COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Revisión del marco regulatorio para la gestión de riesgos de seguridad digital

Análisis y propuesta

Capital Intelectual

Noviembre de 2017

vive digital para la gente

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

@CRCCol /CRCCol /CRCCol CRCCol
WWW.CRCOM.GOV.CO

CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Los grandes ataques informáticos que han ocurrido en los últimos años, como el sucedido en mayo de 2017, donde un secuestro de información conocido como Wannacry atacó a más de 200.000 víctimas en todo el mundo e infectó a más de 300.000 computadoras[1], han evidenciado la importancia de la seguridad digital para todos los usuarios del ecosistema digital. El público en general es cada vez más consciente de la importancia de la seguridad digital, a partir de ataques como el de Yahoo (más de 3 billones de cuentas de usuarios comprometidas[2]) o Equifax[3] que han resultado en el robo de datos personales de millones de usuarios de estos servicios.

El inminente crecimiento de los riesgos cibernéticos (según un estudio de Digiware, se registraron 198 millones de ataques cibernéticos en Colombia el año pasado), y al tener un papel fundamental en el desarrollo económico del país y de la economía digital, no es de extrañar que según ese mismo estudio el sector de telecomunicaciones sea el segundo sector más afectado por los ataques cibernéticos (después del sector financiero)[4]; las redes de telecomunicaciones son siempre un objetivo lucrativo para los ciberdelincuentes, ya que proporcionan la columna vertebral necesaria para el intercambio de información como voz, vídeo, datos y conectividad a Internet y son repositorios de gran cantidad de datos personales. La información robada podría ser utilizada para el robo de identidad, los ataques de phishing, el acceso no autorizado a sistemas, etc. Un ciberataque exitoso en un operador de telecomunicaciones también podría tener serias implicaciones como interrupción de servicios para clientes, vigilancia, cierre de servicios esenciales, entre otros. Es decir, se enfrentan a riesgos de seguridad digital desde dos flancos: potenciales ataques directos de delincuentes cibernéticos con la intención de irrumpir sus organizaciones y las operaciones de red, y potenciales ataques indirectos de aquellos en busca de información de sus usuarios.

En otras partes del mundo ya se han visto ejemplos de cómo los incidentes también afectan a los proveedores de servicios de comunicaciones. En mayo de 2017, fueron comprometidos los sistemas de Bell Canada lo cual resultó en un robo masivo de datos de más de dos millones de usuarios. Cuando la compañía se negó a pagar la recompensa, los criminales publicaron la información en línea[5]. Otro caso ocurrido en 2015, cuando mediante un ataque de denegación de servicio lograron robar datos de 1.2 millones de usuarios de la operatora Talk Talk en Inglaterra[6].

---

1 https://www.newscientist.com/article/mg23431263-500-ransomware-attack-hits-200000-computers-across-the-globe/
2 https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/
3 Nota: 143 millones de usuarios afectados, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
4 http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321
5 http://business.financialpost.com/technology/bell-canada-ignored-hackers-demand-for-ransom-then-the-private-data-of-1-9-million-customers-was-dumped-online
6 https://securelist.com/threat-intelligence-report-for-the-telecommunications-industry/75846/

No sólo las empresas y usuarios se han visto afectados. Los gobiernos cada vez toman más conciencia de la importancia del tema, y Colombia no ha sido la excepción. El creciente uso de Tecnologías de la Información y las Comunicaciones (TIC), el aumento de conexiones a Internet, la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica, y el incremento en la oferta de servicios en línea, ponen de presente que el uso exponencial del entorno digital, acarrea incertidumbres y riesgos inherentes de seguridad digital que, de no ser gestionados adecuada y oportunamente, generan el riesgo de incidentes, amenazas y ataques cibernéticos, con graves consecuencias de tipo económico o social para el país.

