Proyectos de Ciberseguridad en la Región
CIRTs Nacionales

Tercer Foro Regional sobre Interconectividad, Ciberseguridad e IPV6

Panamá, 10 y 11 de Septiembre del 2015

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

La importancia de la Ciberseguridad

- ✓ Mayor espacio para atacar
  - ➢ Aumento de la dependencia de disponibilidad de las TIC
  - ➢ Incremento constante del número de usuarios de Internet (actualmente el 40% de la población mundial)
- ✓ Aumento de crímenes
  - ➢ Se ha estimado un costo global de más de $455 billones
  - ➢ Pérdidas ocasionadas a Sony pictures causó $100 millones en pérdidas
  - ➢ Un aumento en cuatro veces el número de malware en la Banca/Finanzas en la plataforma Android desde 2014Q1 hasta el 2014Q4.

Sources : Symantec (2014)
McAfee (2014)
Trend Micro (2015)

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

Source: Symantec

WSIS y Promoción de una Cultura Global sobre Ciberseguridad

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:

"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 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

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**

Medidas Legales

- **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 enten dimiento del Cibercrimen:
- Una guía para Países en vía s de Desarrollo

Eventos y Capacitación

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

Medidas Técnicas y de Procedimiento

- **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

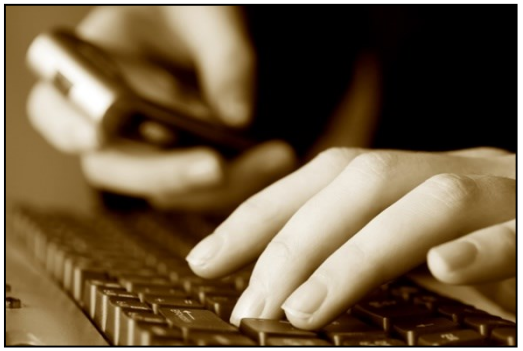
Capacitación/Asistencia

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

Capacitación

- **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

Cooperación Internacional

- **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

Definición de CIRTs Nacional

Un CIRT Nacional es una organización que responde a incidentes de seguridad computacionales o en ciberseguridad y provee servicios necesarios a un sector definido para identificar efectivamente las amenazas, coordinar acciones a nivel Nacional y Regional, diseminar Información y actuar como punto focal para los asuntos de ciberseguridad.

CIRT Nacional

Sectores beneficiados por un CIRT nacional:

