CITEL: Promoviendo cooperación en ciberseguridad y protección de la infraestructura crítica

Graciela Piedras
Especialista Senior de Telecomunicaciones

Comisión Interamericana de Telecomunicaciones (CITEL)

"Foro Regional de la UIT para las Américas sobre Ciberseguridad"

Santo Domingo, República Dominicana,
23 al 25 de noviembre de 2009

Organización de los Estados Americanos

Agenda

1 **Situación actual**

2 **Actividades principales de la CITEL en ciberseguridad:**

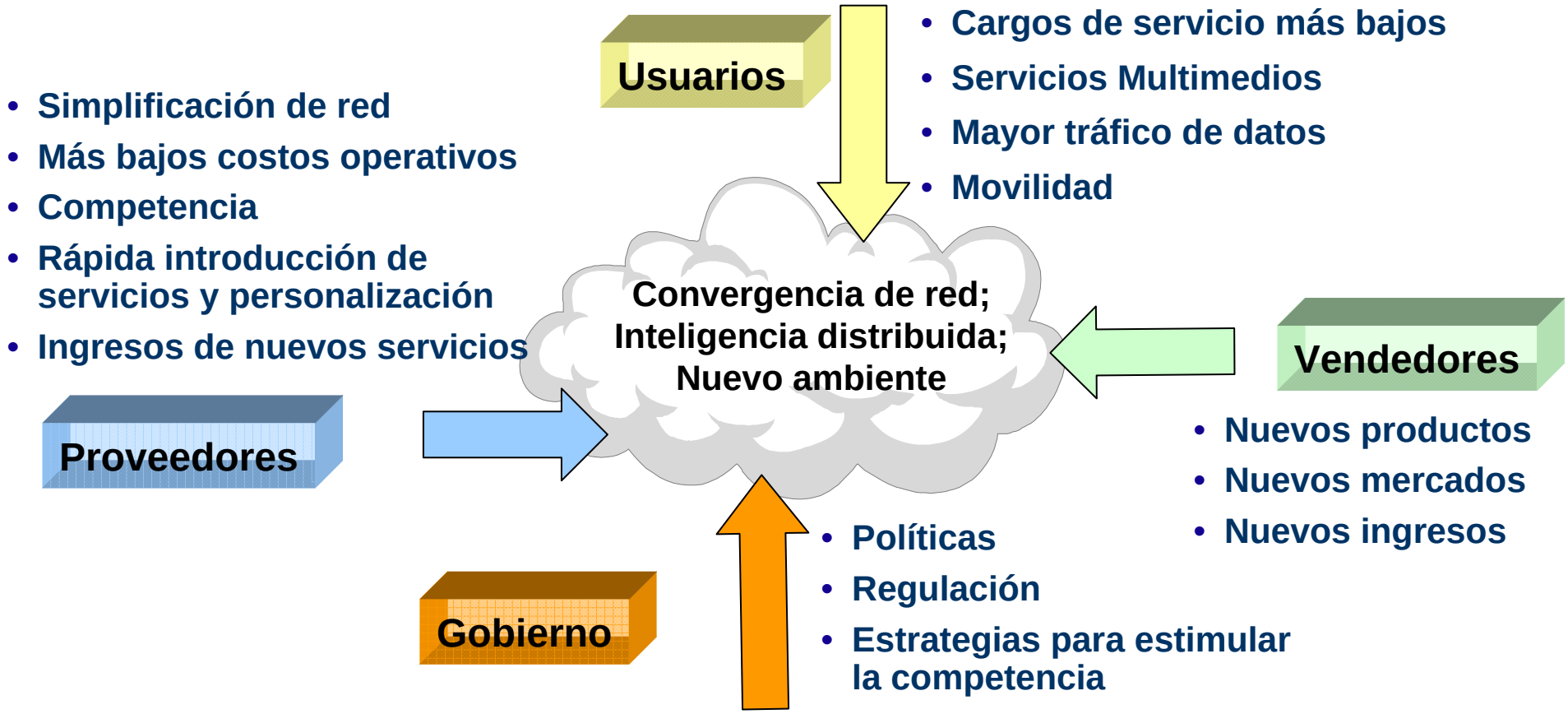
- Coordinación
- Políticas y regulación
- Aspectos de tecnologías
- Compartición de la información