Teniendo en cuenta lo anterior, en 2011, el Gobierno de Colombia a través del Consejo Nacional de Política Económica y Social (CONPES), estableció los Lineamientos de política para ciberseguridad y ciberdefensa, Documento CONPES 3701, bajo los auspicios del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa Nacional, el Departamento Nacional de Planeación (DNP) y otras instituciones nacionales clave. Esta estrategia se centró en el establecimiento de instituciones nacionales necesarias para el desarrollo de la capacidad cibernética en Colombia[7].

Luego, en el año 2014, el Gobierno nacional llevó a cabo una revisión a fondo del Documento CONPES 3701 y solicitó apoyo internacional en la revisión y el desarrollo de una nueva estrategia de seguridad nacional digital. En abril de 2016, se aprobó la nueva Política Nacional de Seguridad Digital, contemplada en el CONPES 3854, el cual articula una visión estratégica en la que se alienta a los distintos actores involucrados a hacer un uso responsable del entorno digital y fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital[8].

Así, en el marco de la seguridad digital basada en la gestión de riesgos, el Documento CONPES 3854 promueve la participación de múltiples actores. Como resultado directo, Colombia es el primer país de América Latina, y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y mejores prácticas internacionales en materia de gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[9].

---

7 CONPES 3701 (2011), Lineamientos de Política Para Ciberseguridad y Ciberdefensa, disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

8 CONPES 3854 (2016), POLÍTICA NACIONAL DE SEGURIDAD DIGITAL, disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

9 Estudio del BID, MINTIC y OEA. Impacto de los incidentes de seguridad digital en Colombia 2017.

Reconociendo la importancia del sector de telecomunicaciones en materia de seguridad digital, el plan de acción del CONPES 3854 identificó que la CRC debía ajustar, dentro del marco de sus competencias, el marco normativo del sector TIC en el periodo inicial de implementación de dicha política 2017-2018 teniendo en cuenta el enfoque de gestión de riesgos de seguridad digital.

Teniendo en cuenta las funciones otorgadas a la CRC en el numeral 7 del artículo 22 de la Ley 1341 de 2009[10], la CRC está facultada para definir las normas técnicas aplicables al sector TIC, incluidas aquellas para a la protección de las comunicaciones de los usuarios, para garantizar que les sea garantizada la inviolabilidad y el secreto de las comunicaciones, el presente estudio busca determinar el rol de los operadores de telecomunicaciones en la gestión de riesgos de seguridad digital, y las medidas que deben tomarse desde el punto de vista regulatorio. Para ello se realizó un benchmark internacional con el fin de conocer las mejores prácticas de gestión de riesgos de seguridad digital, se realizaron, además, encuestas especializadas a los operadores colombianos para evaluar el estado de implementación de modelos de seguridad en sus redes, y se realizó un análisis detallado de la regulación vigente.

La encuesta a los operadores tuvo como grupo objetivo una muestra de 38 PRST, los cuales representan el 99% de la base de suscriptores del mercado; a la encuesta respondieron aproximadamente 24 PRST, siendo esta una muestra significativa, con una participación del 95% de la base de suscriptores del mercado.

En el primer capítulo de esta publicación se documentan los antecedentes y principales iniciativas de política regulatoria en materia de seguridad digital para el sector de las comunicaciones en Colombia. En el capítulo dos se recogen los informes especializados en seguridad digital con información estadística sobre los principales incidentes a nivel global y local para presentar un panorama de amenazas y riesgos de seguridad digital. En el capítulo tres se incluye un benchmarking de los marcos regulatorios adoptados en cuatro regiones del mundo y se documentan las principales iniciativas adoptadas a nivel regulatorio, específicamente para el sector de telecomunicaciones.

