

Sistemas de reacción integrado de múltiples partes interesadas en el cumplimiento de la ley






Simposio internacional sobre la seguridad cibernética y equipos de respuesta
III Foro de seguridad digital

Bogotá D.C., 29 de septiembre de 2016

“Necesidad” por la estabilidad y seguridad del ciberespacio

- Vida diaria de ciudadanos
- Economía nacional
- Seguridad nacional

Peta, 2 IntJ Info Sec & Cybercrime 55 (2013)

-  = 1 user in Asia
-  = 1 user in Europe
-  = 1 user in the Americas
-  = 1 user in Africa
-  = 1 user in Oceania

Internet users in the world

3,460,862,099

All on this page, one by one

watch as they increase



Fuente:
<http://www.internetlivestats.com/watch/internet-users/region/>, consultada 20.09.2016



OECD Digital Economy
Outlook 2015



 **OBJETIVOS DE DESARROLLO SOSTENIBLE**



Documento WSIS-03/GENEVA/4-S. **Declaración de principios**

35. El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo.



**cumbre mundial sobre
la sociedad de la información**
Ginebra 2003 - Túnez 2005





**Policy Options for Connecting and Enabling the Next Billion – Phase II:
Call for Public Input
11 July 2016**

- Nuevos usuarios
- Bajo costo de conectividad
- Opciones de acceso
- Uso
- Acceso significativo
- Acceso con conocimiento de los riesgos

Introduction

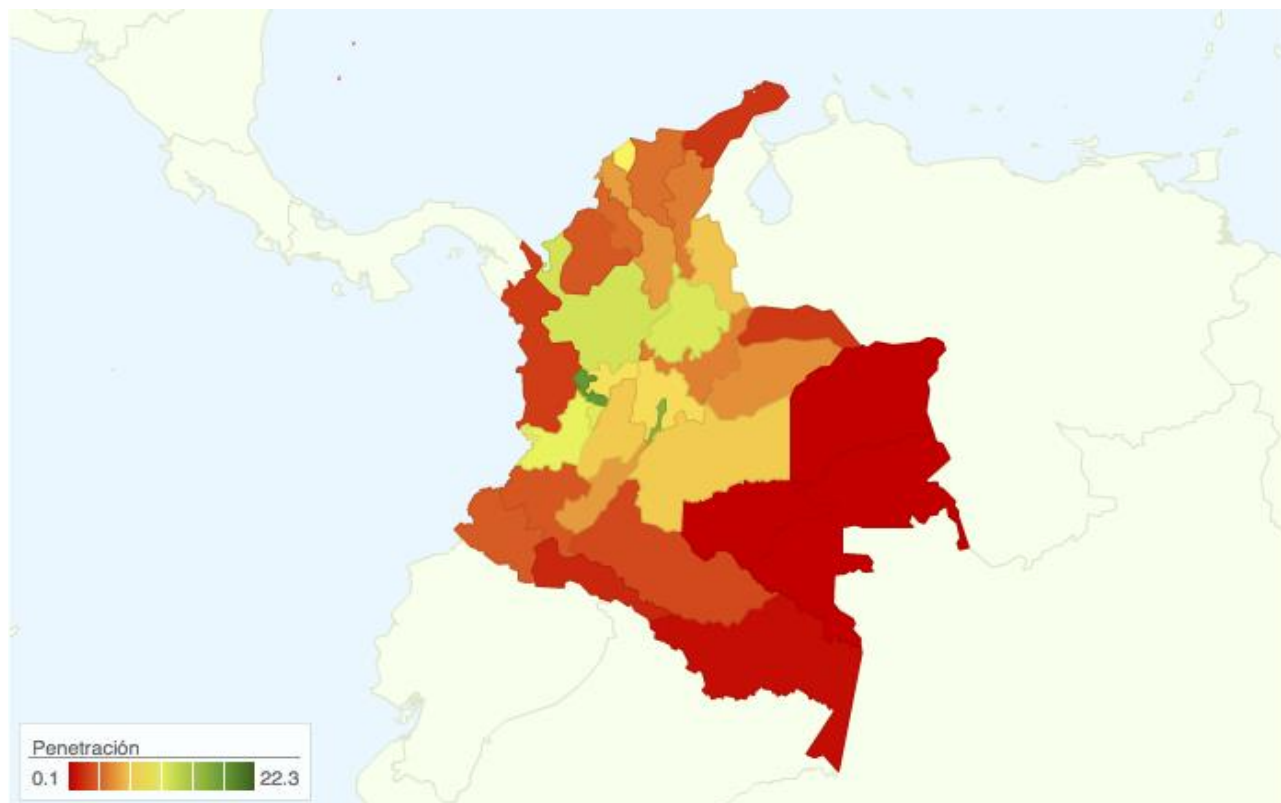
In 2015, over 70 [submissions](#), including 22 from national and regional IGF initiatives (NRIs), contributed to the development of a set of [Policy Options for Connecting the Next Billion](#) that were presented at IGF 2015 in João Pessoa, Brazil, in November 2015.

