UNION INTERNACIONAL DE TELECOMUNICACIONES

CHILD ONLINE PROTECTION

Pablo Palacios

Programme Officer Area Office Chile

Sobre la UIT

La UIT es la agencia especializada de Naciones Unidas para las Tecnologías de la Información y Comunicación (TICs)

Fundada en París en 1865 como la Unión Internacional de Telegrafía

Más de 150 años de experiencia e innovación

Los tres sectores de la UIT

Qué hacemos

‘Comprometidos en conectar el Mundo’

3 Sectores

UIT Radiocomunicaciones

Coordina el espectro de radio-frecuencia y la asignación de espacios de orbitas satelitales

UIT Normalización

Establece **normas** globales

UIT Desarrollo

Reducción de la brecha digital

Miembros UIT

193

MEMBER STATES

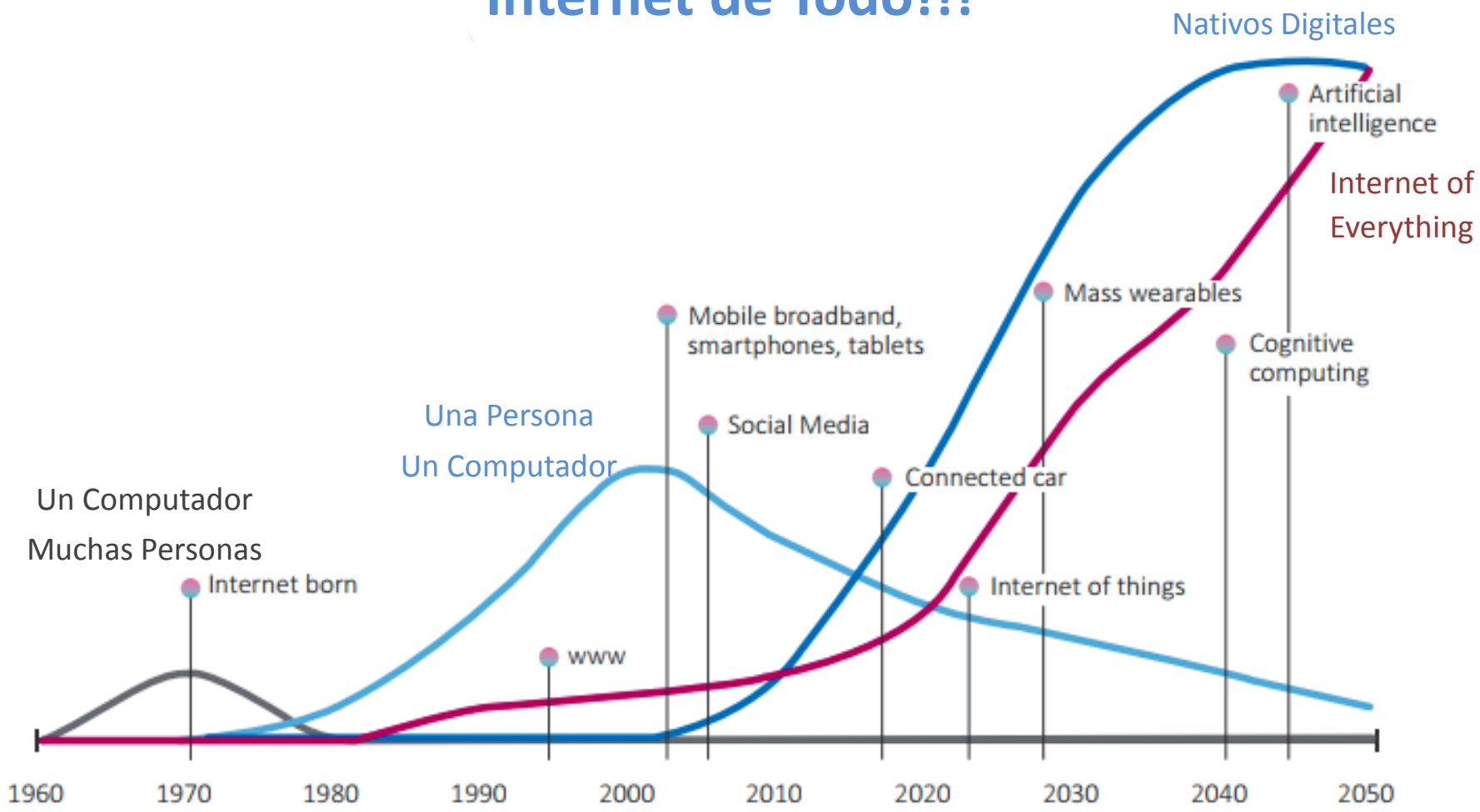
+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