Luego, en el cuarto capítulo se analizan las mejores prácticas, estándares y normas internacionales para la gestión de riesgos de seguridad digital en el sector y se estiman sus niveles de adopción en Colombia a través de mediciones independientes y la encuesta de diagnóstico mencionada anteriormente. En el capítulo cinco se presenta un análisis de las previsiones de seguridad de red que aplican a los proveedores de redes y servicios de comunicaciones, y se analizan los modelos de seguridad adoptados por los operadores para su cumplimiento. Finalmente, el capítulo seis recoge los resultados de los

[10] "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional de espectro y se dictan otras disposiciones*"

análisis presentados y recomienda una serie de medidas orientadas a mejorar la capacidad de las múltiples partes interesadas para gestionar los riesgos de seguridad digital.

Abreviaturas

Anatel:	Agencia Nacional de Telecomunicaciones
APNIC:	(Asia Pacific Network Information Centre) Centro de Información de la Red de Asia Pacífico, por su sigla en inglés.
BGP:	Border Gateway Protocol
BID:	Banco Interamericano de Desarrollo
BER:	Bit Error Rate
CBL:	Composite Blocking List
CCOC:	Comando Conjunto Cibernético
CCP:	Centro Cibernético Policial
CDRs:	Charging Data Record
CE:	Comisión Europea
ColCERT:	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CONPES:	Consejo Nacional de Política Económica y Social
CRC:	Comisión de Regulación de Comunicaciones
CSRIC:	Consejo de Seguridad de Comunicaciones, Confiabilidad e Interoperabilidad
CSIRT:	(Computer Security Incident Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés.
DDoS:	De las siglas en inglés Distributed Denial of Service. Ataques Distribuidos de Denegación de Servicio.
DANE:	Departamento Administrativo Nacional de Estadística
DOS:	(Denial of Service) Denegación de Servicio, por su sigla en inglés.
ECV:	Encuesta de Calidad de Vida
ENISA:	(European Union Agency for Network and Information Security) Agencia de Seguridad de la Red y de la Información de la Unión Europea, por su sigla en inglés.
FAC:	Comités Asesores Federales
FCC:	(Federal Communications Commission) Comisión Federal de Comunicaciones, por su sigla en inglés.
GSM:	(Global System for Mobile communications) Sistema Global para Comunicaciones Móviles, por su sigla en inglés.
IETF:	(Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet, por su sigla en inglés.
IP:	Internet Protocol

Abreviaturas *(continuación)*

ISP:	Proveedores de Servicios de Internet
ISMS:	Information Security Management System
LACNIC:	(Latin America & Caribbean Network Information Centre) Registro de Direcciones de Internet para América Latina y Caribe, por su sigla en inglés.
MinTIC:	Ministerio de Tecnologías de la Información y las Comunicaciones
NAT:	Network Adress Translation
NIST:	(National Institute of Standards and Technology) Instituto Nacional de Estándares y Tecnología, por su sigla en inglés.
OCDE:	Organización para la Cooperación y el Desarrollo Económicos
OEA:	Organización de Estados Americanos
PCI DSS:	Payment Card Industry Data Security Standard
PRST:	Proveedores de Redes y Servicios de Telecomunicaciones
PUA:	Aplicaciones Potencialmente Indeseadas
RPC:	República Popular China
RPKI:	(Resource Public Key Infrastructure) Recurso de Infraestructura de Clave Pública, por su sigla en inglés.
UE:	Unión Europea
UIT:	Unión Internacional de Telecomunicaciones
UMTS:	(Universal Mobile Telecommunications System) Sistema Universal de Telecomunicaciones Móviles, por su sigla en inglés.

Glosario

Adware: es el nombre que se da a los programas diseñados para mostrar publicidad en la computadora, redirigir las solicitudes de búsqueda a sitios web de publicidad y recopilar datos de "marketing" acerca del usuario (como los tipos de sitios web que visita) para mostrar avisos personalizados

Antispoofing: es el nombre que se les da a las técnicas de rechazo de paquetes IP en los que se ha falsificado su dirección de origen.

Archivos binarios sospechosos: son archivos que contienen información en formas diferentes al texto plano, en muchas ocasiones están destinados para su uso por parte del sistema operativo o por otras aplicaciones y pueden no ser leíbles directamente por los humanos.