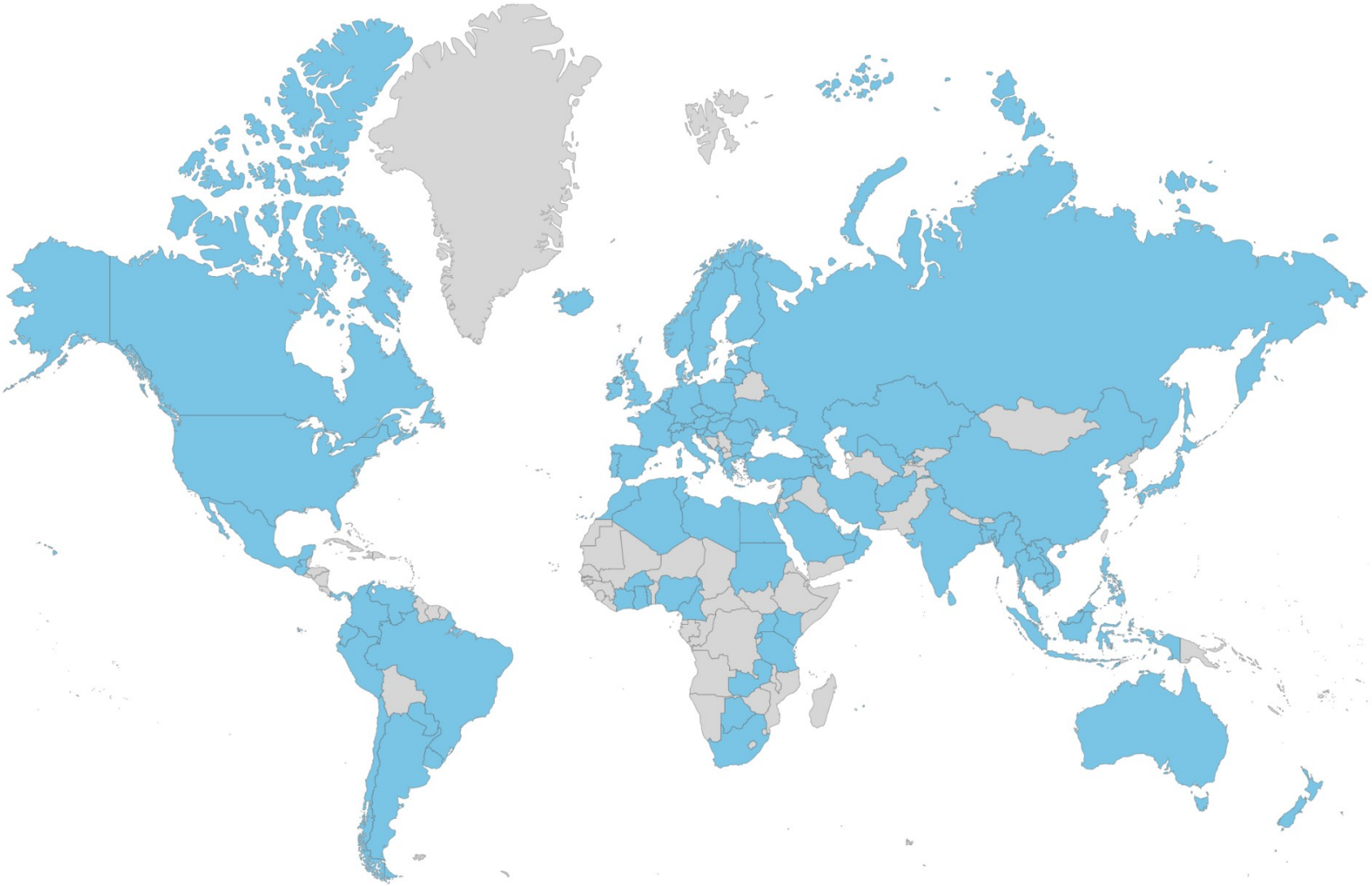
- Organizaciones gubernamentales
- Agencias de reforzamiento de la Ley
- Infraestructuras de Información Crítica
- Academia
- Grupos sectoriales claves

Funciones de un CIRT Nacional

- Punto focal de confianza más allá de las fronteras nacionales;
- Identificar y administrar ciber amenazas que pueden afectar adversamente al país;
- Responder sistemáticamente a incidentes de ciberseguridad y tomar acciones apropiadas;
- Recuperación fácil y eficiente luego de incidentes de ciber seguridad
- Minimizar pérdidas/robo de Información/interrupción de servicio;
- Utilizar la Información adquirida durante el manejo de incidentes para manejo futuro de incidentes;

Funciones de un CIRT Nacional

- Asuntos legales que pueden implicar los incidentes;
- Intercambio de conocimiento con el sector beneficiado;
- Poner a disposición guías y mejores practicas a través de publicaciones, páginas web y otros medios de comunicación;
- Promover o iniciar el desarrollo de la educación, concienciación, y materiales de capacitación apropiados para diversas audiencias;
- Identificar y mantener un listado de CIRTs y puntos de contacto.