+150

ACADEMIA MEMBERS

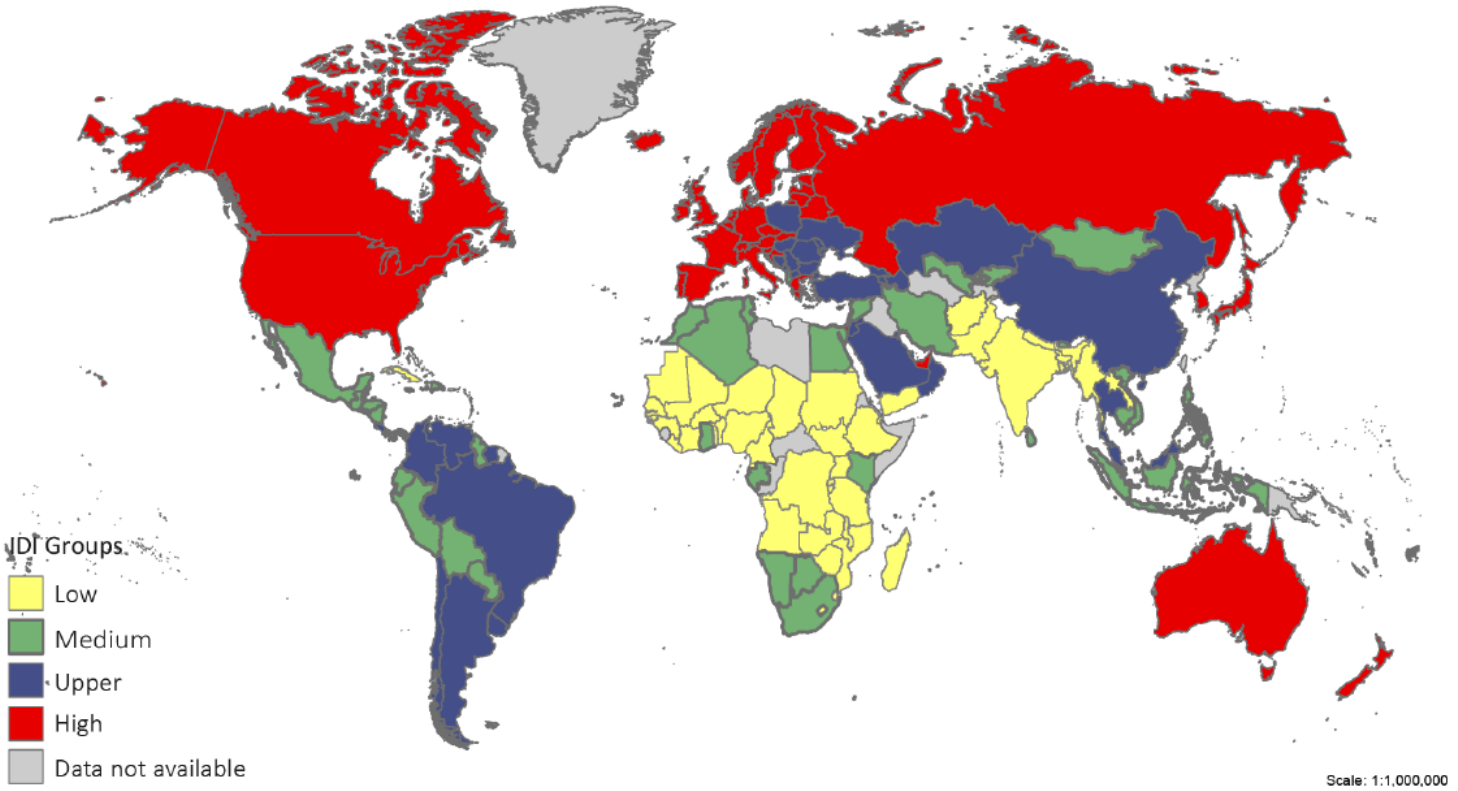
Internet de Todo!!!