Botnet: la palabra Botnet se forma a partir de las palabras 'robot' y red ('net'.). Los ciberdelincuentes usan virus y troyanos especiales para infringir la seguridad de las computadoras de varios usuarios, tomar el control de cada computadora y organizar todas las máquinas infectadas en una red de "bots" que el delincuente puede administrar a distancia.

Ciberseguridad: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Ciberdefensa: es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales**.**

Código dañino: software que realiza funciones no deseadas, no solicitadas o perjudiciales en un sistema infectado.

DIAMETER: es un protocolo de red usado para los procesos de autenticación, autorización y contabilidad centralizada

DNSSEC: extensiones de seguridad del sistema de nombres de domino (DNS – Domain Name Server)

Exploits: son un subconjunto de malware. Estos programas maliciosos contienen datos o códigos ejecutables que son capaces de aprovecharse de una o más vulnerabilidades en el software local o remoto de la computadora

Firewall: una barrera que limita el acceso entre redes de acuerdo con una política local de seguridad.

HTTPS: Protocolo seguro de transferencia de hipertexto, es el protocolo de comunicaciones que garantiza la privacidad e integridad de las comunicaciones en internet a través del uso de una capa cifrada de transporte

IPv4: es la cuarta versión del sistema de direccionamiento del protocolo de Internet, una única dirección de Internet es requerida por cada host y dispositivo que se comunique usando TCP/IP, IPv4 define las direcciones IP en un formato de 32 bits**.**

IPv6: es la versión del sistema de direccionamiento del protocolo de Internet diseñado para reemplazar IPv4, define las direcciones IP en un formato de 128 bits.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.

ISO 27002: código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable.

Malware: programa que es introducido en un sistema, usualmente de manera encubierta, con la intención de comprometer la confidencialidad, la integridad o la disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o para molestar y perturbar a la víctima.

Pharming: es un tipo de ataque en el que se corrompe un servicio de infraestructura como el DNS (Domain Name Server) causando que la víctima sea redireccionada a un verificador falso, con el objetivo de obtener información sensible, o forzar la descarga de software dañino.

Phishing: correos electrónicos que suplantan destinatarios de buena reputación con el fin de inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito.

RADIUS: es el protocolo de red predecesor de DIAMETER, para los procesos de autenticación, autorización y contabilidad centralizada.

Ransomware: consiste en el secuestro del dispositivo (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

Spam: es el abuso de sistemas de mensajería electrónica para enviar de manera indiscriminada grandes cantidades de mensajes no solicitados.

Spear phishing: es una estafa focalizada por correo electrónico cuyo único propósito es obtener acceso no autorizado a datos confidenciales. A diferencia de las estafas por phishing, que pueden lanzar ataques amplios y dispersos, el spear phishing se centra en un grupo u organización específicos. La intención es robar propiedad intelectual, datos financieros, secretos comerciales o militares y otros datos confidenciales.

Spyware: es una categoría de programas maliciosos para la recolección no autorizada de la actividad y datos del usuario. Esta categoría incluye los programas que registran en un archivo las teclas pulsadas en un teclado y el envío de estos archivos a los cibercriminales, la recopilación de mensajes de correo electrónico para bases de datos de spam, etc.

Vector de ataque: es el medio o método que utiliza una amenaza para atacar un sistema.

1. ANTECEDENTES

Desde 2009, la Comisión de Regulación de Comunicaciones (CRC) ha trabajado para desarrollar un marco regulatorio adecuado en materia de seguridad digital, estos esfuerzos iniciaron con el proyecto *"Aspectos regulatorios asociados a la ciberseguridad"*[11], que culminó con la expedición de la Resolución CRT 2258 de 2009, en la cual se establecieron por primera vez las medidas que deben implementar los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) en sus redes, medidas que se mantienen vigentes actualmente.