102 National CIRT established worlwide.

CIRT Nacional – Necesidades

CIRT Nacional

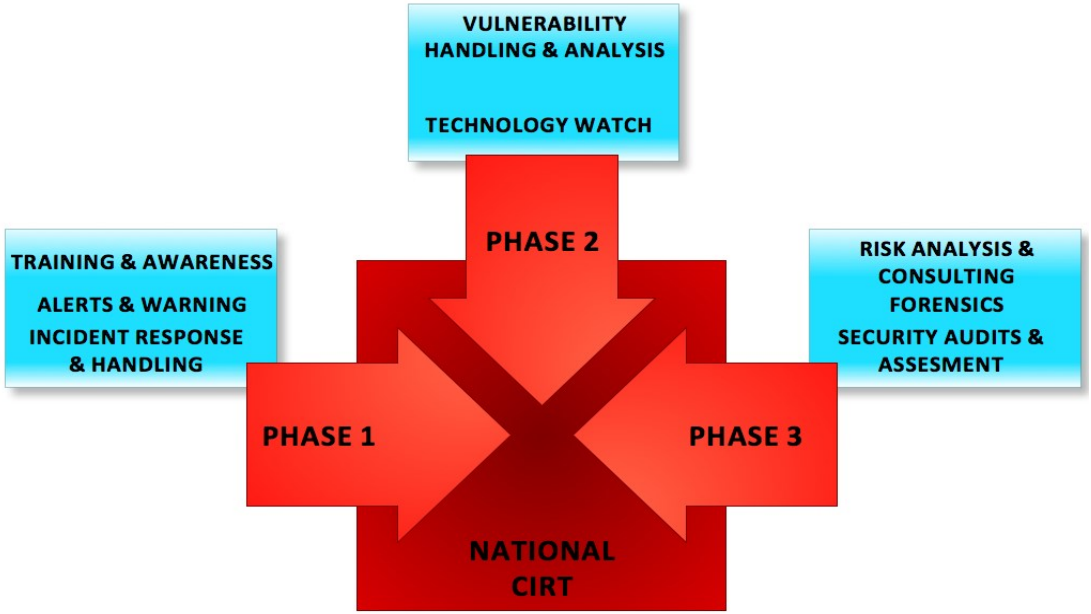
- Asegurar coordinación y cooperación con sectores nacionales y regionales
- Asegurar sostenibilidad en capacidades adquiridas o desarrolladas sobre ciberseguridad, que permitan a la nación construir y extender beneficios a otros sectores públicos y privados