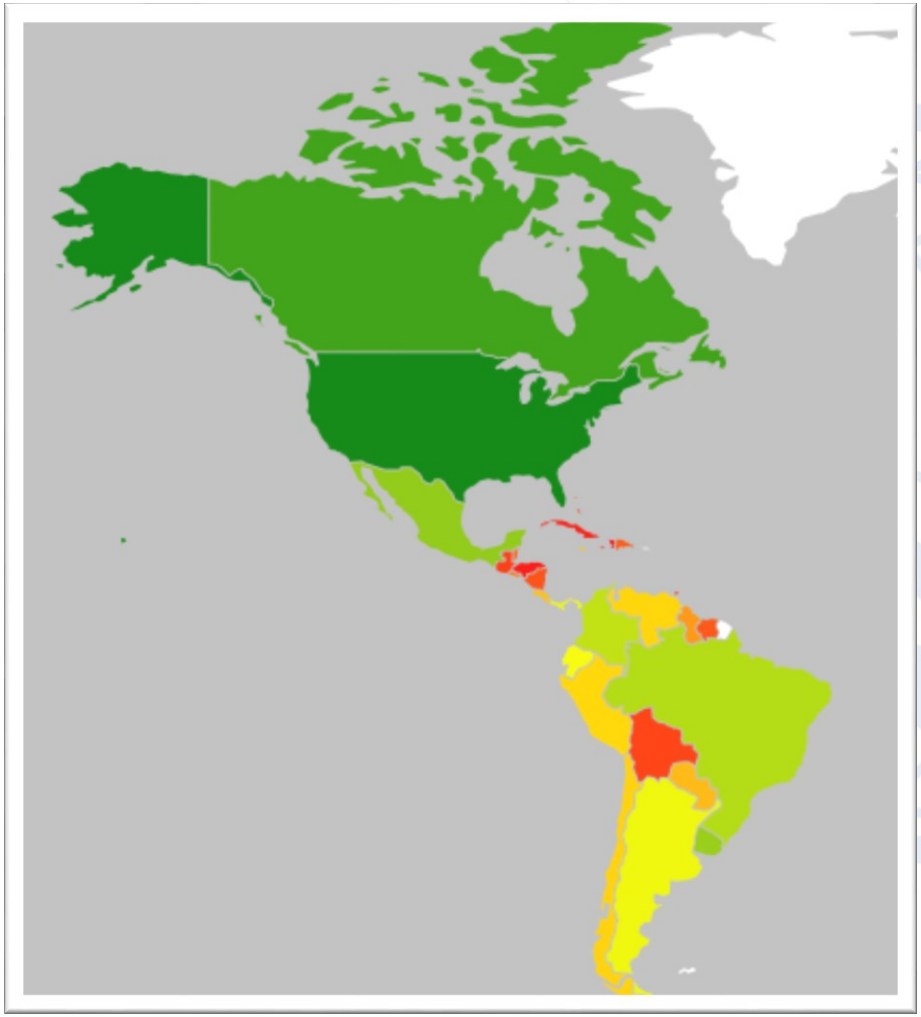
ITU: Trends in Telecommunication Reform 2015, Getting Ready for the Digital Economy

Cómo estamos?
IDI – ICT Índice de Desarrollo

Geographical distribution of IDI quartiles, 2016



Compromisos Nacionales en Ciberseguridad



Member State	Score	Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81
Jamaica	0.339	85
Costa Rica	0.336	86
Paraguay	0.326	87
Barbados	0.273	95
Guyana	0.269	98
El Salvador	0.208	108
Saint Vincent and the Grenadines	0.189	114
Belize	0.182	116
Antigua and Barbuda	0.179	117
Dominican Republic	0.162	122
Suriname	0.155	132
Nicaragua	0.146	125
Bahamas	0.137	129
Bolivia	0.122	134
Grenada	0.115	137
Guatemala	0.114	138
Trinidad and Tobago	0.098	141
Saint Kitts and Nevis	0.066	151
Cuba	0.058	153
Saint Lucia	0.053	156
Honduras	0.048	157
Haiti	0.040	161
Dominica	0.010	163

Las Amenazas son más Inteligentes

"Detalles de la motivación, intenciones y capacidades de actores internos y externos. Amenazas inteligentes incluye tácticas específicas, técnicas y procedimientos. El propósito primario de las Amenazas Inteligentes es informar a los negocios sobre los riesgos y las implicaciones asociadas con las amenazas." *

- **Oportuno:** Necesita tiempo para realizar las acciones;
- **Exacto:** Número de alertas o acciones falsos positivos;
- **Relevante:** Cómo es organizado y entregado para asegurar su afectación;
- **A Medida:** Debe ser provisto a diferentes personas para hacer que sus decisiones sean relevantes para su rol.**

Hay mucho trabajo por hacer en Infraestructura y Ciberseguridad en la Región

* Forrester / ** Silensec

Qué es Ciberseguridad?