Los principales aspectos desarrollados en la mencionada Resolución estaban orientados a establecer las características generales para garantizar la seguridad de la red y la integridad de los servicios. Específicamente, se estableció la obligación de implementar modelos de seguridad que contribuyesen a mejorar la seguridad de las redes de acceso de los proveedores de servicio de internet, de acuerdo con los marcos de seguridad definidos por la UIT en lo que respecta a las recomendaciones pertenecientes a las series X.800[12]. Inicialmente, estas medidas se encontraban dentro del Régimen de calidad vigente en ese momento (Resolución CRT 1740 de 2007).

De otra parte, en esta misma Resolución se establecieron las características generales que deben tener los modelos de seguridad de los PRST, involucrando aspectos como inviolabilidad de las comunicaciones y privacidad de los datos personales. Estas previsiones se integraron dentro del Régimen de Protección a los Usuarios vigente en ese momento (Resolución CRT 1732 de 2007[13]).

Posteriormente, en 2011, a través del CONPES 3701, Colombia adoptó una política nacional de ciberseguridad y ciberdefensa, denominada ***"Lineamientos de política para ciberseguridad y ciberdefensa"***. El objetivo general fue desarrollar una estrategia nacional que contrarrestara el incremento de las amenazas informáticas que afectaban al país e incluyera un fortalecimiento institucional y disposiciones dirigidas a diferentes entidades de gobierno.

---

11 Comisión de Regulación de Comunicaciones. (2017). *Resolución CRT 2258 de 2009*. Recuperado de https://normograma.info/crc/docs/resolucion_crc_2258_2009.htm?q=2258

12 Nota: La resolución adopta las siguientes recomendaciones:
- Autenticación: Recomendaciones UIT X.805 y UIT X.811.
- Acceso: Recomendaciones UIT X.805 y UIT X.812
- Servicio de No repudio: Recomendaciones UIT X.805 y X.813
- Principio de confidencialidad de datos: Recomendaciones UIT X.805 y X.814
- Principio de integridad de datos: Recomendaciones UIT X.805 y X 815
- Principio de disponibilidad: Recomendación UIT X.805.

13 Actualmente el Régimen de protección a los usuarios se encuentran contenido en el Título II de la Resolución compilatoria de la CRC 5050 de 2016.

El documento CONPES 3701 alcanzó un logro fundamental en el 2011 como fue la creación de la institucionalidad para la ciberseguridad y ciberdefensa del país. Esto fue posible por medio de la creación de nuevas instancias, como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, y el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, como se muestra en la **¡Error! No se encuentra el origen de la referencia.**.

Ilustración 1 Institucionalidad CONPES 3701 -2011

Fuente: CONPES 3701 de 2011

Así mismo, dentro del plan de acción asociado al CONPES 3701, se delegó a la CRC la tarea de realizar un análisis sobre los aspectos técnicos que debían cumplir los PRST para garantizar los principios de confidencialidad, integridad y disponibilidad de los datos, así como las medidas para autenticación y acceso de los usuarios a la red y el no repudio de las comunicaciones. Con base en lo que ya había sido desarrollado por la CRC en la Resolución CRT 2258 de 2009, al momento de la actualización de los Regímenes de Calidad y Protección de Usuarios (Resoluciones CRC 3067 y 3066 de 2011,

respectivamente), se mantuvieron las medidas de modelos de seguridad, inviolabilidad de las comunicaciones y privacidad de los datos[14].

Luego, en 2014, por solicitud del Presidente de la República se creó una Comisión de alto nivel con el fin de trabajar en el fortalecimiento de las políticas de ciberseguridad y ciberdefensa para el país. La Comisión fue liderada por los Ministerios de Defensa Nacional, de Justicia y del Derecho, y de Tecnologías de la Información y las Comunicaciones. Esta Comisión identificó la necesidad de incorporar nuevos elementos a las estructuras institucionales, a la legislación y a las acciones existentes, así como incluir en la política principios, lineamientos y directrices en lo relacionado con los derechos humanos en el entorno digital. Se concluyó que aunque la política existente había sido efectiva en contrarrestar incidentes digitales que atentaban contra la defensa y seguridad nacional, se hacía necesario complementar estas acciones con nuevas acciones enfocadas en las necesidades futuras en materia de seguridad digital, teniendo como meta relacionar las actividades de carácter técnico y operativo con los objetivos de prosperidad económica y social planteados en la política de Estado.