- 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

Fases de Establecimiento de un CIRT

12 Meses

COUNTRY'S CIRT CAPABILITY ROADMAP



6 Meses

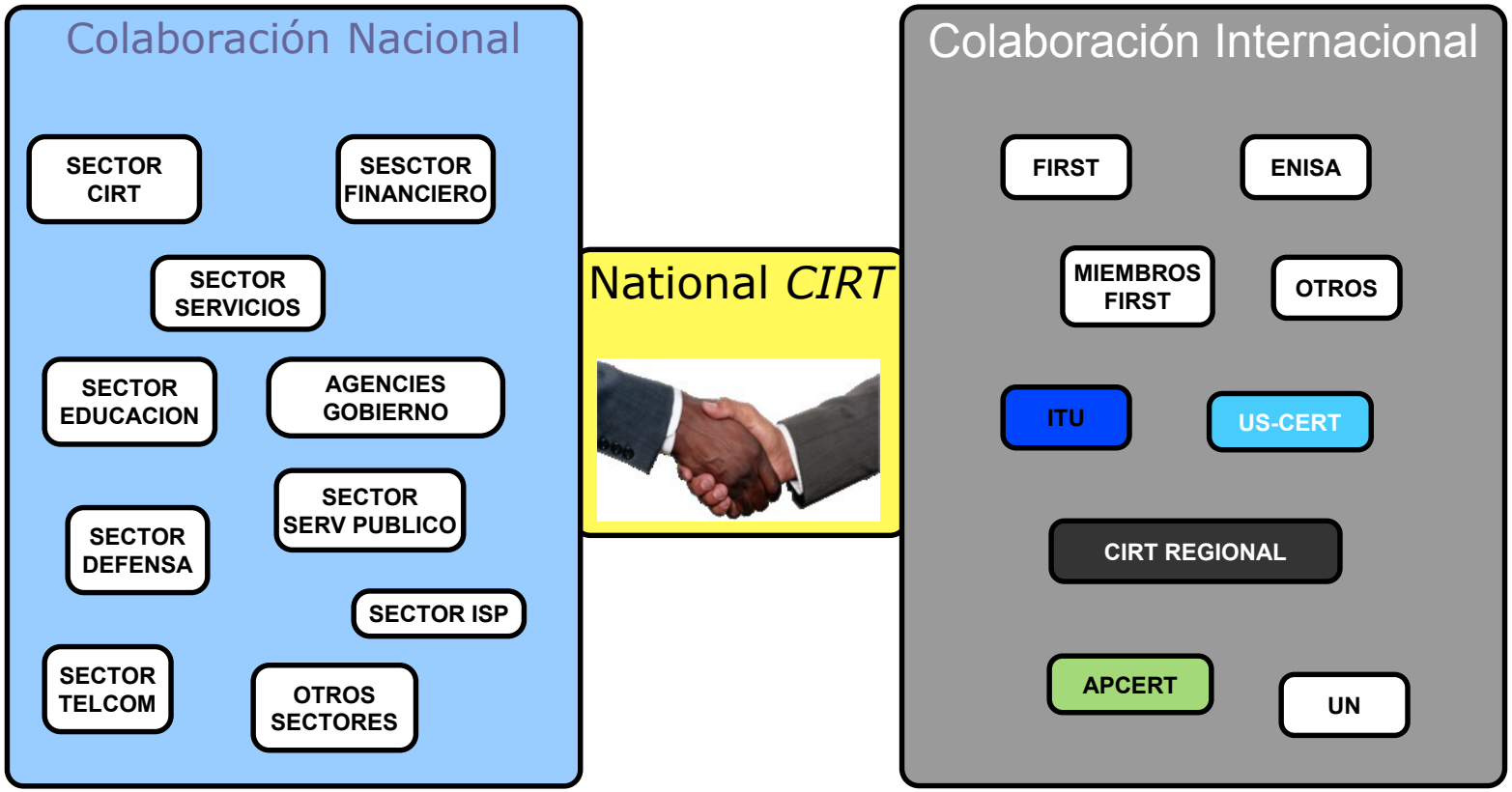
18 - 24 Meses

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

Colaboración



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

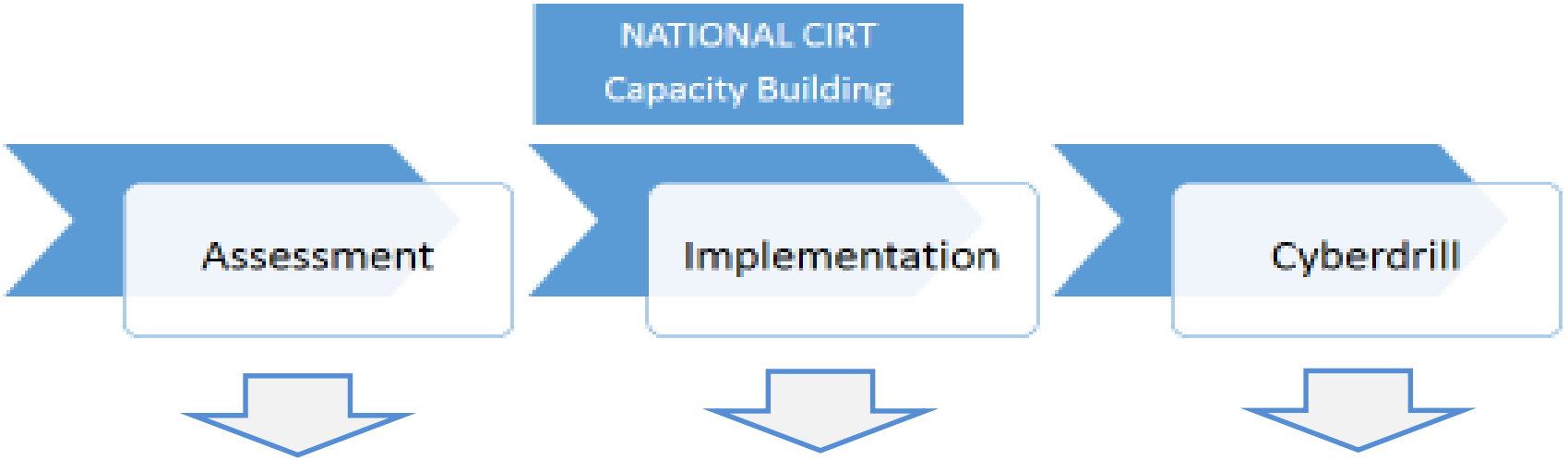
Factores Críticos de Éxito – Establecimiento de CIRT Nacional