Herramientas

Guías

Certeza

Políticas

Tecnologías

Entrenamiento

Mejores Prácticas

Manejo de Riesgos

Conceptos Seguridad

Salvaguardias Seguridad

Proteger el Ciber Ambiente

Organización / Activos de Usuarios / Dispositivos / Personal / Infraestructura / Aplicaciones / Servicios / Sistemas de Telecomunicaciones

La totalidad de información transmitida y/o almacenada en el ciber ambiente

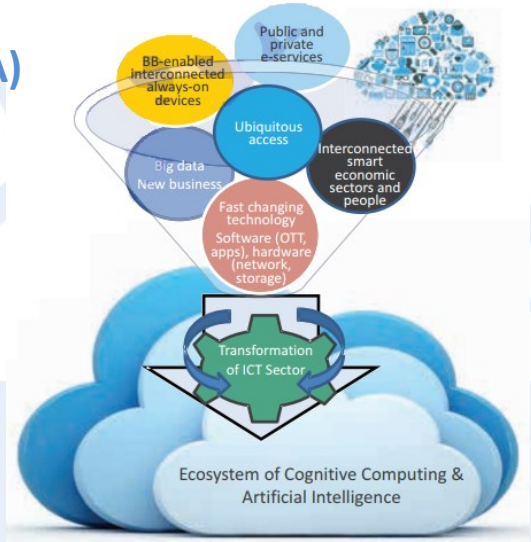
Objetivos de Ciberseguridad

Confidencialidad Disponibilidad Integridad: Autenticidad y No Repudiación

Ecosistema Digital – Hacia todo Interconectado

Digital Object Architecture (DOA)
ITU - Y.IoT-Interop

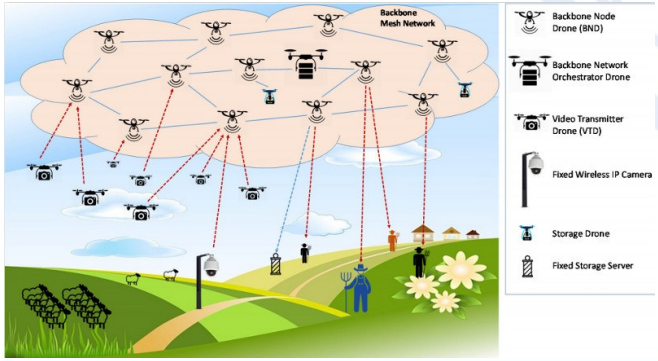
- Seguridad e Interoperabilidad entre aplicaciones IoT;
- Permite que la información sea identificada y encontrada sin importar su localización o almacenamiento.



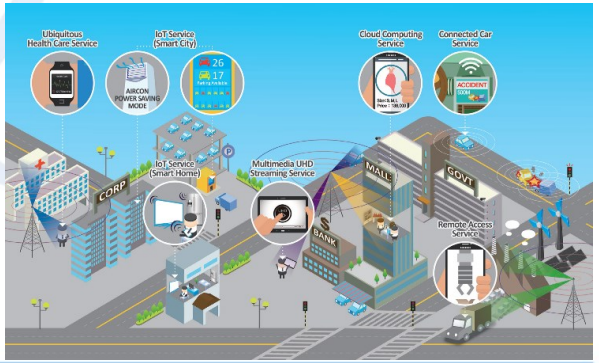
Redes 5G / Ciudades inteligentes
Cloud Computing / Big Data

