

---

# Foro de Ciberseguridad y Tercer Taller Ejercicio Práctico de Aprendizaje Aplicado para Equipos de Respuesta Ante Emergencias Cibernéticas para la Región de América



## Una revisión de las actividades de la UIT sobre Ciberseguridad

3 de Agosto 2015  
Bogotá - Colombia



*Committed to connecting the world*

---

# Definición de Ciberseguridad

---

- De acuerdo a la recomendación UIT-T X.1205, sobre Ciberseguridad:
- Ciberseguridad es la colección de herramientas, regulaciones, conceptos de seguridad, dispositivos de seguridad, guías, manejo de riesgos, acciones, entrenamiento, mejores practicas, aseguramiento y tecnologías que pueden ser utilizadas para proteger el ciber entorno y los activos de los Usuarios y de la Organización. Estos activos incluyen equipos computacionales de conexión, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de Información transmitida o almacenada en el ciber entorno. El esfuerzo en Ciberseguridad es por asegurar el éxito y el mantenimiento de las propiedades en seguridad de los activos de los usuarios y de la organización contra los riesgos relevantes de Ciberseguridad. Los objetivos generales de seguridad son:
  - Disponibilidad
  - Integridad, lo que incluye autenticidad
  - Confidencialidad

12% de usuarios de **redes sociales** dicen que alguien los ha intervenido con una cuenta ficticia en su red social



25% de los usuarios comparte sus claves de acceso a sus redes sociales con otras personas y se conectan con gente que no conocen



# WSIS y Promoción de una Cultura Global sobre Cyberseguridad

## De WSIS fase II: *Agenda de Tunesia*

**39.** Buscamos construir confianza y seguridad en el uso de las TIC a través del fortalecimiento de un marco de trabajo de confianza. **Reafirmamos la necesidad de promover, desarrollar e implementar una cultura global de ciberseguridad en cooperación con los sectores interesados**, como está establecido en la resolución 57/239 UNGA y otros marcos de trabajo regionales.

Esta cultura requiere una **acción nacional** y el **incremento de cooperación internacional** para fortalecer la seguridad mientras se mejora la protección de la información personal y la privacidad de los datos. El desarrollo continuo de la cultura de ciberseguridad debe mejorar el acceso y las transacciones y debe tomar en cuenta el desarrollo económico y social de cada país tomando en cuenta los aspectos de desarrollo de la Sociedad de Información.

# Marco de trabajo global sobre Ciberseguridad

---

En la Cumbre Mundial de la Sociedad de la Información (WSIS) en 2005, los líderes de la comunidad internacional confiaron a la UIT que actúe como facilitador de

## Línea de Acción WSIS C5:



**world summit**  
on the **information society**  
Geneva 2003 - Tunis 2005

## “Construyendo confianza y seguridad en el uso de las TICs”

Resolución 130 Plenipotenciario Busan, 2014

Fortalecer el rol de la UIT para construir confianza y seguridad en el uso de las TIC

Resolución 174 Plenipotenciario Busan, 2014

El rol de la UIT con respecto a asuntos de políticas públicas internacionales relacionado con el riesgo del uso malintencionado de las TIC

Resolución 179 Plenipotenciario Busan, 2014

El rol de la UIT en Protección de la Niñez en el uso de las TIC



Committed to connecting the world

# Agenda Global de Ciberseguridad - UIT

---

## “Construyendo confianza y seguridad en el uso de las TICs”

En el 2007, el Secretario General de la UIT lanzó

La **Agenda Global de Ciberseguridad**, un marco de trabajo internacional para colaborar en asuntos de ciberseguridad que considera

### Cinco áreas principales:

1. Asuntos Legales
2. Medidas técnicas y de procedimiento
3. Estructura organizacional
4. Capacitación
5. Cooperación Internacional





## ▪ **Objetivo:**

Armonización de marcos legales y elaboración de estrategias para legislación global de cibercrimen  
Aplicable e interoperable con medidas nacionales/regionales

### Actividades/Iniciativas relacionadas

#### Recursos

- Recursos legislativos de la UIT sobre Cibercrimen
- UIT Toolkit para Legislación sobre Cibercrimen