- 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

Programa UIT CIRTs Nacionales

- Evaluaciones nacionales conducidas en 65 países
  24 en las Américas
- Implementaciones completadas en 11 países
  2 en las Américas
- Varias implementaciones en progreso
- **12** cyber drills conducidos con más de **100** países participantes
  En América el ultimo fue en Bogotá-Colombia del 3 al 5 de Agosto del 2015

Programa UIT CIRT Nacional



- Evaluar capacidades o necesidades existentes de mecanismos nacionales de ciberseguridad
- Evaluaciones en sitio a través de reuniones, capacitaciones, entrevistas, sesiones y visitas al sitio
- Recomendaciones para un plan de acción (requerimientos institucionales, organizacionales y técnicos)

- Implementar considerando las necesidades identificadas y las estructuras organizacionales del país
- Ayudar con planificación, implementación y operación del CIRT
- Colaboración continua con el CIRT establecido para brindar el apoyo necesario
- Capacitación técnicas y operacionales

- Ejercicios organizados a nivel Regional e Internacional
- Ayudar el mejoramiento de la comunicación y las capacidades de respuesta de los participantes de los CIRTs
- Mejoramiento general de preparación en Ciberseguridad en la Región
- Provee oportunidades de cooperación público-privado

Developing National CIRTs

- Todavía hay mucho que trabajar en la preparación de los CIRTs especialmente en los países en desarrollo
- Los ataques puedes ser lanzados hacia las redes de las naciones menos que generalmente son de los países menos desarrollados
- Esto incrementa la necesidad de trabajar en la preparación de los países menos desarrollados
- Establecimiento de CIRT nacionales su capacitación
- Cooperación regional e Internacional

