



LOGROS 2010 - 2015

Colombia vive una revolución digital

RIESGOS DE
SEGURIDAD
DIGITAL EN
COLOMBIA



**DE 24
A 6**

NIÑOS POR TERMINAL



40%

CRECIERON LOS PAGOS
ELECTRÓNICOS EN 2014



+400

TRÁMITES CON
EL ESTADO SE PUEDEN
REALIZAR TOTALMENTE
EN LÍNEA



82%

DE CIUDADANOS
INTERACTUARON POR
MEDIOS ELECTRÓNICOS
CON EL ESTADO
DURANTE 2014



79%

DE EMPRESAS
INTERACTUARON CON EL
ESTADO POR MEDIOS
ELECTRÓNICOS DURANTE
2014

**COLOMBIA #4 EN
DATOS ABIERTOS A
NIVEL MUNDIAL Y
#1 EN AMÉRICA
LATINA**

RIESGOS DE SEGURIDAD DIGITAL EN COLOMBIA



TIC, ECONOMÍA DIGITAL Y RIESGOS DE SEGURIDAD DIGITAL

▶ EVOLUCIÓN CRECIENTE DE LAS
TIC

▶ DIGITALIZACIÓN

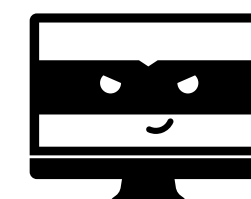
▶ ACTIVIDADES ECONÓMICAS Y
SOCIALES

▶ ECONOMÍA DIGITAL

▶ IMPACTOS POSITIVOS



INCERTIDUMBRES,
AMENAZAS Y
VULNERABILIDADES



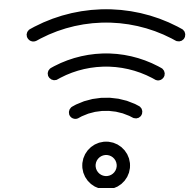
RIESGOS DE SEGURIDAD
DIGITAL



INCREMENTO DE MALWARE



ALTOS COSTOS DE LA
ACTIVIDAD MALICIOSA

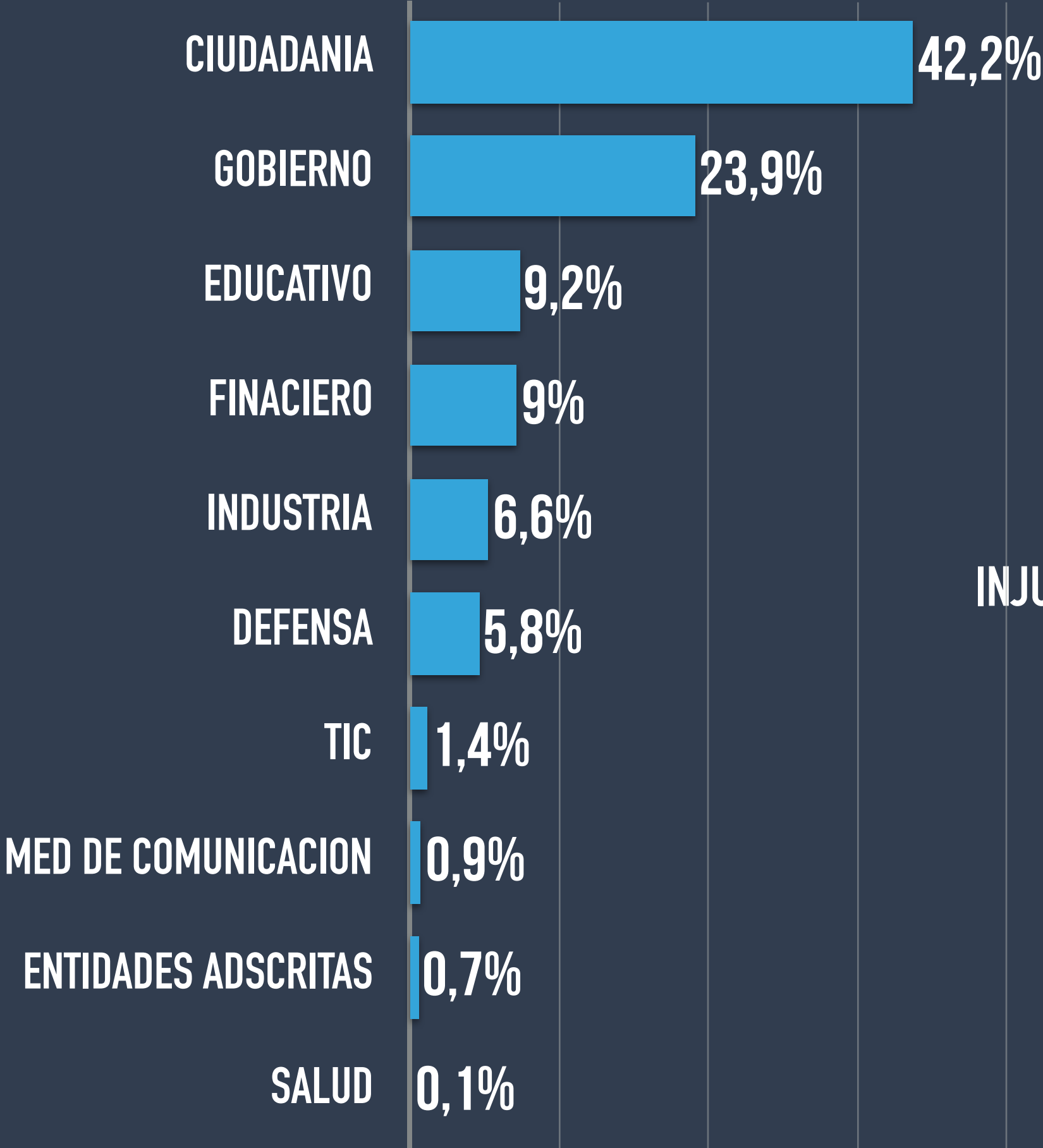


AFECTACIÓN DE
INFRAESTRUCTURA CRÍTICA

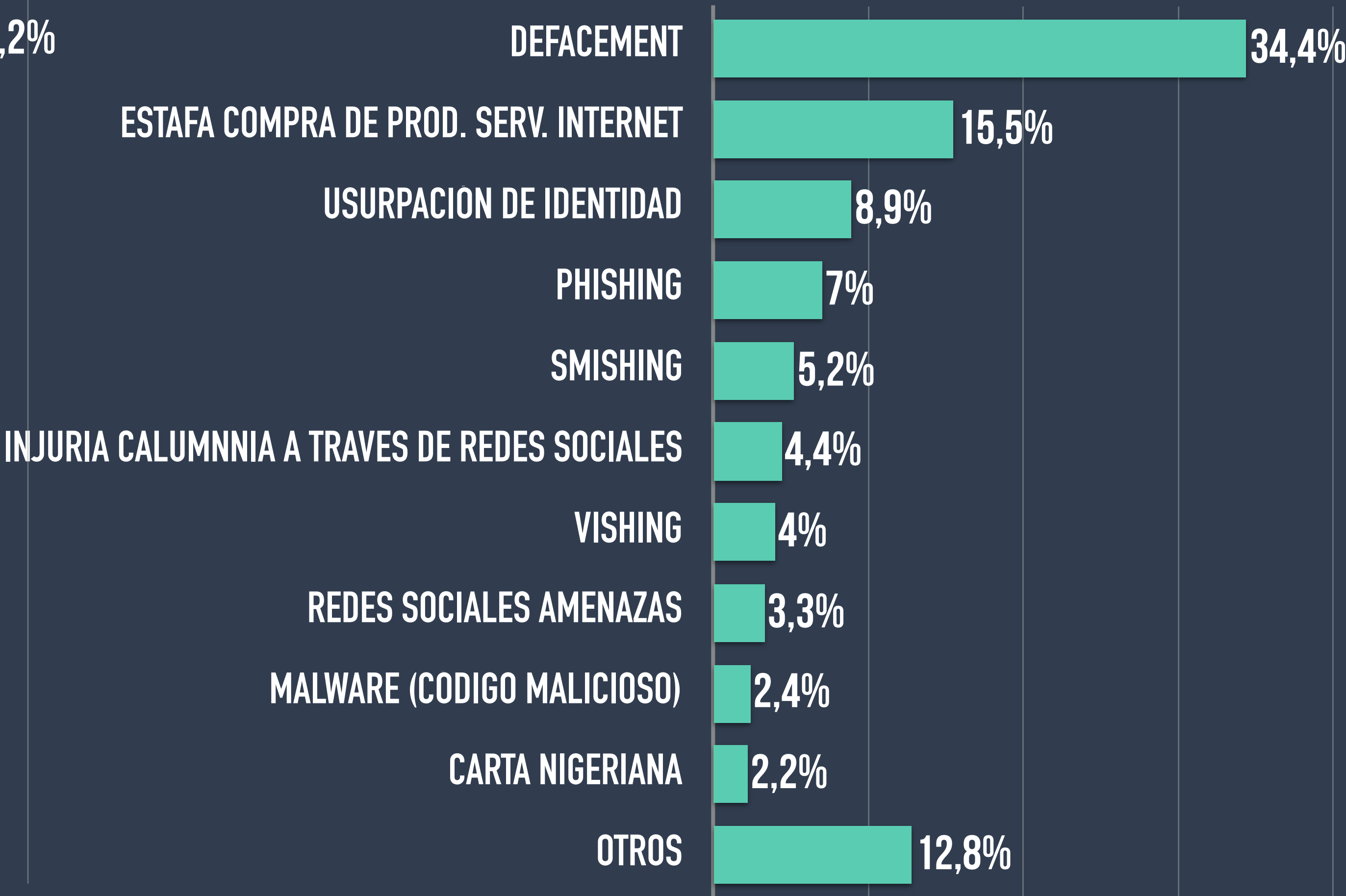
DIAGNÓSTICO INCIDENTES



SECTORES AFECTADOS EN COLOMBIA POR INCIDENTES DIGITALES, 2015