#### Publicaciones

- Publicación UIT sobre entendimiento del Cibercrimen:
- Una guía para Países en vías de Desarrollo

#### Eventos y Capacitación

- Capacitación, entrenamiento (capacitación para jueces, etc.)
- Talleres regionales y eventos



## ▪ **Objetivo:**

Desarrollo de estrategias para el establecimiento De protocolos globales aceptados en seguridad, normas, criterios mínimos de seguridad y esquemas de acreditación para aplicaciones y sistemas de hardware y software



## Actividades/Iniciativas Relativas

### Actividades

- UIT Trabajo en Normalización
- Colaboración en promoción del Roadmap de Normas de Seguridad TIC
- Actividades sobre seguridad del sector de Radiocomunicaciones de la UIT

### Grupos de Estudio

- ITU-T Comisión de Estudio 17
- ITU-D Comisión de Estudio 2
- ITU-D Comisión de Estudio 1

# Estructura Organizacional



## ▪ Objetivo:

Elaboración de estrategias globales para la creación de estructuras organizacionales nacionales y regionales y políticas sobre cibercrimen, vigilancia, advertencia y respuesta ante incidentes y sistemas de identidades universal

### Actividades/Iniciativas Relacionadas

#### Sociedades

- Sociedades con entidades - servicios específicos a países miembros

#### Proyectos

- **Desarrollo de national computer incident response teams (CIRTs)** y vigilancia, advertencia y capacitación relacionada con respuesta ante incidentes

#### Capacitación/Asistencia

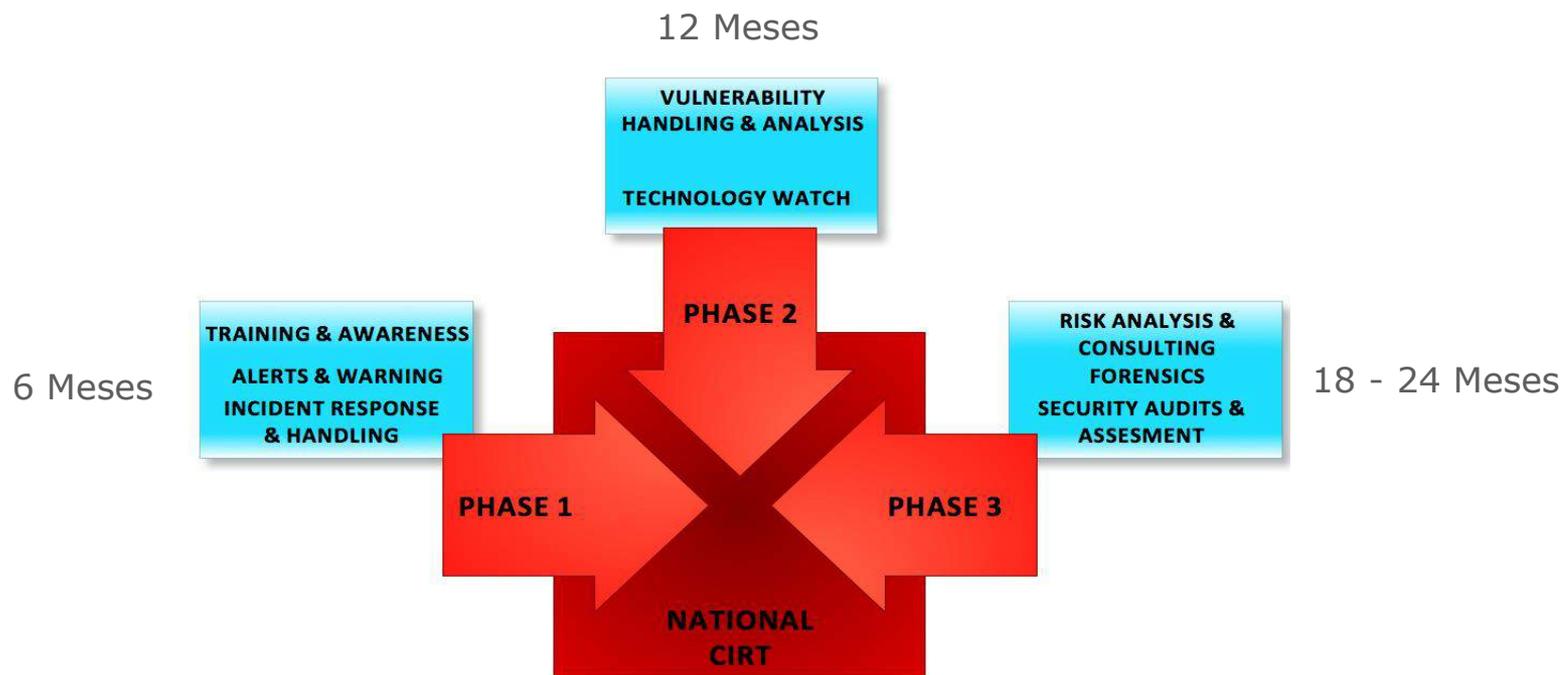
- Capacitación
- Talleres Regionales y eventos
- Asistencia directa a países