Por lo expuesto anteriormente, durante el desarrollo de la revisión de la estrategia nacional de seguridad que culminó con la expedición en el 2016 del CONPES 3854 **– *"Política Nacional de Seguridad Digital"***, se consideró que era necesario cambiar el enfoque tradicional e incluir la **gestión de riesgo** como uno de los elementos más importantes para abordar la temática, estableciendo como objetivo general: "*Fortalecer las capacidades de las múltiples partes interesadas para identificar,* ***gestionar, tratar y mitigar los riesgos de seguridad digital*** *en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país."* (NFT)

Este enfoque se encuentra alineado con las sugerencias de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que en su recomendación "*Digital Security Risk Management for Economic and Social Prosperity*"[15] de 2015 plantea que la gestión de riesgos de seguridad digital debe iniciar con la definición de los objetivos económicos y sociales de seguridad o el diseño de las actividades específicas, para luego, en la etapa conocida como gestión del riesgo, evaluar cuál es el nivel de riesgo de dicha actividad, determinando todos los resultados posibles sobre los objetivos sociales y económicos. Posteriormente, en la etapa de tratamiento del riesgo, se determina cómo deberían ser

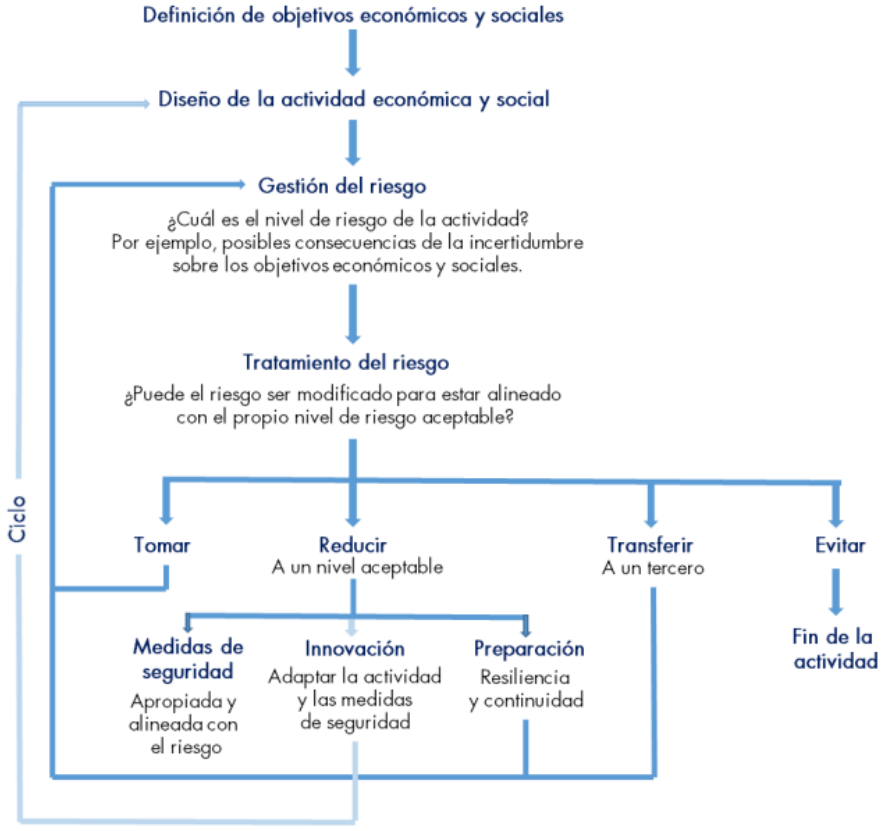
---

14 Nota: Al respecto pueden consultarse los artículos: 2.1.4.1. INVIOLABILIDAD DE LAS COMUNICACIONES, ARTÍCULO 2.1.4.2. SEGURIDAD DE LOS DATOS E INFORMACIÓN, y ARTÍCULO 5.1.2.3. SEGURIDAD DE LA RED de la Resolución compilatoria CRC 5050 de 2016.