INCIDENTES DIGITALES GESTIONADOS POR CCP Y CSIRT PONAL EN EL ENTORNO DIGITAL EN COLOMBIA, 2015



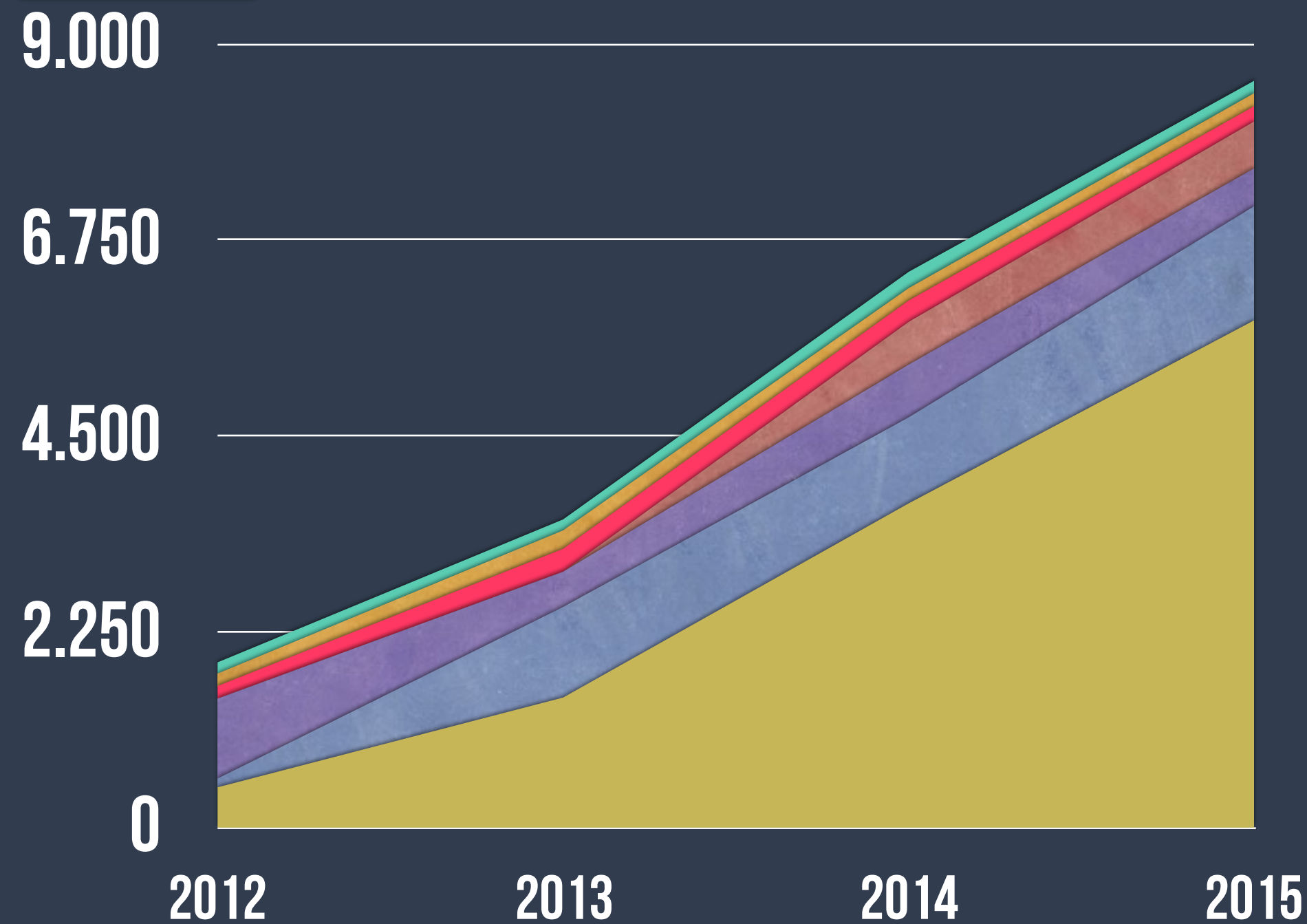
RIESGOS DE
SEGURIDAD
DIGITAL EN
COLOMBIA



DIAGNÓSTICO DENUNCIAS



DENUNCIAS PROCESADAS POR LA
INICIATIVA TE PROTEJO 2012 -
2015

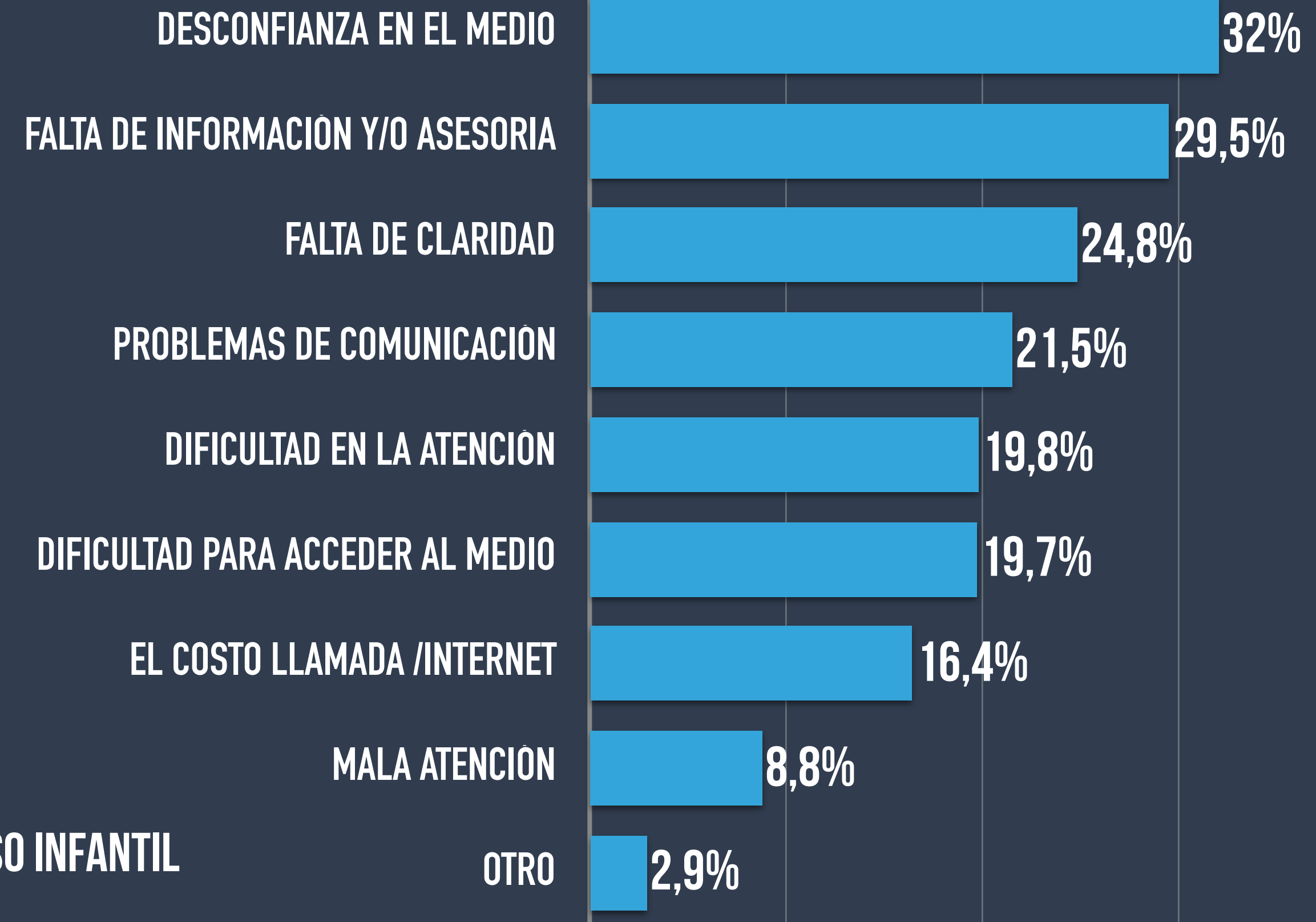


PORNOGRAFÍA INFANTIL
OTROS
CONTENIDOS INAPROPIADOS
INTIMIDACIÓN ESCOLAR

MALTRATO, TRABAJO Y ABUSO INFANTIL
CIBERACOSO
VENTA DE ALCOHOL



BARRERAS PARA REALIZAR TRÁMITES Y
SERVICIOS EN LÍNEA EN UN COMPUTADOR
(MINTIC – INFOMETRIKA 2014)