Incremento del Acceso a Banda Ancha
Cualquier parte del Mundo

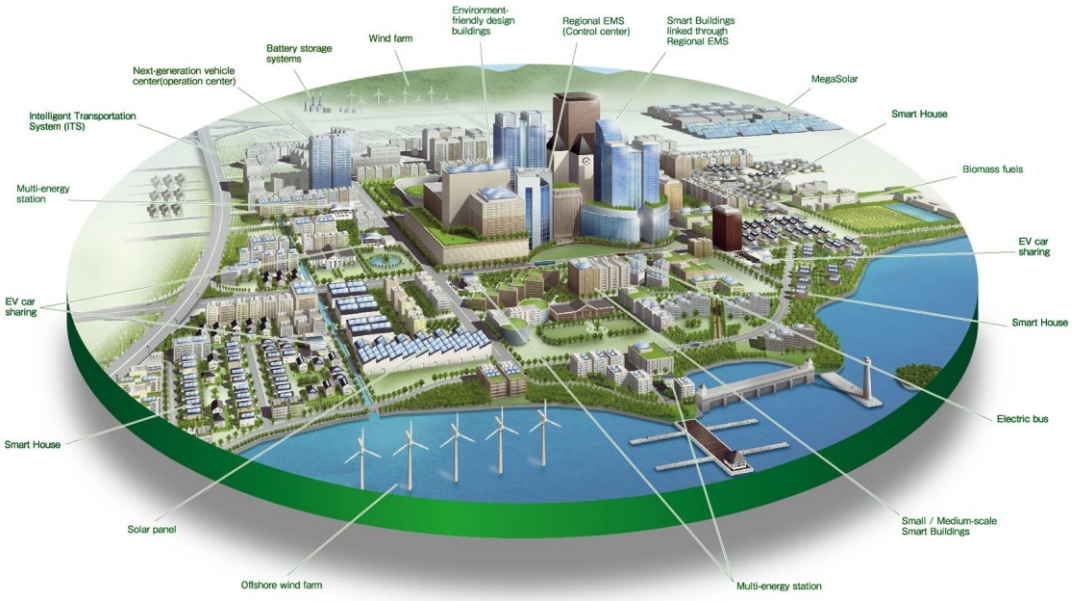
e-health / e-learning / e-government / e-commerce / e-banking / e-money / Entertainment / Media / Redes Sociales / Comunicaciones en Emergencias / GPS / Agricultura / Accesibilidad



Inteligencia Artificial / Robótica
Autos Autónomos
Casas y Ciudades Inteligentes



Infraestructura Interconectada en Ciudades Inteligentes



Low Power Wide Area (LPWA) para completar vacíos de conectividad

Desarrollo de Aplicaciones sostenibles comerciales

La industria debe proveer plataformas IoT para intercambio de datos con protección de la información

Lograr la visión de ciudades inteligentes totalmente integradas

Todo Interconectado / eficiencia y sostenibilidad / análisis en tiempo real / decisiones efectivas / manejo inteligente de recursos

Híper complejidad | Híper conectividad | Híper volumen de Datos = Híper vulnerabilidad

Cada nueva Conexión abre una puerta para Ciber ataques

ITU Magazine No2 2016 Building Smart and Sustainable Cities for tomorrow

Inteligencia Artificial

Inteligencia Artificial (AI) en términos generales significa la capacidad de una unidad funcional de simular inteligentes habilidades humanas como razonamiento y aprendizaje. Sus fundamentos incluye matemáticas, lógica, filosofía, lingüística, neurociencia y teoría de decisiones. Muchos campos caen dentro de AI como robótica, visión, aprendizaje de máquinas, procesamiento de lenguaje natural.

Un algoritmo de aprendizaje de máquina habilita para identificar patrones en datos analizados, construir modelos para explicar el mundo y predecir cosas sin tener reglas y modelos pre programados.

SG13-TD187/GEN: Maini, Vishal. Sabri, Samer. (2017). Machine Learning for Humans. (p.9).
Retrieved from https://www.scribd.com/document/260490729/Machine-Learning-for-Humans

Tendencias

Servicios Over-The-Top y alta demanda de velocidades de interconexión, banda ancha,

Teléfonos Inteligentes

IoT

Autos interconectados, etc.

La tecnología de AI tecnología ayuda a mejorar sus relaciones con los clientes

Uso de agentes inteligentes como Asistentes Digitales (Chatbots)

Análisis de datos y AI puede estudiar la red para evitar colapsos, analizar su probabilidad, severidad y localidad para minimizar su impacto a los clientes.