3 **Acciones de futuro**

La sociedad moderna depende la infraestructura de comunicaciones

Fuente: Document CITEL-0344/06

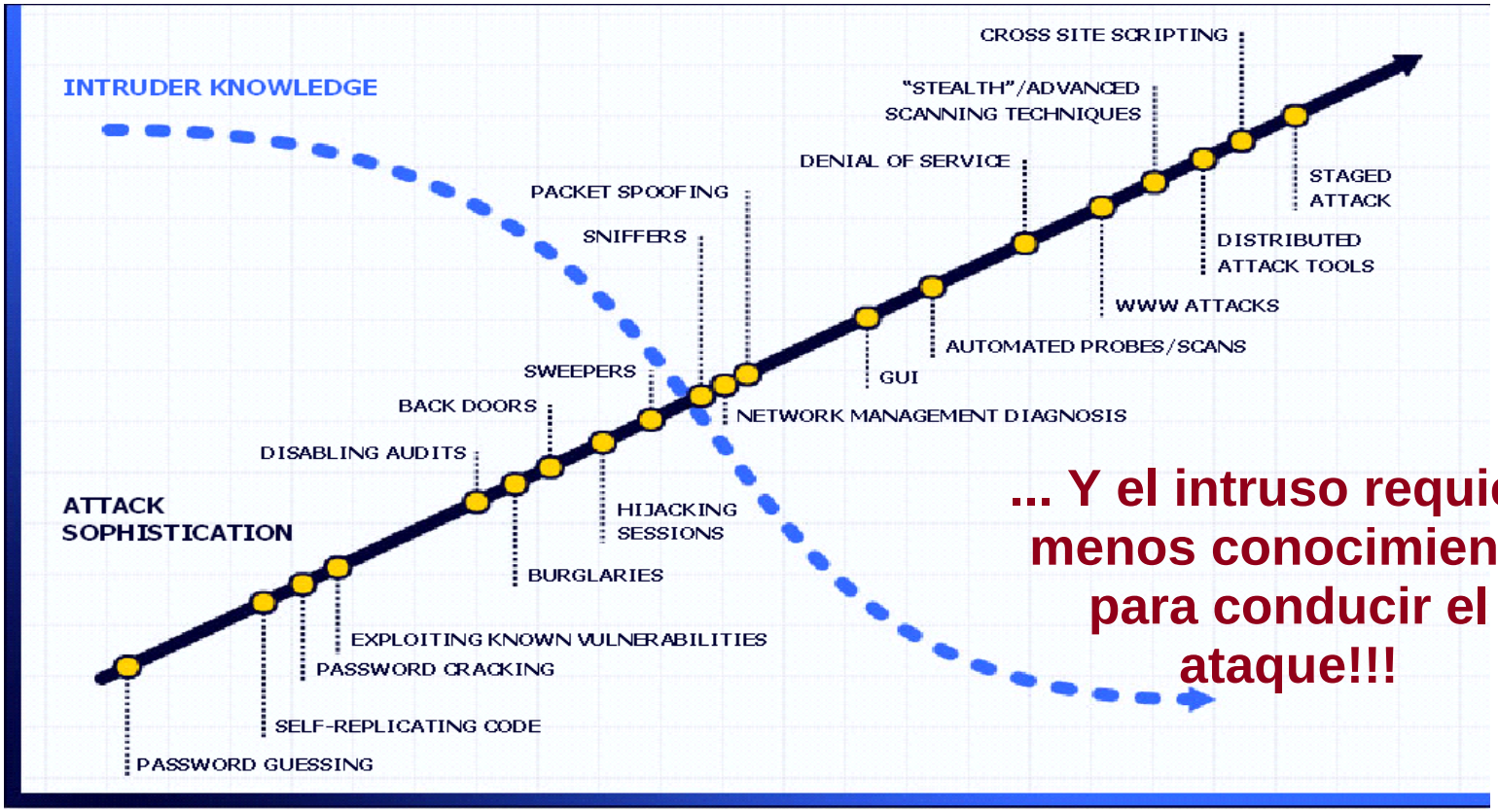
Elementos que afectan el cambio de la red



Las redes de comunicaciones están teniendo muchos cambios para satisfacer las demandas del mercado