The first phase of the IGF intersessional project *Policy Options for Connecting the Next Billion* (2015) focused on developing a set of policy options aiming at the creation of enabling environments, including deploying infrastructure, increasing usability, enabling users and ensuring affordability.

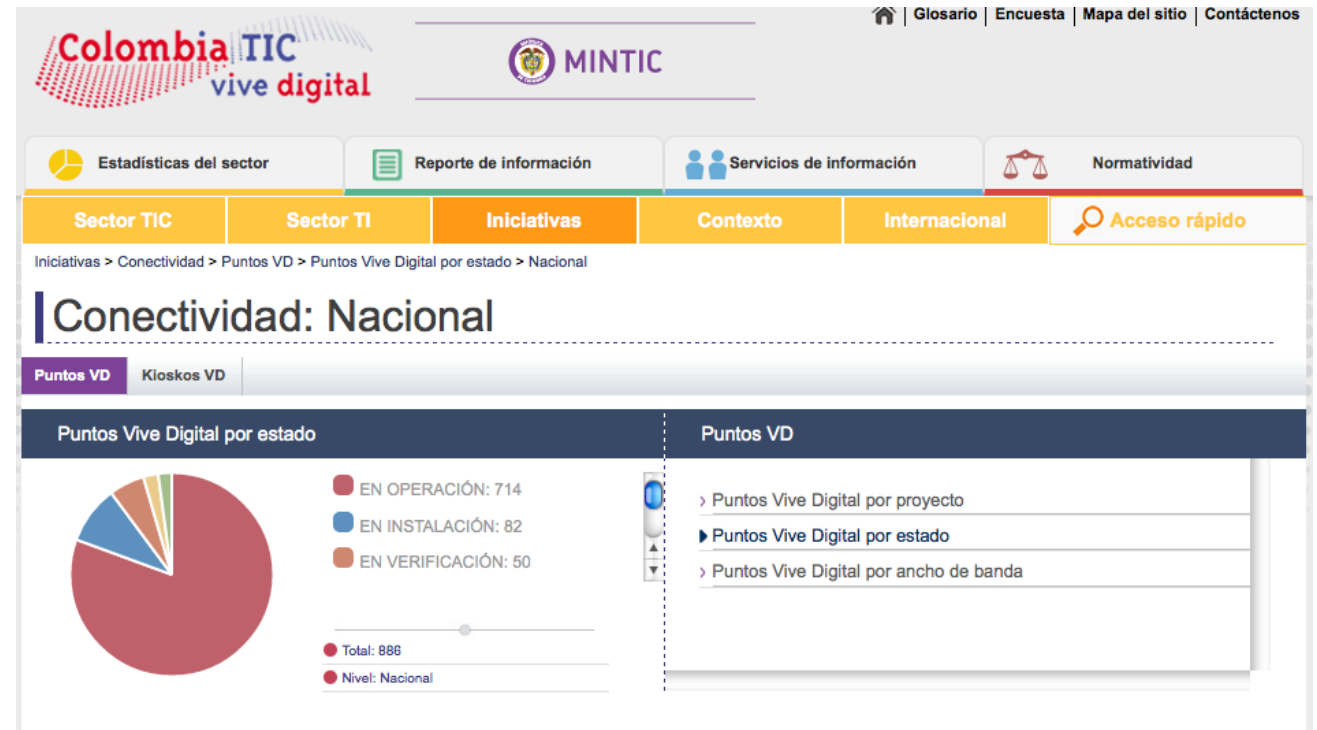
In April 2016, the MAG decided to explore further developing the IGF “*Policy Options for Connecting the Next Billion*”.