El aprendizaje de máquinas se puede aplicar en ventas.

Pronósticos inteligentes puede ayudar a predecir futuras necesidades para minimizar almacenamiento de productos.

El manejo inteligente ayudar en eficiencia de economías de escala

Servicios OTT, IoT, Cloud, Big Data, Pagos digitales, Realidad Virtual Aumentada (VR/AR)

Confianza en el uso de las TIC

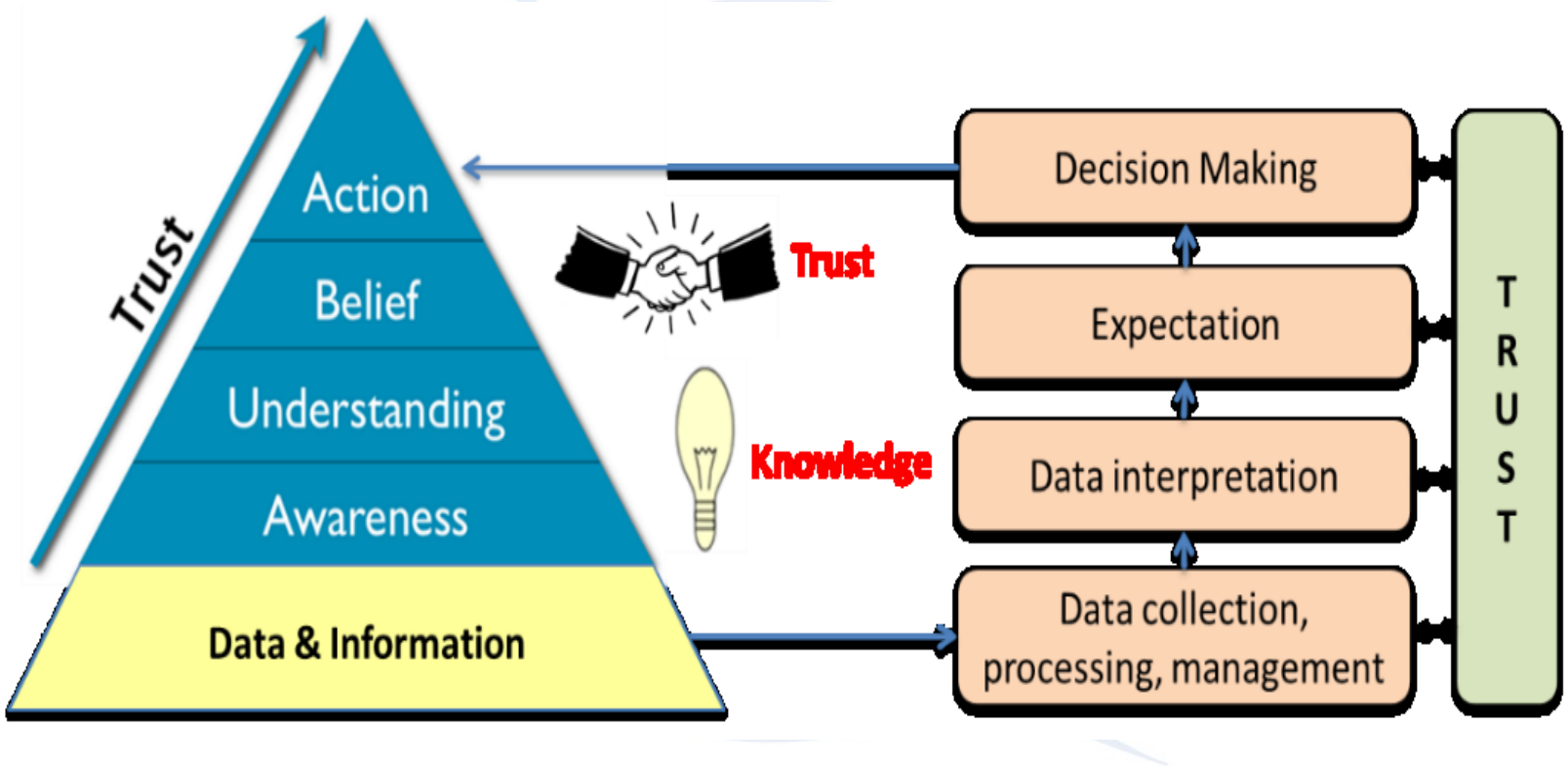
Logros

- Reporte “Trust provisioning for future ICT infrastructures and services”
- Recomendaciones sobre principios básicos para ambientes confiables Y.trusted-env
- Conceptos para redes confiables inter-cloud Draft Rec Y.CCTIC