RIESGOS DE
SEGURIDAD
DIGITAL EN
COLOMBIA



DIAGNÓSTICO INSTITUCIONAL

RIESGOS DE SEGURIDAD DIGITAL EN COLOMBIA



**NO SE CUENTA CON UNA VISIÓN
ESTRATÉGICA** BASADA EN LA GESTIÓN
DE RIESGOS



**LAS MÚLTIPLES PARTES INTERESADAS
NO MAXIMIZAN SUS OPORTUNIDADES** AL
DESARROLLAR ACTIVIDADES
SOCIOECONÓMICAS EN EL ENTORNO
DIGITAL



**SE NECESITA REFORZAR LAS
CAPACIDADES DE CIBERSEGURIDAD** CON
UN ENFOQUE DE GESTIÓN DE RIESGOS DE
SEGURIDAD DIGITAL



**SE NECESITA REFORZAR LAS
CAPACIDADES DE CIBERDEFENSA** CON
UN ENFOQUE DE GESTIÓN DE RIESGOS
DE SEGURIDAD DIGITAL



**LOS ESFUERZOS DE COOPERACIÓN,
COLABORACIÓN Y ASISTENCIA,
NACIONAL E INTERNACIONAL,
RELACIONADOS CON LA SEGURIDAD
DIGITAL NO SON SUFICIENTES Y
REQUIEREN SER ARTICULADOS**



CONPES DE SEGURIDAD DIGITAL



POR QUÉ UN CONPES?

Es el máximo
organismo de
coordinación de la
política económica y
social de Colombia

Tiene seguimiento
de Alto Nivel

Establece
lineamientos y
orientaciones de
la política pública

Mejor instrumento para
que miembros de Alto Nivel
del gobierno central
atiendan instrucciones
directas de la Presidencia
de la República

El Conpes anterior
(3701 de 2011),
tenía acciones
definidas hasta el
2015

Es una
oportunidad
para tener
recomendaciones
de Alto Nivel

POLÍTICA ANTERIOR

AVANCES DE LAS RECOMENDACIONES ESTABLECIDAS EN EL **CONPES 3701 DE 2011**
(90% DE ACTIVIDADES CUMPLIDAS EXITOSAMENTE)

LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA (2011 a 2015)

