.4 El Coordinador de Proyecto presentará a los socios financieros, el Estado Financiero del Proyecto, el que será actualizado por el Departamento correspondiente en la sede de la UIT.

9. MONITOREO Y EVALUACIÓN

9.1 Se vigilará el progreso del Proyecto a través de Informes periódicos que serán preparados por el Coordinador del Proyecto.

9.2 Se preparará al final del Proyecto, un Informe final de evaluación.

9.3 Se necesitarán probablemente Informes especiales y serán proporcionados de acuerdo a la situación.

9.4 Se organizarán visitas de campo a aquellas actividades de capacitación presenciales que requieran una evaluación directa de su progreso.

9.5 Se podrán organizar reuniones de coordinación y evaluación según lo decidan las Partes involucradas

9.6 El Coordinador del Proyecto, en estrecha coordinación con las Partes preparará un Informe de Cierre del Proyecto.

10. PLAN DE TRABAJO

Actividades	2012		2013				2014	
	3T	4T	1T	2T	3T	4T	1T	2T
Identificación del socio principal de financiamiento								
Informe/Evaluación sobre "Los Retos y Perspectivas de la Ciberseguridad en América Latina"								
Informe de Progreso								
Implementación de las actividades de capacitación en línea sobre los "Recursos Jurídicos de la UIT"								
Implementación de las actividades de capacitación en línea sobre la "Guía de la UIT para la Estrategia Nacional de Ciberseguridad"								
Informe de Progreso								
Implementación de un Taller presencial, regional/subregional sobre el establecimiento de Equipo Nacional de Respuesta ante Incidentes Informáticos (CIRT)								
Informe de Progreso								
Informe Final								
Cierre del Proyecto								

11. PRESUPUESTO

El presupuesto estimado para el Proyecto es el siguiente:

Clase de Financiación	Descripción	Presupuesto en Dólares Americanos
3000	GASTOS DE PERSONAL	90,000
3100	GASTOS DE MISIÓN	79,000
3300	SERVICIOS EXTERNOS	36,000
	MISCELANEO Y OTROS GASTOS	36,875
	PRESUPUESTO TOTAL:	241,875