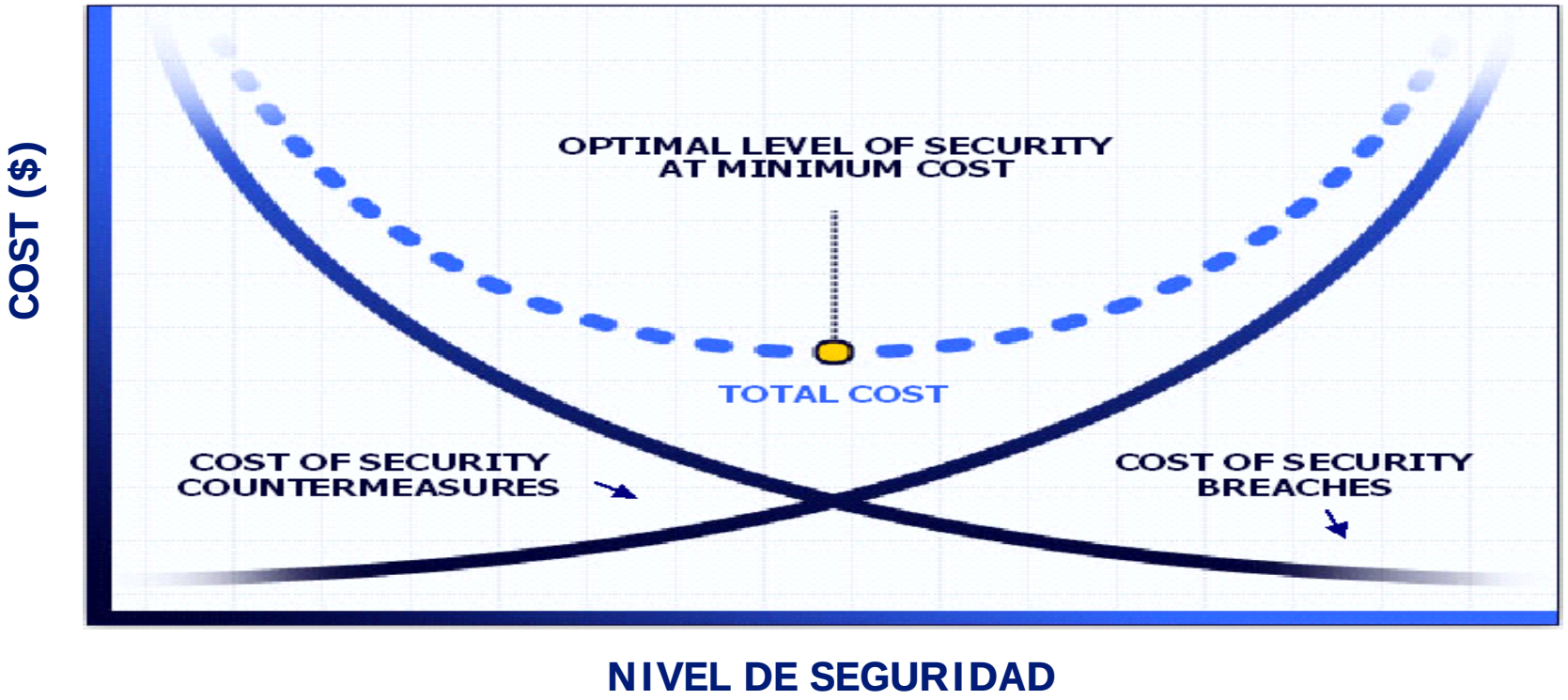
Fuente: CCP.I

Sofisticación de los ataques está en crecimiento…



Fuente: CERT/CC, *CERT/CC Overview - Incident and Vulnerability Trends*

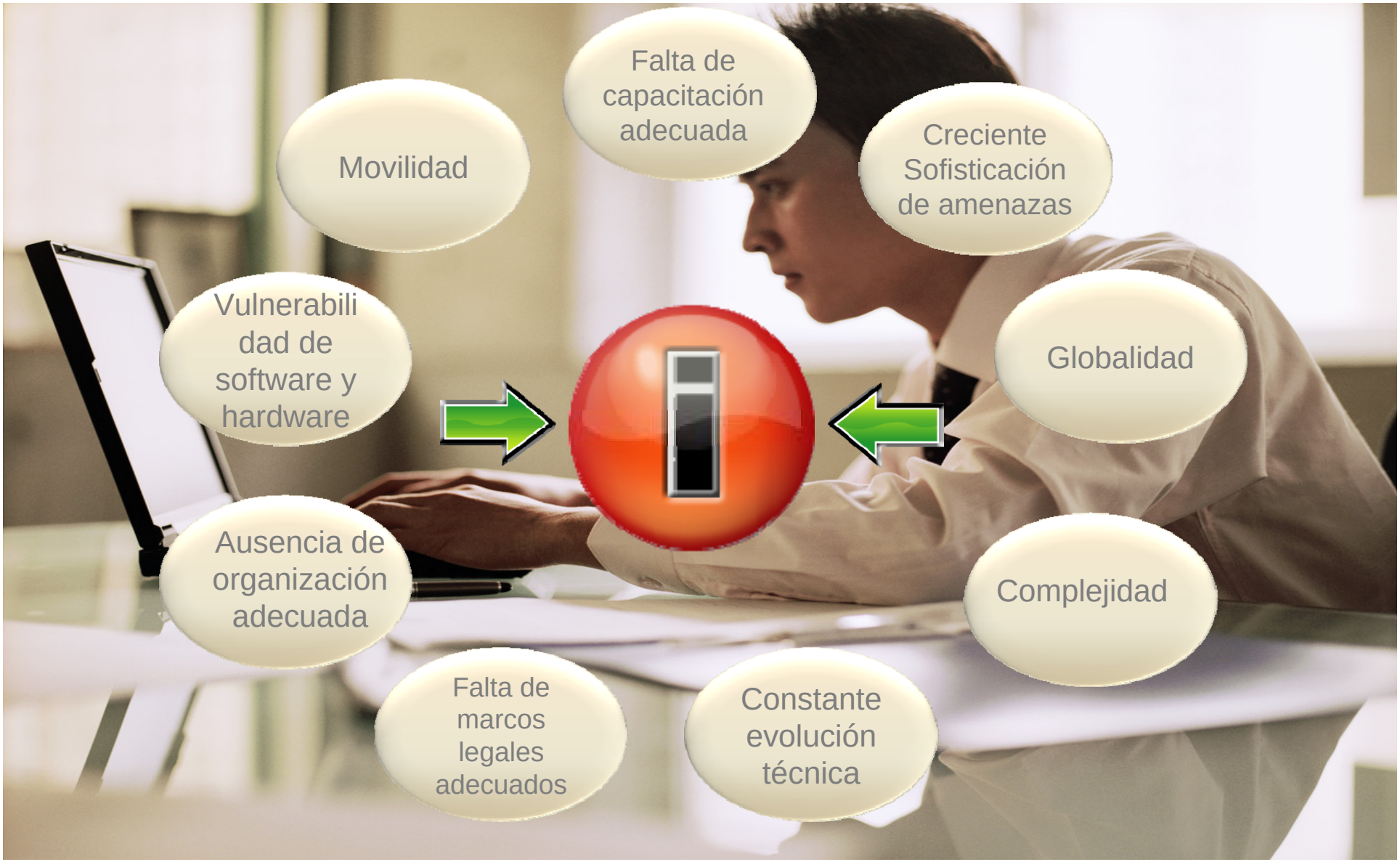
La cantidad de presupuesto es limitada



La protección debe tener sentido a nivel del negocio

Cuáles son los desafíos de la SI?