Proyectos en la Región

- 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

Global Cyberseecurity Index

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

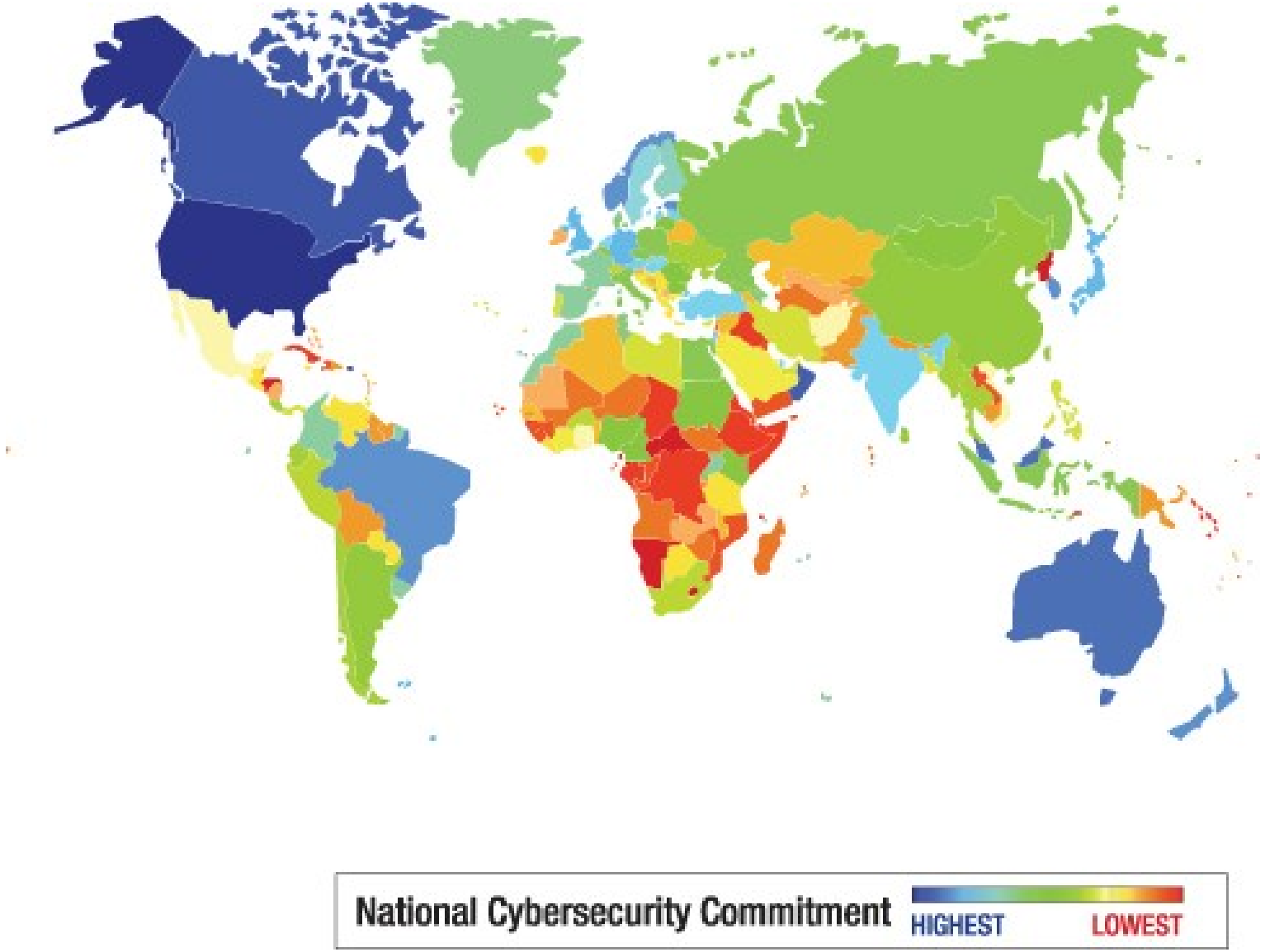
Conducir esfuerzos de implementación entre industrias y sectores

Integrar seguridad en el núcleo del progreso tecnológico

Fomentar una cultura global de ciberseguridad

http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

ABIresearch® | ITU | Global Cybersecurity Index


National Cybersecurity Commitment
HIGHEST
LOWEST

Perfiles País Cyberwellness

Información de logros de ciberseguridad de cada país **basado en los pilares de la GCA**

Se invita a los países para mantener actualizada la Información: cybersecurity@itu.int

EJEMPLO →

CYBERWELLNESS PROFILE
PANAMA

BACKGROUND

Total Population: 3 625 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 42.90%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

-Penal Code

-Law on Electronic Signature

1.1.2 REGULATION AND COMPLIANCE

Panama does not have specific regulations and compliance requirements pertaining to cybersecurity.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Panama has established an officially recognized National CIRT.

1.2.2 STANDARDS

Panama has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the National Cybersecurity Strategy.

1.2.3 CERTIFICATION

Panama does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Panama has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

Panama is currently developing the national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The National Innovation Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Panama does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

ITU-T

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

ITU-R

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

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

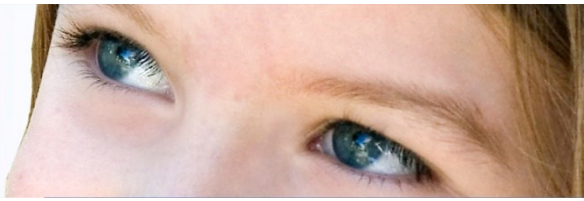
- Utiliza el trabajo de la UIT (SG17, Q22, etc) y el modelo GCA apoyando el desarrollo de las estrategias nacionales de Ciberseguridad

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…

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

Objectivos

- 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 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/

o Contacte: cybmail@itu.int