### *CIRT Nacional*

- Asegurar coordinación y cooperación con sectores nacionales y regionales
  - Asegurar sostenibilidad en capacidades adquiridas o desarrolladas sobre ciberseguridad, que permitan a la nación construir y extender beneficios a otros sectores públicos y privados
- Asegurar coordinación de ciberseguridad nacional sobre defensa y recuperación
  - Asegurar continuidad en servicios esenciales para ciudadanos en situaciones de crisis
  - Asistir en protección y recuperación de servicios esenciales de infraestructuras de información crítica para la nación
  - Reestablecer control en diseminación de información durante un incidente

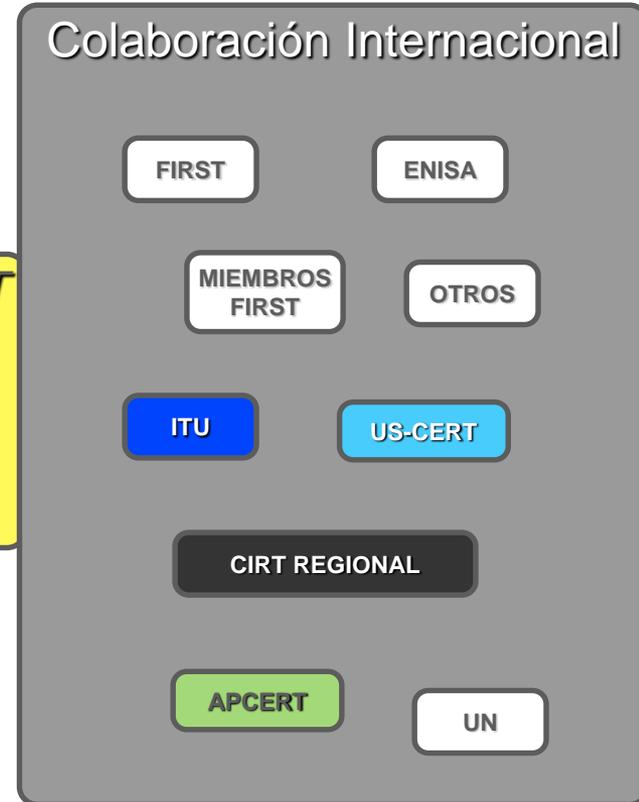
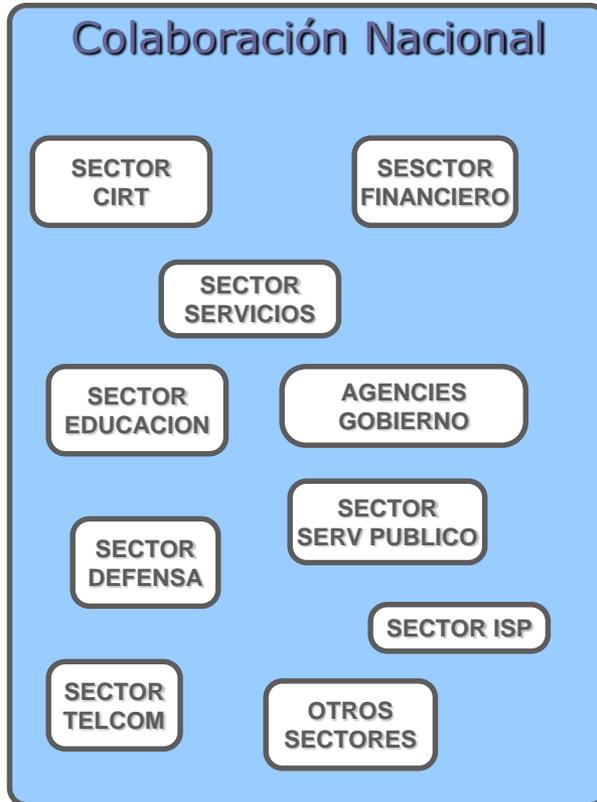