Organización de los Estados Americanos



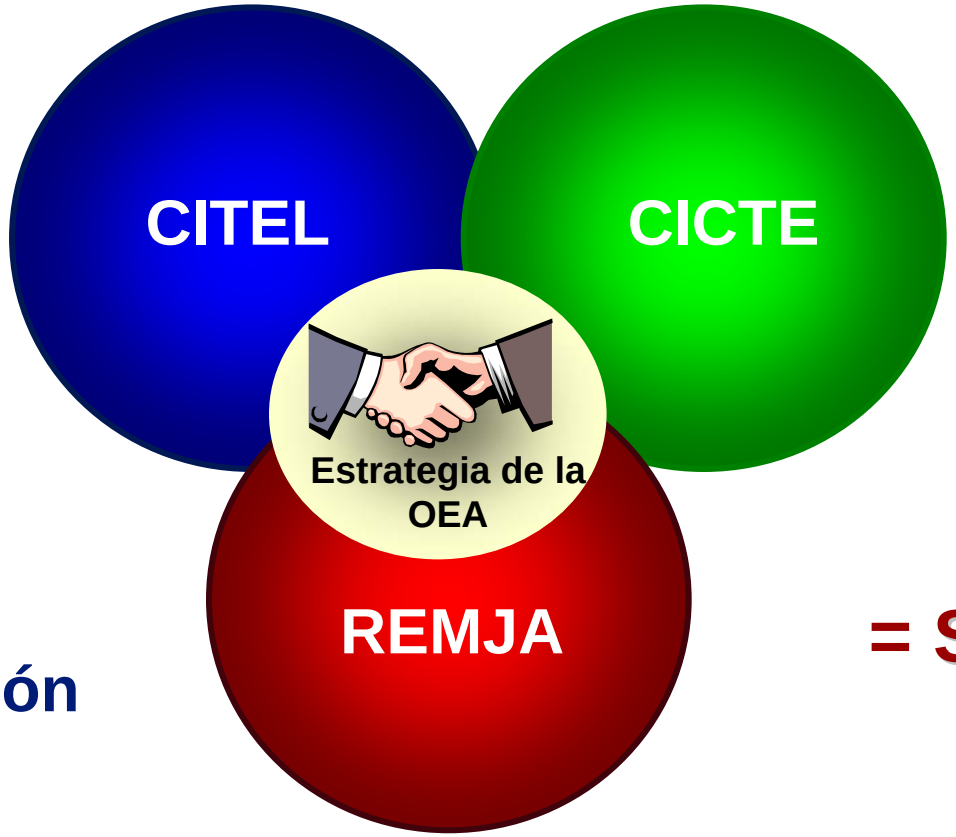
Fuente gráfico: M. Rohr

Organización de los Estados Americanos

Para sobrevivir los desafíos

Compartición de Información

+



Construir confianza

+

Crear Colaboración

+

= Sinergias

+

Exitos

"AG/RES. 2004 (XXXIV-O/04)
ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA"