 **PRESIDENCIA**

Comisión
Nacional Digital y
de Información
Estatel
Dec. 32 de 2013

Institucionalidad
enfocada en la
seguridad desde
perspectiva técnica

 **MINJUSTICIA**

 **MINTIC**

 **MINDEFENSA**

 **CANCILLERÍA**

colCERT

**CIBERSEGURIDAD
PONAL**

 **CENTRO CIBERNÉTICO
POLICIAL**

**CIBERDEFENSA
CGFM**

CCOC

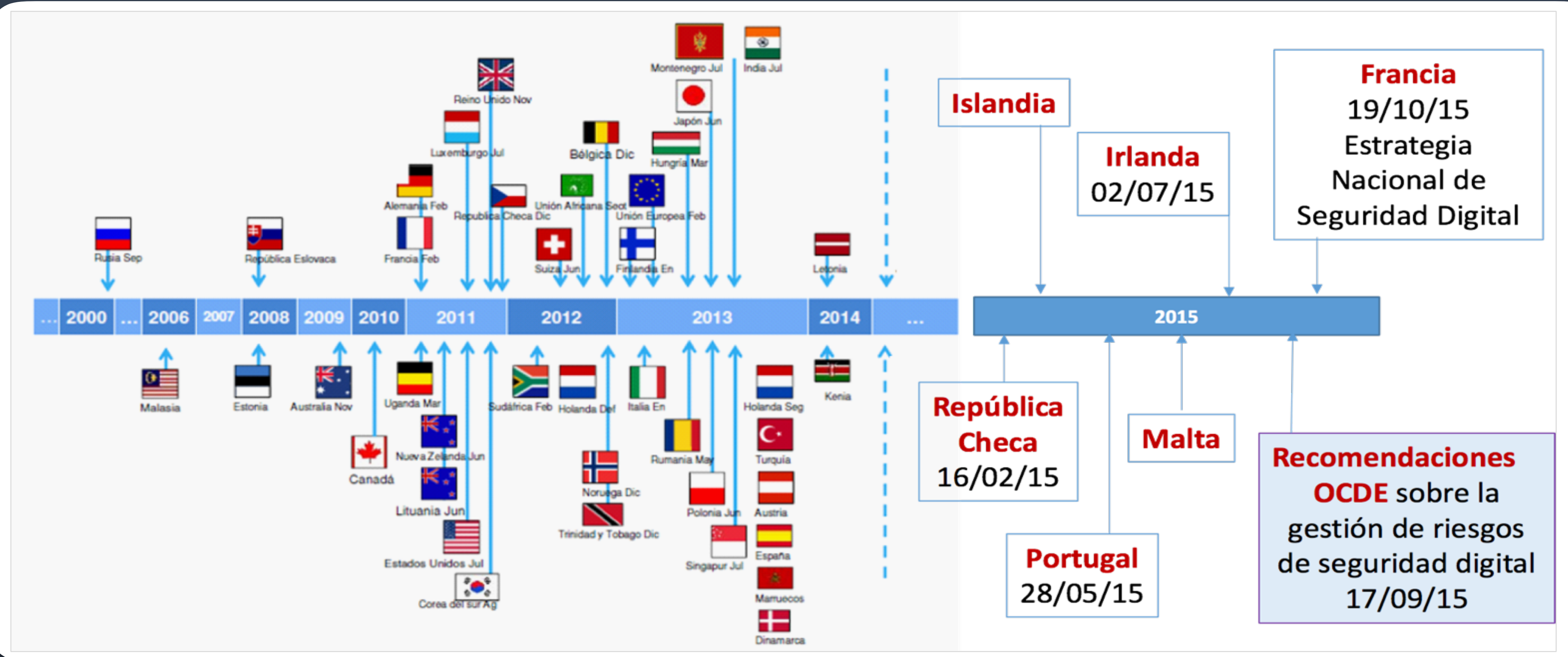


MESAS DE TRABAJO CON EXPERTOS NACIONALES E
INTERNACIONALES EN 2014 Y 2015 PARA ANALIZAR EL
ESTADO DE LA POLÍTICA VIGENTE

CONPES
SEGURIDAD
DIGITAL



POLÍTICAS / ESTRATEGIAS INTERNACIONALES



CONPES
SEGURIDAD
DIGITAL



- ESTRATEGIAS ENMARCADAS EN UN CONJUNTO DE PRINCIPIOS GENERALES
- BASADAS EN LA GESTIÓN DE RIESGOS
- DISTINCIÓN ENTRE OBJETIVOS DE PROSPERIDAD ECONÓMICA Y SOCIAL, Y DEFENSA NACIONAL Y LUCHA CONTRA EL CRIMEN Y LA DELINCUENCIA DIGITAL

MEJORES PRÁCTICAS PARA ABORDAR RIESGOS DE SEGURIDAD DIGITAL

CONPES
SEGURIDAD
DIGITAL



- ▶ Enfoque de gestión del riesgo
- ▶ Liderazgo alto nivel del gobierno
- ▶ Defensa y seguridad nacional
- ▶ Enfoque multidimensional
- ▶ Responsabilidad compartida
- ▶ Salvaguardar derechos humanos
- ▶ Concientizar y educar

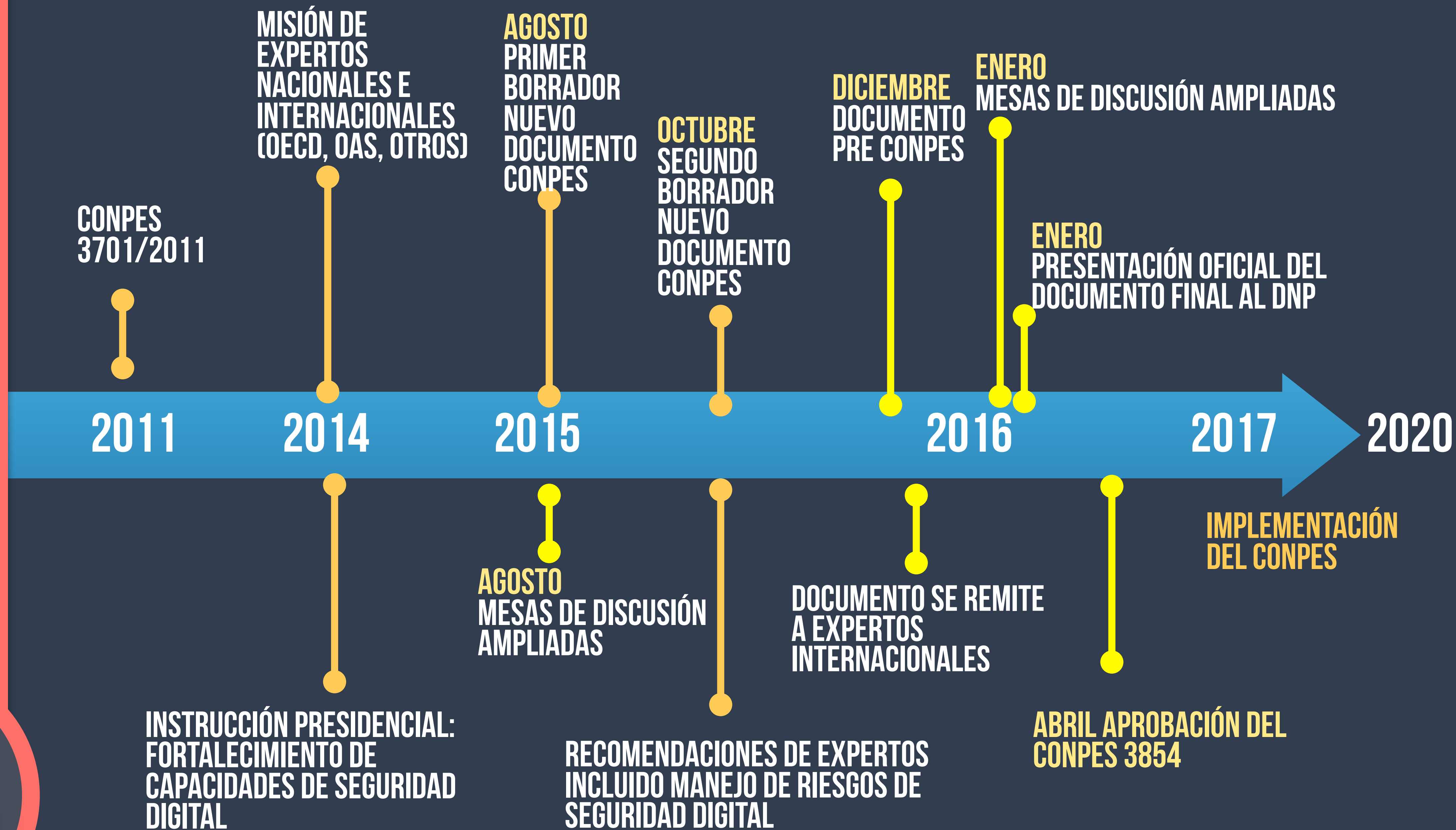


Organization of
American States



Information Technology
Industry Council

¿CÓMO LO HICIMOS?