Penetración de internet en Colombia 2015-1

Fuente: Colombia TIC, Vive digital. En línea,
<http://estrategiaticolombia.co/estadisticas/stats.php?id=25&pres=map&jer=1&cod=>

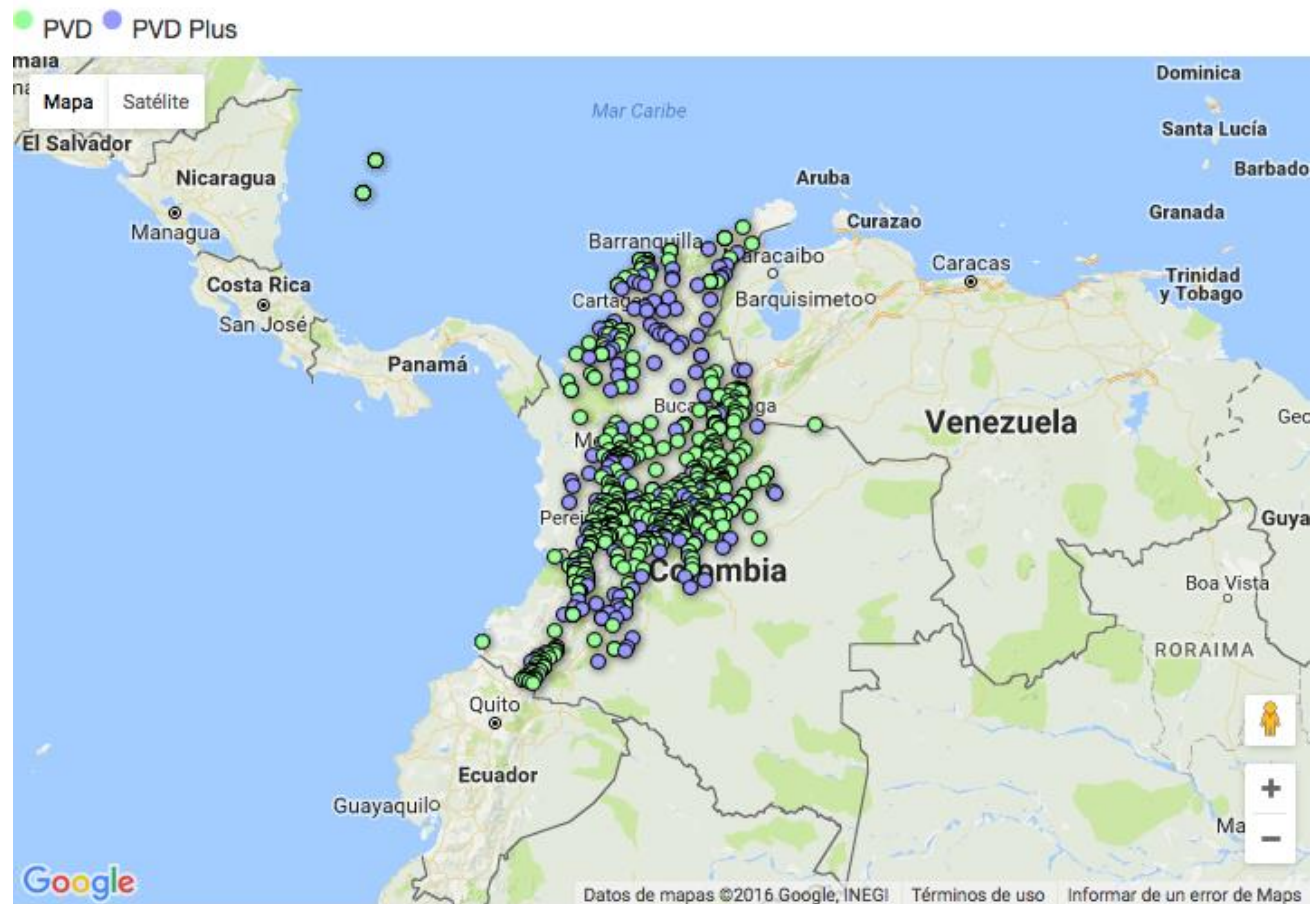


Iniciativas: conectividad puntos vive digital



Fuente:

http://micrositios.mintic.gov.co/vivedigital/mapas/mapa_4_municipios_puntos_vive_digital.php



Iniciativas: conectividad kioskos vive digital



Fuente:

http://micrositios.mintic.gov.co/vivedigital/mapas/mapa_3_kioscos_vive_digital.php



- Seguridad es un medio, no un fin
 - Administración del riesgo
 - Mejorar el futuro
- ¿La seguridad es algo de pocos?
- Ciberseguridad vs seguridad en medios físicos

Geer, 1 Harv. Nat'l Sec. J. i (2010)

Ciberdefensa y Ciberseguridad

Establecimiento de roles

- Empresa
- Gobierno
- Usuarios
- Organizaciones/empresas de ciberseguridad

Respuesta

- Tecnológica
- Jurídica
- Social

¿Cambiar el régimen de responsabilidad?

- PSI/ISP – “clean pipes”
 - Responsabilidad del productor de software
 - Gobierno
 - Usuario final
-
- **OPCIÓN: reacción que contemple a las contrapartes comprometidas es el fundamento de la concientización**

Regulación por riesgos

- Identificación
- Administración
- Prevención efectiva
- Mitigación

¿Cómo empoderar? = conocimiento

- Conciencia de ciberseguridad entre el público general y particularmente usuarios TI