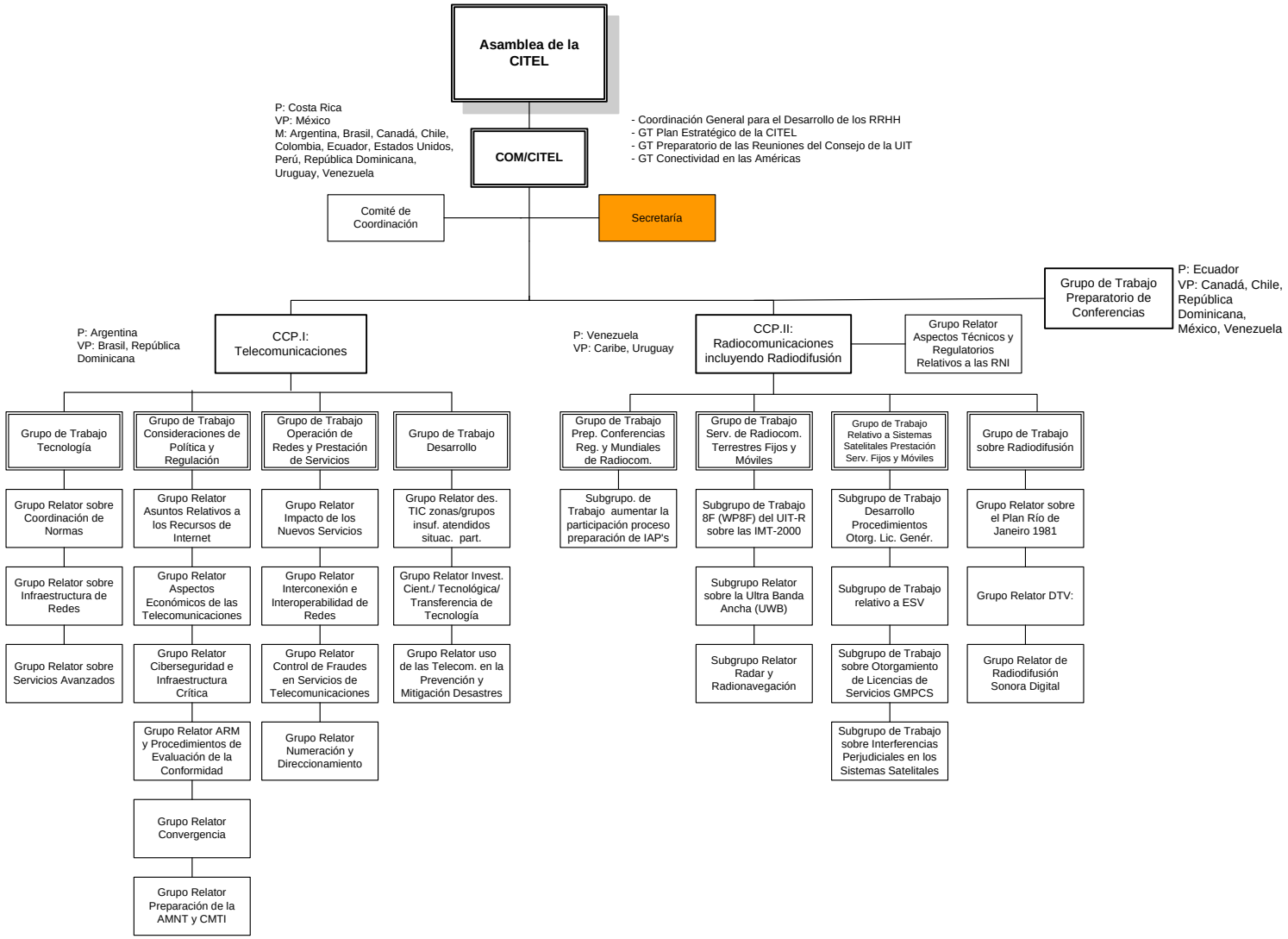
La CITEL

- Organismo asesor de la OEA, especializado en telecomunicaciones

- Enfoque de trabajo de la CITEL destaca:
  - Colaboración/coordinación con organismos regionales/internacionales de telecomunicaciones e instituciones de crédito y desarrollo.
  - Capacitación en telecomunicaciones de funcionarios de gobierno y de ejecutivos del sector privado.
  - Fomento del logro de posiciones comunes.
  - Determinación de las prioridades en la región en telecomunicaciones.

Organización de los Estados Americanos

Estructura de la CITEL



Qué hace la CITEL?

Organización de los Estados Americanos

Guías y mejores prácticas
Procedimientos
Enfoques nacionales
y regionales

Gobierno

Capacitación
Talleres y Seminarios

Políticas y regulaciones

Compartición de Información

Sociedad civil

Organismos

CITEL

Coordinación

Regional e internacional

Tecnologías e implementación

Carpetas técnicas
Coordinación de normas
Desarrollo de servicios
Evaluación de la conformidad

Sector privado

Fuente gráfico: D. Leguit

Perspectiva de la CITEL

Protección de la Infraestructura crítica

•Energía y utilidades (elétrica, gas y sistemas de trans petró

Prevención y Preparación

de radiodifusión)

•Transporte

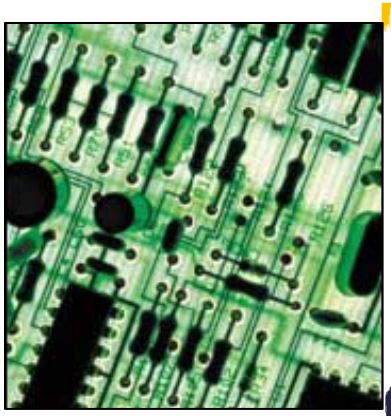
Recuperación y adaptabilidad

(seguridad nuclear, búsqueda y rescate y de emergencia)

Incremento de confianza

•Servicios (incluye financieros, distribución de comidas y de salud)

Ciberseguridad



Objetivos estratégicos

Fuente gráfico: Ministerio del Interior e Industry Canada

Coordinación a nivel nacional e internacional

- **A nivel Nacional la CITEL promueve:**
  - Gobierno y la industria desarrolle un plan conjunto para proteger la infraestructura en el sector de telecomunicaciones
  - Desarrollo de guías para mejorar el conocimiento de las tecnologías avanzadas
  - Fomento de la participación de todos los proveedores de servicio y los operadores y vendedores
  - Creación de un ambiente de confianza para la promoción de enlaces y de intercambio de información
  - Incrementar la concientización en los institutos nacionales de normas y los foros industriales de las normas de seguridad.