Qué viene

- Requerimientos, capacidades y escenarios para confianza
- Arquitectura para redes confiables
- Soluciones técnicas
- Análisis confiable de Big Data
- Manejo confiable Inter Cloud

Conocimiento y Confianza



Acciones en Protección de la Infancia en Línea

- Un Niño es todo ser humano menor de 18 años de edad.
- Cada niño es diferente y sus necesidades especificas deben ser objeto de atención particular
- Considerar factores locales legislativos y culturales
- Cada vez más fácil alcance a un mundo digital
- Los costos de los dispositivos inteligentes disminuye cada vez mas
- Los niños y jóvenes son los actuales ciudadanos digitales
- Y están expuestos a: Intimidación, Acoso, Usurpación de identidad abuso en línea, contenido prejudicial o ilícito, pedofilia, etc.

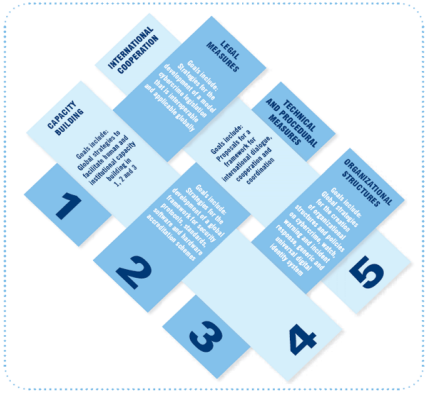
UIT y Ciberseguridad

world summit on the information society
Geneva 2003 - Tunis 2005

Ginebra 2003 – Túnez 2005

WSIS UIT como único facilitador Línea de Acción C5

"Construyendo Confianza y Seguridad en el uso de las TICs"



2007

Secretario General de la UIT lanzó la Agenda Global de Ciberseguridad (GCA)

Un esquema de trabajo para cooperación internacional sobre ciberseguridad

2008 – 2010

Membresía UIT en respaldo de la GCA como la estrategia global de cooperación internacional.

WSIS reconoce la necesidad de proteger a los niños y jóvenes en el Ciberespacio

Iniciativa Child Online Protection (COP)

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

- Hacia un alcance **global**.
- Direccionada en un **marco de trabajo internacional** 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.

COP contribuye directamente a los ODS

Fin del Abuso, explotación, tráfico y todas las formas de violencia y tortura.

Cinco áreas principales para proteger y promocionar los derechos de los niños en el ambiente online

Procesos de regulaciones y administración	Contenido de abuso sexual infantil	Ambiente seguro y apropiado por edad	Educar niños, padres y profesores	Promover el positivo uso de las TIC
Integra los derechos de los niños en regulaciones y procesos de administración	Desarrollo de procesos para manejo de contenido de abuso sexual de la niñez	Desarrolla ambientes online seguros y apropiados a la edad	Educa niños, padres y profesores sobre seguridad de los niños en el manejo de las TIC	Promueve tecnología digital como un modelo para buena ciudadanía

La propuesta de las guías es proveer:

- ✓ Un plan de acción que puede ser adaptado localmente por la industria
- ✓ Establecer una comparación de mercado de acciones recomendadas
- ✓ Guía para identificar, prevenir y mitigar riesgos
- ✓ Guía para apoyar los derechos de los niños

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

Actividades

- Eventos de concienciación;
- Trabajo en las comisiones de Estudio ITU-T SG 17;
- Reportes;
- Encuestas en line;
- Planes Nacionales de Ciberseguridad;
- Recomendación de asignación de líneas de protección a la niñez marcando 116 o 116 111;
- Índices de Ciberseguridad;
- Trabajo con partners.