GENERALIDADES

PRINCIPIOS FUNDAMENTALES

- ▶ SALVAGUARDAR DERECHOS HUMANOS
- ▶ ENFOQUE INCLUYENTE Y COLABORATIVO
- ▶ RESPONSABILIDAD COMPARTIDA
- ▶ ENFOQUE DE GESTIÓN DE RIESGO

DIMENSIONES ESTRATÉGICAS

- ▶ GOBERNANZA
- ▶ MARCO LEGAL Y REGULATORIO
- ▶ GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL
- ▶ CULTURA CIUDADANA
- ▶ CAPACIDADES PARA LA GESTIÓN DEL RIESGO

OBJETIVOS ESTRATÉGICOS - ENTORNO DIGITAL

- ▶ ESTABLECER UN MARCO INSTITUCIONAL BASADO EN LA GESTIÓN DE RIESGOS
- ▶ CREAR CONDICIONES PARA GESTIONAR Y GENERAR CONFIANZA
- ▶ FORTALECER LA SEGURIDAD DE LOS INDIVIDUOS Y DEL ESTADO
- ▶ FORTALECER LA DEFENSA Y SOBERANÍA NACIONAL
- ▶ IMPULSAR LA COOPERACIÓN, COLABORACIÓN Y ASISTENCIA EN SEGURIDAD DIGITAL

CONPES
SEGURIDAD
DIGITAL



POLÍTICA ACTUAL: CONPES 3854 DE 2016

CONPES
SEGURIDAD
DIGITAL



CÓMO LO VAMOS A LOGRAR DESDE EL MINTIC



**MODELO DE GESTIÓN DE
RIESGOS DE SEGURIDAD
DIGITAL**



**TANQUE DE
PENSAMIENTO**



EVALUACIÓN Y SEGUIMIENTO

**CONPES
SEGURIDAD
DIGITAL**



CÓMO LO VAMOS A LOGRAR DESDE EL MINTIC



**EVALUACIÓN IMPACTO NEGATIVOS
SOBRE LA PROSPERIDAD ECONÓMICA
Y SOCIAL**

▶ **ESTUDIO SOBRE EL IMPACTO DE LOS
DELITOS Y CRÍMENES EN EL
ENTORNO DIGITAL**



**GENERACIÓN DE CONFIANZA EN EL USO DEL
ENTORNO DIGITAL**

▶ **PROGRAMAS, PROYECTOS Y
CAMPAÑAS DE APROPIACIÓN,
SOCIALIZACIÓN Y CONCIENTIZACIÓN**

▶ **FORTALECER LAS CAPACIDADES DE
GESTIÓN DE RIESGOS DE SEGURIDAD
DIGITAL EN EL ESTADO.**

**CONPES
SEGURIDAD
DIGITAL**



CÓMO LO VAMOS A LOGRAR DESDE EL MINTIC



**MECANISMOS PARA LA COOPERACIÓN,
COLABORACIÓN Y ASISTENCIA
INTERNACIONAL**

- ▶ **DEFINIR UNA AGENDA
ESTRATÉGICA INTERNACIONAL**



**MECANISMOS PARA LA COOPERACIÓN,
COLABORACIÓN Y ASISTENCIA
NACIONAL**

- ▶ **DEFINIR UNA AGENDA ESTRATÉGICA DE
COOPERACIÓN, COLABORACIÓN Y
ASISTENCIA EN EL ÁMBITO NACIONAL**
- ▶ **ADELANTAR JORNADAS DE
INTERCAMBIO Y TRANSFERENCIA DEL
CONOCIMIENTO**

**CONPES
SEGURIDAD
DIGITAL**



FINANCIAMIENTO

ENTIDADES	PARTICIPACIÓN
MDN	47,0%
MINTIC	48,70%
DNI	1,80%
MJD	0,50%
DNP	1,10%
MEN	0,40%

\$23.443

\$21.692

\$21.483

\$18.452

2016

2017

2018

2019

TOTAL \$ 85.070
MILLONES DE PESOS

CONPES
SEGURIDAD
DIGITAL



Fuente: DIES y DJSG, DNP.

POSCONFLICTO Y SEGURIDAD DIGITAL - CONTEXTO

POSCONFLICTO
Y SEGURIDAD
DIGITAL



6.9 MILLONES DE DESPLAZADOS
INTERNOS (PAÍS CON MAYOR
DESPLAZAMIENTO INTERNO*)



90 MIL SOLICITUDES DE RESTITUCIÓN DE
TIERRAS



8 MILLONES DE VÍCTIMAS REGISTRADAS



51% LOS DESPLAZADOS INTERNOS
RESIDEN EN LAS 25 CIUDADES
PRINCIPALES *



MARCO LEGAL, INSTITUCIONES Y
CREACIÓN DE SISTEMAS (EJ. LEY 1448
DE 2011)



INSTITUCIONALIDAD ESPECIALIZADA
(EJ. UAV, URT, ACR, CNMH)

* FUENTE: ACNUR - AGENCIA DE LA ONU PARA LOS REFUGIADOS

POSCONFLICTO Y SEGURIDAD DIGITAL - CONTEXTO

POSCONFLICTO
Y SEGURIDAD
DIGITAL



FUENTE: RNI - RED NACIONAL DE INFORMACIÓN - REGISTRO ÚNICO DE VÍCTIMAS

POSCONFLICTO Y SEGURIDAD DIGITAL - CONTEXTO

LA POLÍTICA PÚBLICA RECONOCE LA IMPORTANCIA DE GESTIONAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN UN ESCENARIO DE POSCONFLICTO:

E2.1. Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital (DE1)

Esta estrategia busca involucrar a las múltiples partes interesadas en la gestión del riesgo de seguridad digital, de tal forma que asuman la responsabilidad que les corresponde de acuerdo a su rol y función, y participen activamente tanto en la fase de construcción de los elementos que se consignan en este documento, como en la implementación de la política.

...