- **A nivel Internacional la CITEL promueve:**
  - La no duplicación de esfuerzos y el trabajo conjunto con los organismos internacionales
  - El desarrollo y la promoción de soluciones para:
    - Reducir las vulnerabilidades de protocolos y su mejor diseño
    - Optimizar las redes, su gestión y mantenimiento
    - Mejorar la administración de Internet

Políticas y regulaciones

Necesidades del gobierno:

- Crear conciencia sobre la importancia de la seguridad en todos los sectores del Estado
- Confianza que se tienen suficientes medidas y prácticas para proteger las redes públicas
- Suficiente información para permitir la respuesta en situaciones de emergencia

Necesidades de la industria:

- Seguridad de servicios
- Satisfacción del cliente
- Confianza del inversor
- Rentabilidad

Necesidades del usuario:

- Confianza en los medios de comunicación
- Seguridad y privacidad de su información
- Costos asequibles
- Conectividad adecuada siempre

Carpeta técnica sobre "Ciberseguridad"

Objetivos:

- Provee una compilación sobre información disponible sobre ciberseguridad
- Destaca las actividades estratégicas que se están realizando en la región
- Considera aspectos relevantes para desarrollar estrategias a nivel nacional
- Considera cuestiones de spam, respuesta a incidentes, asociaciones público-privadas y la concientización y aplicación de normas de seguridad relevantes
- Incluye apéndices con experiencias nacionales

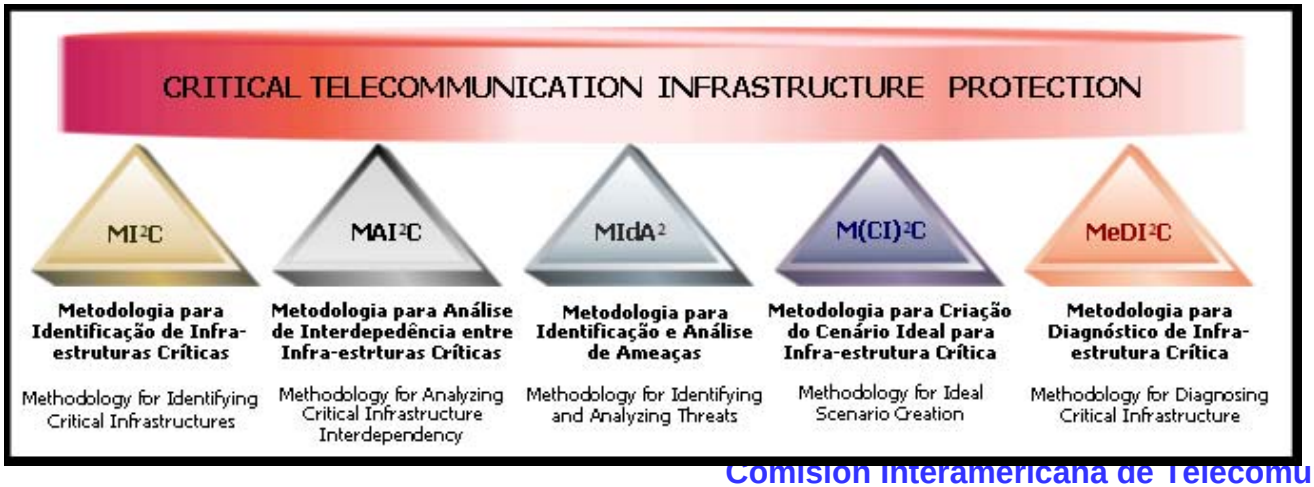
Ejemplos de actividades para establecer una estrategia nacional :

- Llevar a cabo discusiones a nivel de políticas con personas con poder de decisión con respecto a las amenazas y vulnerabilidades.
- Identificar la institución líder para un esfuerzo nacional; determinar la conformación y los requerimientos gubernamentales para la instalación y puesta en operación de un equipo de respuesta.
- Identificar los participantes interesados y puntos de contacto en los ministerios, el gobierno a nivel estatal y local, y el sector privado.
- Identificar roles, responsabilidades y mecanismos de cooperación para y entre todos los participantes.
- Sumarse a los esfuerzos de información internacional para abordar temas de seguridad.
- Evaluar en forma periódica la condición actual de la seguridad cibernética y la IC.
- Identificar los requerimientos de entrenamiento y la necesidad de intercambios técnicos.

Carpeta técnica sobre "Protección de la infraestructura crítica"

- ¿Cuáles son las IC que deben protegerse?
- ¿Cuáles son los componentes de una IC en particular?
- ¿Cuáles son las amenazas frente a las cuales se debe proteger la IC?
- ¿Cuáles son las repercusiones (sociales, económicas y/o políticas de los incidentes (naturales, accidentales o maliciosos) en una IC?
- ¿Cómo se priorizan las inversiones para proteger la IC de modo eficiente?
- ¿Cómo deberá realizarse el proceso de recuperación de una IC después de un incidente?