15 OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity.* Recuperado de http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

modificadas las estrategias, con el fin de aumentar la probabilidad de éxito de la actividad y preservar los objetivos definidos, decidiendo si el riesgo debe ser tomado, reducido, transferido o evitado. Si se decide reducirlo, se pueden seleccionar y aplicar medidas de seguridad, se puede considerar la innovación, o las medidas de preparación para su tratamiento.

Ilustración 2 Modelo de gestión sistemática y cíclica de riesgos de seguridad digital



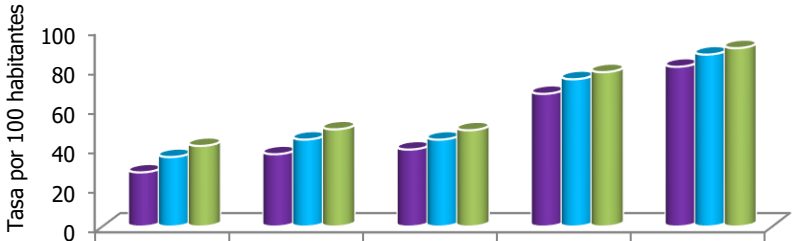
Fuente: OCDE (2015)

Este nuevo enfoque de responsabilidad compartida y gestión de riesgo se ve reflejado en el gran número de actores involucrados en el plan de acción del CONPES 3854. Por lo menos nueve entidades del gobierno tienen acciones por adelantar y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) se encuentra desarrollando un modelo de gestión de riesgos de seguridad digital para que sea adoptado a nivel nacional. A continuación se describe el estado del arte de las vulnerabilidades y amenazas a los que se enfrentan las organizaciones, así como las diversas formas de gestionar los riesgos.

2. VULNERABILIDADES Y AMENAZAS GLOBALES Y LOCALES

De acuerdo con distintas organizaciones dedicadas a la seguridad de redes de telecomunicaciones (Cisco, Kaspersky Lab, McAfee, entre otros), dichas redes se encuentran cada día más expuestas a distintas amenazas y vulnerabilidades de los ataques cibernéticos. Este comportamiento se explica en parte por el rápido crecimiento en el uso del Internet. Así, para 2016 cerca de 7 mil millones de personas alrededor del mundo vivían en un área cubierta por redes móviles, un 84% de la población mundial tenía redes de banda ancha y el número de usuarios de Internet siguió creciendo a una tasa anual cercana al 10%[16]. Bajo esta dinámica, los ciberdelincuentes cuentan con más espacio para actuar y más opciones para atacar.

Gráfica 1 Número de suscriptores de Internet móvil por cada 100 habitantes

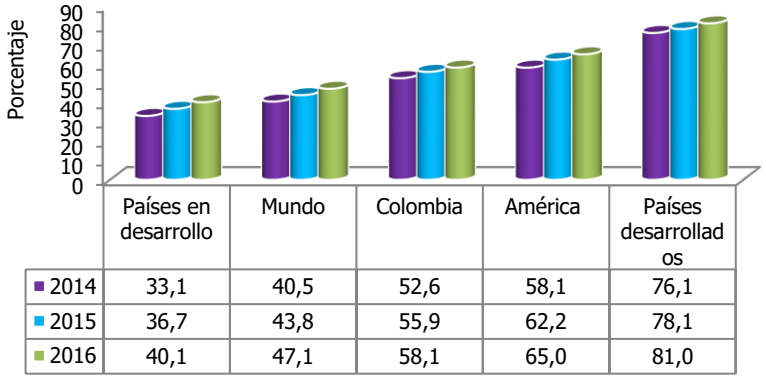


	Países en desarrollo	Mundo	Colombia	América	Países desarrollados
2014	27,5	36,7	39,1	67,3	80,9
2015	35,3	44,2	44,1	74,6	87,1
2016	40,9	49,4	48,9	78,2	90,3

Fuente: UIT y Colombia TIC. Elaboración CRC.