Los entregables de la UIT es solamente para la fase 1

### Capacidades Nacionales del CIRT en la FASE 1

- Concienciar en el país sobre Actividades de Ciberseguridad
- Enviar Alertas y advertir varios sectores
- Manejar y Responder incidentes de Ciberseguridad



**ESTABLECER COLABORACIÓN DESDE EL PRIMER DÍA (INCLUIR OTROS CIRT/CERT COMO SOCIOS ASISTENTES EN LA IMPLEMENTACIÓN DEL CIRT)**

# Factores Críticos de Éxito – Establecimiento de *CIRT* Nacional



- Comprometimiento del País al más alto nivel
- Apoyo al más alto nivel para inclusión de agencias relevantes
- Comunicar el valor estratégico al Programa País de Ciberseguridad
- Diseñar y comunicar la visión del *CIRT* y el plan operacional para alinearse al país
- Implementar Herramientas y procesos del *CIRT* Nacional alineados con la visión y el plan operacional
- Anunciar al país las operaciones del *CIRT* Nacional
- Evaluar periódicamente la efectividad del *CIRT*
- Revisiones periódicas para ajustarse al Roadmap del *CIRT* Nacional



Committed to connecting the world



- Evaluación nacional CIRT Bolivia  
Octubre 2014
- CIRT Trinidad y Tobago  
Implementación y capacitación  
11 al 22 de Mayo 2015
- CIRT Jamaica  
Implementación y capacitación  
25 de Mayo al 5 de Junio 2015
- CIRT Barbados  
En proceso de implementación durante 2015
- Existe la Necesidad de un Centro Regional y Centros Subregionales  
de Ciberseguridad





## ▪ **Objetivo:**

Desarrollo de estrategias globales para facilitar capacitación humana e institucional en todos los aspectos de ciberseguridad



## Actividades/Iniciativas Relacionadas

### Recursos y Toolkits

- Herramientas UIT  
Ciberseguridad Nacional/  
CIIP Autoevaluación
- UIT Toolkit para  
promocionar una cultura de  
ciberseguridad
- **Borrador de guías de  
Estrategia Nacional de  
Ciberseguridad**

### Capacitación y Eventos

- Capacitación y entrenamiento  
en todos los pilares de la GCA
- Eventos y talleres

# Guías de Estrategia de la UIT sobre Ciberseguridad Nacional



- Provee ayudas para desarrollo de Estrategias de Ciberseguridad Nacional
- Provee guías para reguladores sobre:
  - Direccionamiento de asuntos de Ciberseguridad nacional
  - Consejos para formular estrategias nacionales de Ciberseguridad
- Utiliza el trabajo de la UIT (SG17, Q22, etc) y el modelo GCA apoyando el desarrollo de las estrategias nacionales de Ciberseguridad





## ▪ **Objetivo:**

Desarrollo de propuestas para mejorar el dialogo internacional sobre asuntos que conciernan a la Ciberseguridad y mejore la cooperación y coordinación de actividades relevantes



## Actividades/Iniciativas Relacionadas

### Trabajo Conjunto

- Secretaría-General UIT  
Entregables del Alto Grupo de Expertos (HLEG)