- Capacitación de especialistas
- ¿Quién?

Cooperación internacional

- Compromiso internacional es necesario pero ciertamente insuficiente
(*Geer, 1 Harv. Nat'l Sec. J. i 2010*)
 - Experiencias en la lucha internacional contra el crimen organizado

Cooperación

- Entre Estados, entre entidades gubernamentales, o autoridades de supervisión
- Empresarios: de manera individual y a través de agremiaciones
- Por parte de la sociedad civil
 - Denuncia
 - Informarse

“No decidir es decidir”

Cambio de paradigmas

- Sociedad de la información ha desafiado al derecho
 - Contractual
 - Responsabilidad
 - Propiedad intelectual
 - Protección al consumidor
 - Protección de datos personales
 - Delitos informáticos
 - Delitos económicos por medios electrónicos
 - Derecho procesal y derecho probatorio

Retos regulatorios *(U. Sieber)*

- La sociedad de la información requiere medidas no penales para la PREVENCIÓN del delito computacional/delitos informaticos.
- OTRAS MEDIDAS:
 - Estándares de seguridad tecnológica
 - Sistemas de control de acceso
 - Instrucciones para los usuarios
 - Condiciones generales de derecho civil y administrativo son más importantes que las disposiciones penales

Múltiples partes interesadas

- Señalar roles y responsabilidades
- Empoderar
- Retos

¿Preguntas?

Línea de investigación en Comercio Electrónico
adriana.castro@uexternado.edu.co