Ejemplo: Modelo de CIP de Brasil



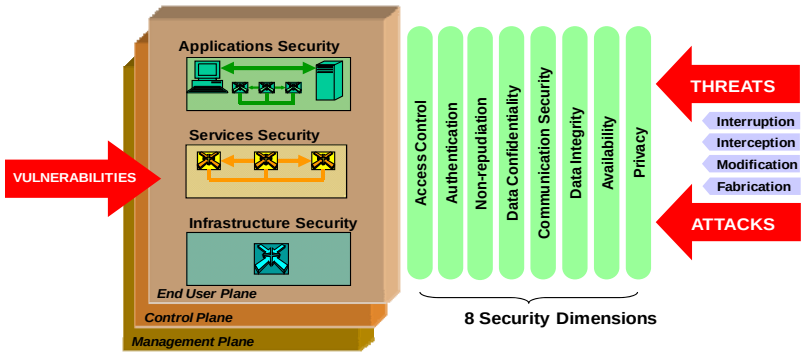
Tecnología e implementación

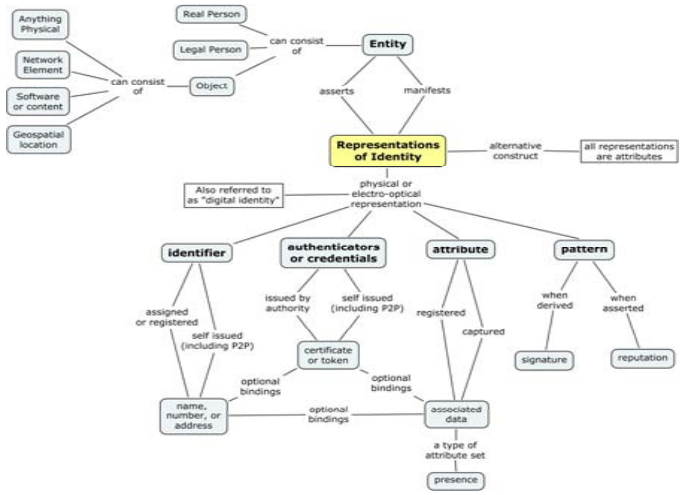
Identificación de tópicos de normas de seguridad:

- Marco de seguridad, privacidad, prevención de fraude
- Definición de servicios y arquitectura de Multimedia
- Requisitos y protocolos de señalización (redes convergentes)
- Servicios basados en IP (Voz sobre IP, Video sobre IP, etc.)
- Servicios de Emergencia
- Interconexión entre redes de telecomunicaciones tradicionales y redes en evolución
- Redes de transporte ópticos Metropolitanos y de larga distancia
- Red de acceso transporte (LANs, LANs Inalámbricas, xDSL, Ethernet, cable modem, fibra, etc.)
- Terminales (PC, TV, PDA, teléfono, etc.)
- Gestión de servicios de comunicaciones, redes y equipos
- Aspectos de redes IMT y posteriores (Internet inalámbricos, armonización y convergencia, control de red, movilidad, roaming, etc.)
- Numeración, Direccionamiento (ENUM)
- Performance y QoS
- Gestión de la identidad

Carpeta técnica «Redes de Próxima generación»

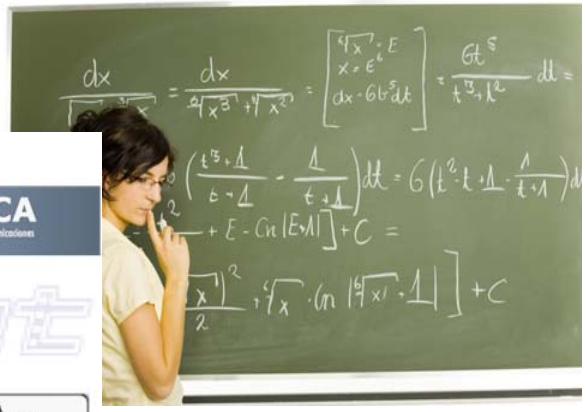
- Provee información técnica de NGN, incluyendo aspectos seguridad que está disponible para los Estados miembros y la industria.
- Documenta las normas de NGN completadas o en desarrollo que pueden ser consideradas para desarrollos futuros.
- En relación a seguridad se han identificado:
  - Protocolo de seguridad de Internet (IPsec)
    - Sucesión de protocolos de seguridad del IETF (RFC 2401) que protegen las comunicaciones de la Internet por cifrado, autenticación y confidencialidad.
  - Arquitectura de seguridad UIT-T (Rec. X.805)
  - Gestión de encripción





Compartición de información

Capacitación en telecomunicaciones



Centros Regionales de Capacitación

COMTELCA
Comisión Técnica Regional de Telecomunicaciones

UNIVERSIDAD NACIONAL DE INGENIERIA
INICTEL - UNI

cenet

Universidade de Brasília

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO
La primera opción y el mejor ejemplo