### Compartir Información

- Colaboración
- ITU Cybersecurity Gateway
- **Iniciativa de la UIT sobre Child Online Protection (COP)**

### Conferencias/Eventos

- Foro Mundial de Política de las Telecomunicaciones/TIC (WTPF) 2009
- Foros regionales sobre ciberseguridad



## ▪ **Objetivo:**

Capacitación, cooperación entre CERTs de la región,  
Trabajo conjunto, establecimiento de redes de trabajo  
en Ciberseguridad, práctica con escenarios reales

## Eventos Realizados

### Cyberdrill 2013

- Primer Cyberdrill
- Montevideo Uruguay
- 26 al 28 Agosto 2013

### Cyberdrill 2014

- Segundo Cyberdrill
- Lima Perú
- 8 al 10 Septiembre 2014

### Foro Ciberseguridad 2015

- Foro Regional y Tercer  
Cyberdrill 2015
- Bogotá Colombia
- 3 al 5 de Agosto 2015



## ITU-T Study Group 17

- Grupo líder para Seguridades de las Telecomunicaciones
- Mandato Cuestión 4/17 (Q.4/17): Ciberseguridad
- Provee Normas de Seguridades en las TIC
- ITU-T Cybersecurity Information Exchange Framework (CYBEX)
- ITU-T Security Manual "Security in telecommunications and information technology"
- Focus Group sobre Identity Management (IdM)
- Aprobadas más de 100 Recomendaciones sobre seguridad para las comunicaciones
- JCA en COP



## **La UIT-R ha establecido principios claros de seguridad para redes International Mobile Telecommunications-2000 (3G and 4G).**

- ITU-R M.1078: Security principles International Mobile Telecommunications-2000
- ITU-R M.1223: Evaluation of security mechanisms for IMT-2000
- ITU-R M.1457: Detailed specifications radio interfaces of IMT-2000
- ITU-R M.1645: Framework and overall objectives future development of IMT-2000
- ITU-R M.2012: Detailed specifications terrestrial radio interfaces of IMT-Advanced
- ITU-R S.1250: Network management architecture for digital satellite systems
- ITU-R S.1711: Performance enhancements transmission control protocol over satellite



## **Objetivo**

El Global Cybersecurity Index (GCI) intenta medir y establecer en rangos a al nivel de desarrollo en ciberseguridad en las cinco áreas:

- Medidas legales
- Medidas técnicas
- Medidas organizacionales
- Capacitación
- Cooperación Nacional e Internacional

## **Meta**

Promover estrategias de gobierno a nivel nacional

Conducir esfuerzos de implementación entre industrias y sectores

Integrar seguridad en el núcleo del progreso tecnológico

Fomentar una cultura global de ciberseguridad

**ABI**research®



# Global Cybersecurity Index

international  
telecommunication  
union

# Proyecto de Mejorando Ciberseguridad en los Países menos Desarrollados

- Intenta apoyar a los Países menos desarrollados para fortalecer sus capacidades en Ciberseguridad.
- Evaluación de ministerios claves y la posterior provisión de soluciones
- Protección de la infraestructura nacional lo que incluye infraestructura de Información crítica, para tener un acceso más seguro en la utilización del Internet y proteger a los usuarios
- Servir a la prioridades nacionales y maximizar beneficios socio-económicos alineado con el World Summit on the Information Society (WSIS) y los Objetivos de Desarrollo del Milenio (MDGs).
- Mejorar capacidad técnica nacional en Ciberseguridad
- Talleres en línea o presenciales
- Mejorar la respuesta nacional ante ciber amenazas
- Guías personalizadas de legislación en Ciberseguridad
- Equipos y dispositivos de Ciberseguridad entregados a los ministerios
- Programas de capacitación técnicos y de regulaciones



**La parte más débil de la cadena indica nuestra seguridad...**

..... November 2010 .....