De igual forma, el coordinador nacional creará una agenda nacional de seguridad digital durante el año 2017, con el fin de priorizar los intereses nacionales en torno al tema, involucrando a las múltiples partes interesadas, e identificando variables de impacto nacional (por ejemplo, pérdidas económicas, afectación de personas, consecuencias medioambientales o correlación de la afectación con otras partes), bajo el marco de los principios fundamentales de la política nacional de seguridad digital. **El coordinador nacional de seguridad digital debe incluir en la agenda un capítulo específico de vinculación de las múltiples partes interesadas para gestionar los riesgos de seguridad digital en un escenario de posconflicto.**

...

POSCONFLICTO
Y SEGURIDAD
DIGITAL



POSCONFLICTO Y SEGURIDAD DIGITAL - RETOS



IMPLEMENTAR LOS SISTEMAS DE INFORMACIÓN REQUERIDOS



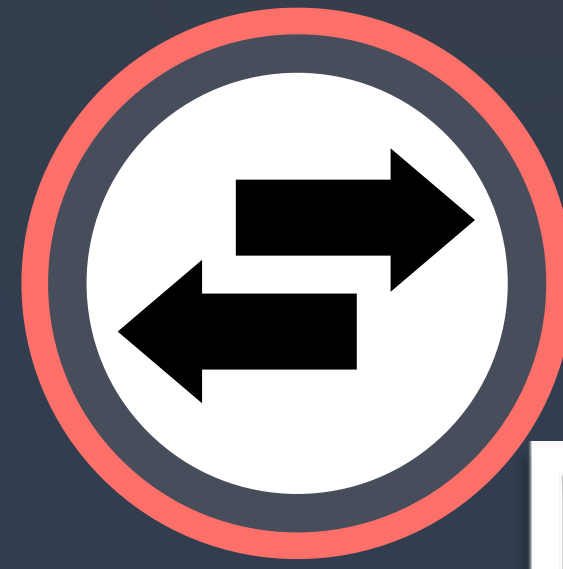
EJEMPLO: RED NACIONAL DE INFORMACIÓN

POSCONFLICTO
Y SEGURIDAD
DIGITAL



- SISTEMA NACIONAL DE ATENCIÓN Y REPARACIÓN DE VÍCTIMAS
- SISTEMA DE INFORMACIÓN PARA LA REINTEGRACIÓN
- NODO DE TIERRAS
- SISTEMA NACIONAL DE DERECHOS HUMANOS
- OTROS SISTEMAS DE INFORMACIÓN INSTITUCIONALES Y SECTORIALES
- ...