ANTEL
TELECOMUNICACIONES

Unión Internacional de Telecomunicaciones

Universidad Católica

ITBA 50 MEDIO SIGLO
TECNOLÓGICO DE BUENOS AIRES
UNIVERSIDAD PRIVADA

CCAT
CENTRO DE CAPACITACION EN ALTA TECNOLOGIA

United States Telecommunications Training Institute

ITLA

UNIVERSIDAD TECNOLOGICA DE CHILE
nacap

ACIEM

CITEC CENTRO DE INNOVACIÓN TECNOLÓGICA

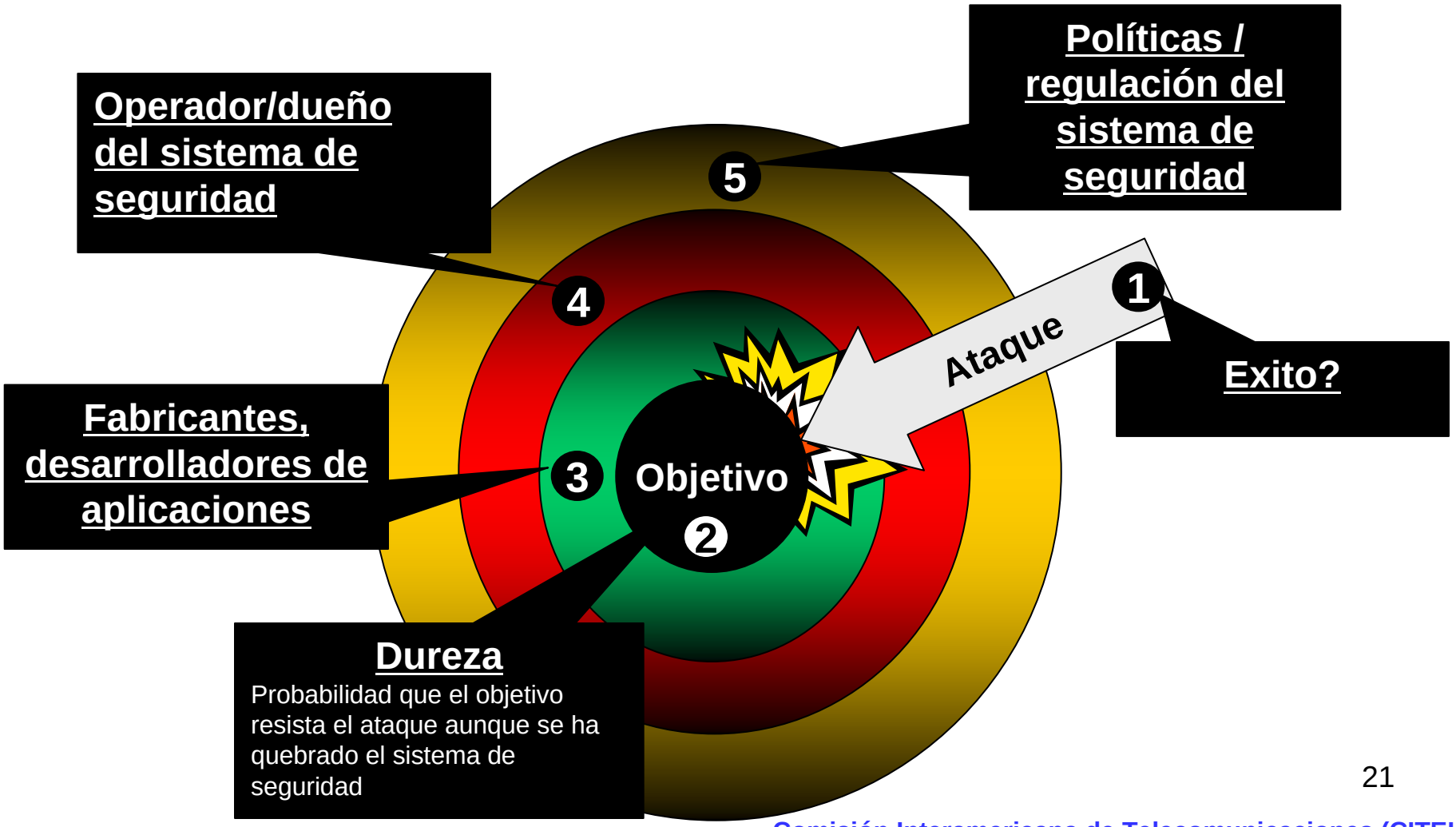
TELESUR

Acciones

Organización de los Estados Americanos

- Incrementar la sinergia entre todas las partes interesadas: entes de vigilancia y control, entes de políticas y regulación, las empresas y los usuarios
- Impulsar el desarrollo de normas compatibles a nivel global
- Concientizar sobre las vulnerabilidades para proveer protección en forma independiente de las amenazas que están constantemente cambiando y pueden ser desconocidas
- Fomentar que la investigación y el desarrollo a través de la academia
- Colaborar con la industria en el análisis de resultados y en la identificación de soluciones
- Incentivar la necesidad de conocer los requisitos de los usuarios y de proveer información detallada a los mismos en relación con el uso seguro de equipos y servicios
- Capacitación en temas prioritarios
- Fomentar la consistencia a nivel internacional en la clasificación de datos para mejorar el flujo de información
- Estimular el desarrollo de regulación adecuada
- Promover la mayor seguridad a la infraestructura interna y externa por parte de los operadores.
- Continuar con la difusión sobre cuestiones de ciberseguridad y la evaluación de mejores prácticas para el establecimiento de estrategias nacionales
- Analizar modelos para la recuperación y la adaptación de las IC
- Continuar con la Cooperación regional e internacional. Es crítica!

Seguridad en capas



Trabajo conjunto de todas las partes

Fuente gráfico Douwe Leguit

Organización de los Estados Americanos

Muchas gracias por su atención

Graciela Piedras

Especialista Senior de Telecomunicaciones

CITEL

E-mail: **gpiedras@oas.org**