Committed to connecting the world

# Child Online Protection



## ■ Child Online Protection (COP)

COP es una iniciativa creada por la UIT,  
Su intención es enfrentar asuntos sobre ciberseguridad, legales, técnicos, organizacionales y de procedimiento, capacitación y cooperación internacional

[www.itu.int/cop](http://www.itu.int/cop)



## Objetivos

- Identificar riesgos y vulnerabilidades de la niñez en ciberespacio
- Concienciar
- Desarrollar herramientas prácticas para minimizar riesgos
- Compartir conocimiento y experiencia

# Iniciativa Child Online Protection (COP)

---

En el 2008 la UIT lanzó la iniciativa sobre Child Online Protection (COP) con la GCA cuyo objetivo es juntar y trabajar con todos los sectores de la comunidad global para asegurar una experiencia en línea segura para la niñez.

## Objetivos principales de COP

- Identificar riesgos y vulnerabilidades para la niñez en el ciberespacio;
- Concienciar sobre los riesgos y problemas a través de canales múltiples;
- Desarrollar herramientas prácticas que ayuden a los gobiernos, organizaciones, educadores a reducir los riesgos; y
- Compartir conocimiento y experiencia y facilitar sociedades estratégicas internacionales para definir e implementar iniciativas concretas.



# Uso responsable de las TIC

- Mientras ya existen **muchos esfuerzos** para mejorar child online protection, su alcance ha sido más nacional o regional y menos **global**.
- Para que la seguridad de la niñez sea global, es necesario que sea direccionada en un **marco de trabajo internacional** a través de una **estrategia coherente** que juegue un **rol** importante para los sectores interesados.
- Child online protection **no sólo** significa proteger a la niñez de amenazas potenciales que incluyen explotación de la niñez, abuso y violencia, pero también significa **incentivar** un comportamiento **positivo y responsable**.
- Una **respuesta amplia** a la seguridad de la niñez para su acceso en línea enfatizaría la capacidad de Internet para apoyar el **positivo compromiso de niños** y jóvenes en sus comunidades. Como ciudadanos digitales, niños y jóvenes serían completamente empoderados para contribuir activamente en la vida cívica.



# Guías COP



Desarrollados con la cooperación de COP partners, son las primeras guías que cuentan con diferentes sectores interesados. Disponible en los seis UN idiomas

---

Para la niñez: Las guías aconseja a la niñez sobre posibles actividades perjudiciales existentes en línea como es intimidación, acoso, robo de identidad, abuso, etc. Las guías también ofrecen consejos sobre contenido en línea no apropiado e ilegal o sobre jóvenes expuestos a acoso sexual, la producción, distribución y colección de contenido de abuso de menores.

Para los padres y educadores: las guías proveen recomendaciones sobre qué pueden hacer para que la experiencia de uso de las TIC por los menores sea positiva.

---

Para la industria: una guía para proteger los derechos de los niños en línea para las empresas que desarrollan, proveen o hacen uso de las TICs. Las guías han sido desarrolladas para alinearse con las guías de las Naciones Unidas sobre principios para Negocios y Derechos Humanos, y explican no sólo qué pueden hacer las compañías para proteger la seguridad de la niñez en línea, sino también pueden habilitar el positivo uso de las TIC por los niños.

Las guías también incluyen una lista para sectores específicos que recomiendan acciones para operadores móviles, proveedores de servicios de Internet, radiodifusores de servicios públicos y privados, proveedores de contenido, vendedores online, desarrolladores de aplicaciones, generadores de contenido y fabricantes de dispositivos.



---

Para los reguladores: las guías ayudarán a los países a planificar estrategias para proteger el acceso en línea de la niñez a corto, mediano y largo plazo. Para formular una estrategia nacional enfocada en la seguridad de la niñez en línea, los reguladores necesitan considerar un rango de estrategias que incluyan el establecimiento de un marco legal, desarrollar capacidades de empoderamiento de la ley, disposición de recursos y mecanismos de reporte y proveer recursos para educación y concienciación.

---

# Gracias!

Para más información sobre las actividades de la UIT sobre ciberseguridad: [www.itu.int/cybersecurity/](http://www.itu.int/cybersecurity/)

o Contacte: [cybmail@itu.int](mailto:cybmail@itu.int)



*Committed to connecting the world*