POSCONFLICTO Y SEGURIDAD DIGITAL - RETOS



GARANTIZAR LA INTEROPERABILIDAD
CON SEGURIDAD

POSCONFLICTO
Y SEGURIDAD
DIGITAL

EJEMPLO:
NODO DE
TIERRAS

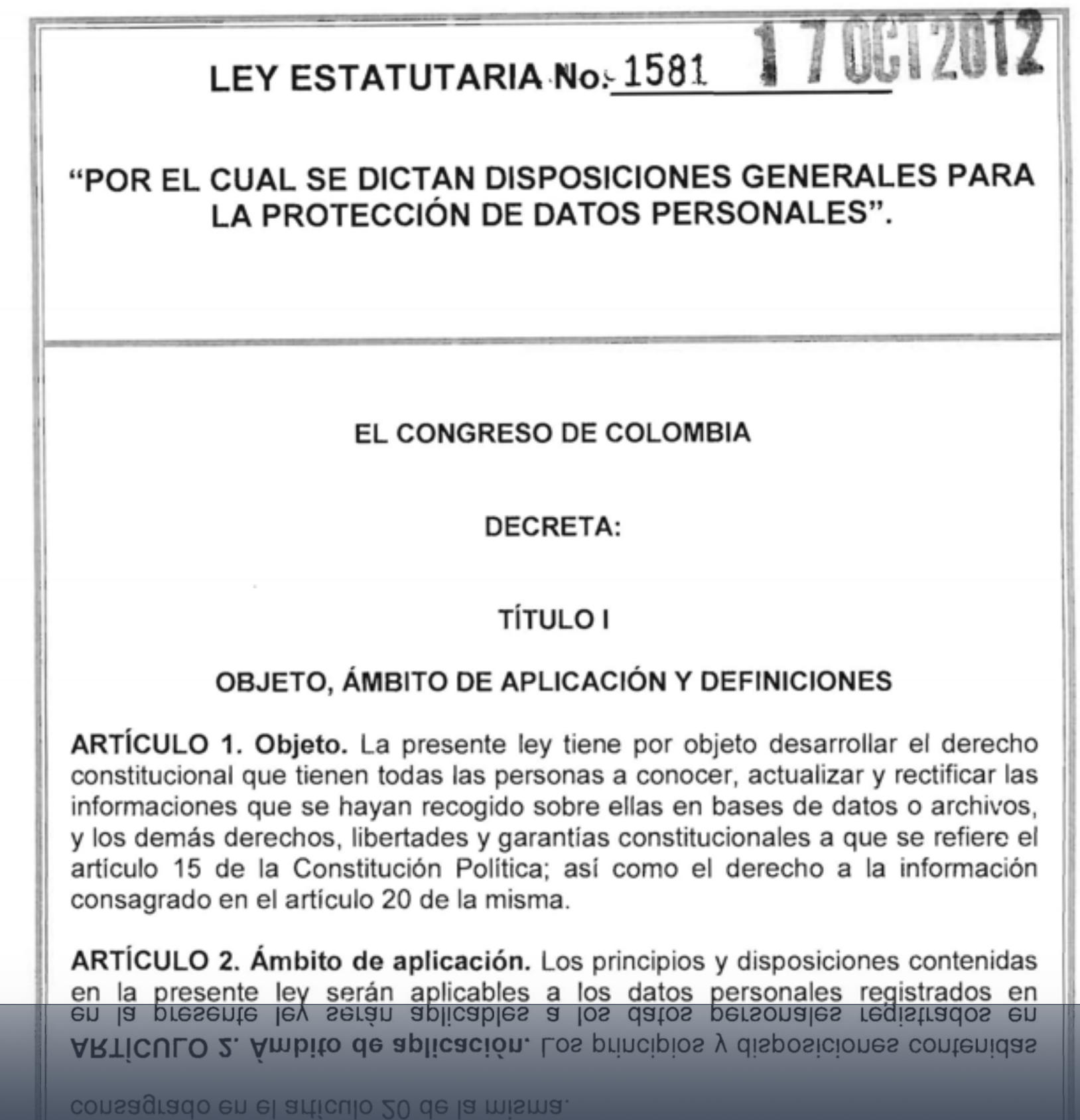
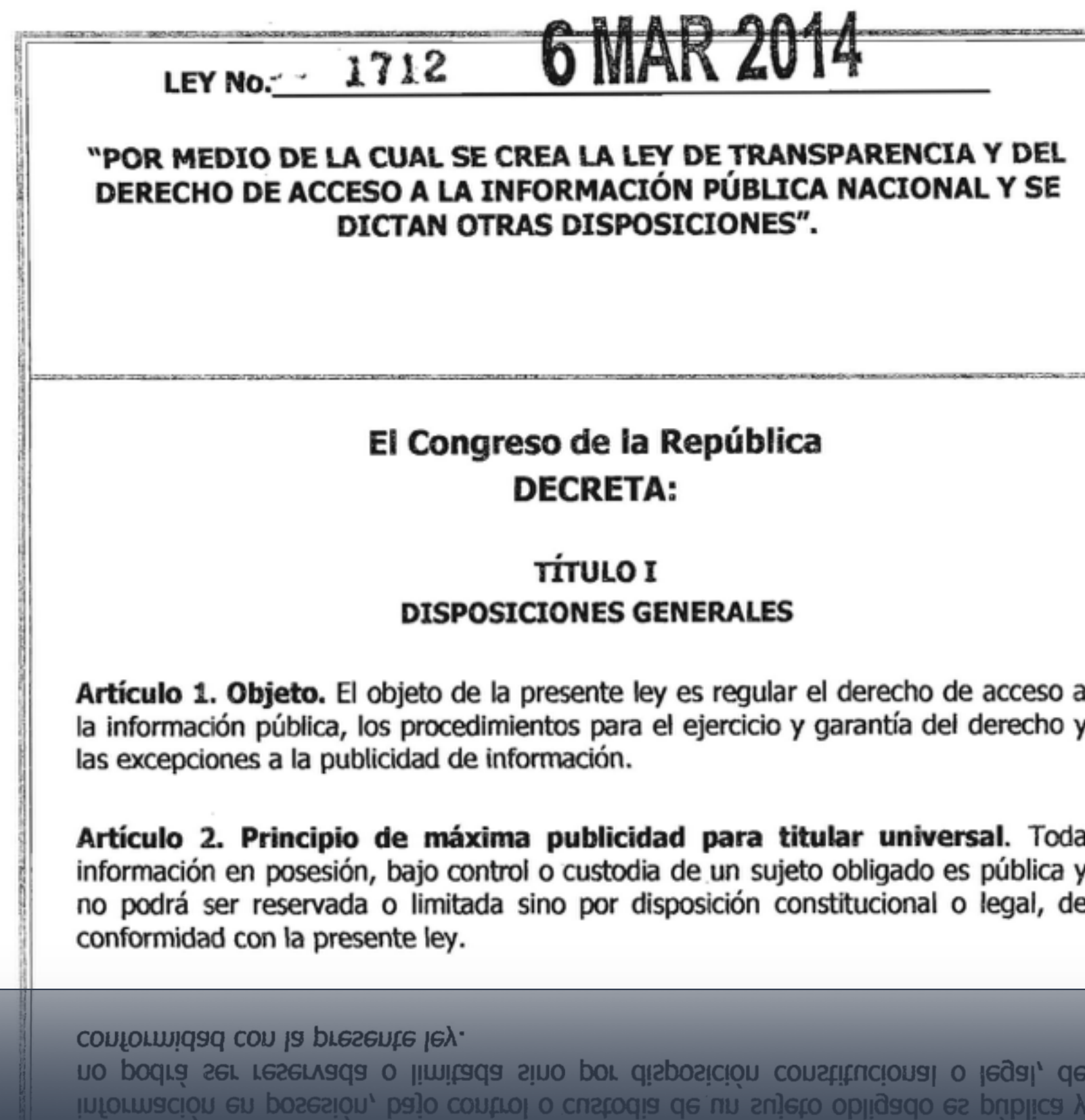


POSCONFLICTO Y SEGURIDAD DIGITAL - RETOS



ENTENDIMIENTO CLARO DE LIMITES
ENTRE TRANSPARENCIA Y
PROTECCIÓN DE DATOS PERSONALES

POSCONFLICTO
Y SEGURIDAD
DIGITAL



POSCONFLICTO Y SEGURIDAD DIGITAL - OPORTUNIDADES

POSCONFLICTO
Y SEGURIDAD
DIGITAL



MATERIALIZAR SOLUCIONES
ARTICULADAS Y “DE ESTADO”



POSICIONAR EL LADO “HUMANO” DE
LAS SOLUCIONES TECNOLÓGICAS



ELEVAR LOS NIVELES DE DISCUSIÓN
SOBRE LA SEGURIDAD DE LA
INFORMACIÓN



MODERNIZAR SOLUCIONES Y AFINAR
CONTROLES, PROCESOS Y
PROCEDIMIENTOS



VALORAR PROCESOS DE CAPACITACIÓN
ESPECIALIZADA EN SEGURIDAD Y
PRIVACIDAD



FACILITAR LA ADOPCIÓN DE
POLÍTICAS, NORMAS Y LINEAMIENTOS



A TRABAJAR POR NUESTRA GENTE



MINTIC

vive **digital**
para la gente



TODOS POR UN
NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

María Isabel Mejía
VICEMINISTRA TI

@marisabelmejia