A considerar

- Aprendizaje en línea y contribuir a crear una mejor sociedad
- No existe una solución única e infalible para proteger a los niños en línea
- Se requiere colaboración mundial de todos los segmentos de la sociedad
- Entretenimiento y redes sociales
- Incremento en Juegos en línea
- Incremento en Mundos virtuales / Comercio digital
- Cortesía Digital: Ser un ciudadano responsable en esta nueva sociedad
- Comunicación Digital: Intercambio electrónico de Información
- Alfabetización Digital
- Acceso digital: No exclusión digital
- Derechos y Responsabilidades
- Seguridad Digital: Autoprotección

Normas de Conducta Ciudadanía Digital

- De 5 a 7 años: Primeras experiencias con la tecnología. Se debe vigilar al niño todo el tiempo. Se considera muy útil el software de filtrado o la implementación de otras medidas como listado de sitios seguros, etc.
- De 8 a 12 años: Etapa de transición del niño, exploran y buscan respuestas por si mismos. Implementar software de filtrado, listas seguras, antivirus;
- De mayores de 13 años: Utilizan la tecnología con mucha destreza, software de filtrado ya no es muy útil. Su curiosidad sobre asuntos sexuales los puede llevar a situaciones difíciles, por lo que es importante que comprendan como estar seguros en línea y los peligros que existen.

Pon Límites

- Privacidad en redes sociales. Concatenando información se puede encontrar información privada tuya y de tu familia;
- Uso de seudónimos en redes sociales. Utiliza configuración de privacidad incluso en mensajes instantáneos.
- No publiques tu dirección, numero de teléfono u otros datos personales;
- No publiques fotos de tus amigos sin su consentimiento;
- Piensa dos veces antes de subir algo en línea, quizás no puedas borrarlo posteriormente y no sabes donde pueda terminar;
- Ten cuidado con las apariencias, confirma la información de fuentes confiables
- Tienes derechos. No te dejes acosas o intimidar como en la vida real;
- No ingreses a sitios con restricción de menores de 18 años.

Consejos

- Piensa antes de reunirte con un amigo en línea, y acude con alguien de confianza;
- A veces los contactos en línea se pueden convertir en amigos.
- Cuidado con invitaciones de desconocidos;
- Las redes sociales no es un concurso de acumulación de contactos.
- Protégete y rechaza contenido que te disguste, no accedas a cadenas;
- Abandona conversaciones de sitios con contenido no adecuado;
- Bloquea a todo el que te envíe mensajes groseros, inoportunos o amenazantes;
- Puedes guardar el mensaje como prueba y solicita guía de un adulto;
- Mantente alerta cuando un desconocido quiere hablarte de sexo – Reportarlo;
- Si has caído en la trampa de actividades sexuales o enviar imágenes sexuales tuyas, infórmalo a tus padres o a tu tutor;
- Puedes reportar al administrador de la Web;
- Puedes reportar actividades ilícitas o ilegales a la policía;
- Tu huella Digital: Todo lo que subas a Internet permanecerá por años y podrá verlo todo el mundo

Consejos

- Utilizar Firewalls y programas antivirus;
- Instalar actualizaciones;
- Utiliza controles parentales;
- No abras archivos de desconocidos;
- Verifica donde estas conectado;
- Tienes derecho a proteger tu identidad;
- Tienes derecho a participar, divertirte y acceder a información para tu edad;
- Tienes derecho a expresarte libremente y ser tratado con respecto;
- Tienes derecho a decir NO ante pedidos incómodos;
- Trata de determinar si el sitio es fiable / hay pop ups? / Es fácil encontrar al autor? / Evitar paginas falsas / Indica la fecha de la última actualización? / Contiene avisos de carácter jurídico, privacidad?;
- Utiliza contraseñas difíciles de descifrar y usuarios de correo complejos;
- Activa la restricción de spam;
- Utiliza dos direcciones de correo, una personal y otra para suscripciones en línea.

Consejos

- Colocar las PCs en un salón común;
- Establecer reglas generales de utilización del Internet que consideren privacidad, edad, restricción de sitios, acoso, etc.;
- Informarse de los sitios que los hijos frecuentan y los dispositivos que utilizan;
- Guiar y enseñar a los hijos sobre los riesgos de la difusión de la información personal, encuentros con desconocidos, utilización de cámaras web;
- Estar atentos a cualquier cambio de comportamiento;
- Cuidado con la utilización no autorizada de tarjetas de crédito;
- Cuidado con la utilización de la cuenta de correo de los padres para sobrepasar restricciones parentales;
- Educadores pueden ser victimas de amenazas de los alumnos.

Gracias a nuestros partners

MUCHAS GRACIAS!!!

PREGUNTAS?