[16] International Telecommunication Union, ITU. (2016). *Measuring the Information Society Report 2016*. Recuperado de https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf

Gráfica 2 Porcentaje de individuos que usan Internet



	Países en desarrollo	Mundo	Colombia	América	Países desarrollados
2014	33,1	40,5	52,6	58,1	76,1
2015	36,7	43,8	55,9	62,2	78,1
2016	40,1	47,1	58,1	65,0	81,0

Fuente: UIT y DANE. Elaboración CRC.

Ahora bien, gran parte de la masificación en el uso del Internet está enfocada en el comercio electrónico. Es decir, con las actividades relacionadas con la compra y venta de productos o de servicios a través de medios electrónicos, principalmente Internet. De acuerdo con el estudio del *McKinsey Global Institute*, aproximadamente 12% del comercio mundial de bienes se realiza a través de plataformas de comercio electrónico[17]. Así mismo, se estima que el 50% del comercio mundial de servicios se realiza de manera digital[18].

En coherencia con la dinámica de crecimiento del tráfico de Internet a nivel mundial, las empresas se ven obligadas a equiparar este crecimiento con la madurez de su infraestructura de seguridad[(19)]. Así, en el estudio comparativo sobre capacidades de seguridad de Cisco de 2017[20], se mostró que las tasas de crecimiento de madurez de la seguridad son muy bajas en comparación con el crecimiento del tráfico de Internet. De igual forma, se observa en la Gráfica 3 Madurez de la seguridad y tasas de crecimiento

---

17 McKinsey Global Institute. (2016). *Digital Globalization: The New Era of Global Flows*. Recuperado de http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

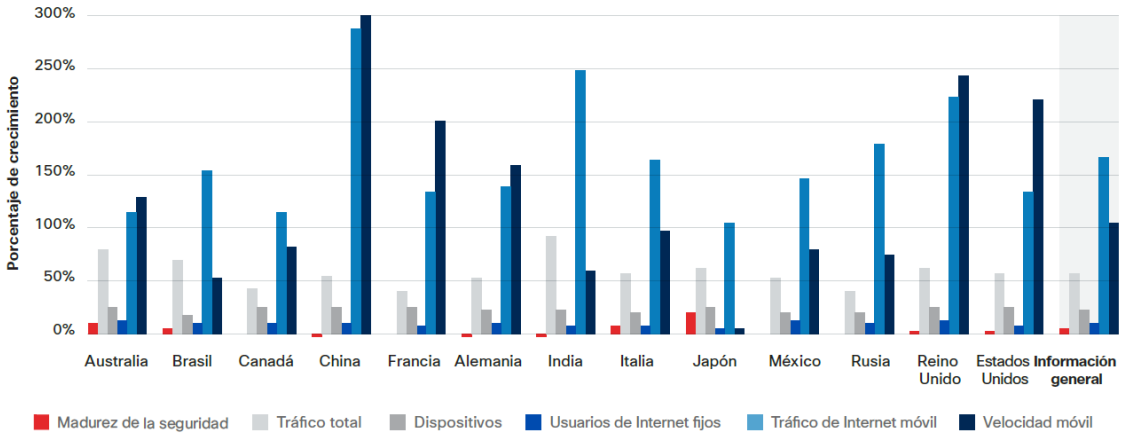
18 Information Technology and Innovation Foundation. (2015). *Cross-Border Data Flows Enable Growth in All Industries* Recuperado de http://www2.itif.org/2015-cross-border-data-flows.pdf

19 Nota: El Modelo de Madurez de Capacidad (CMM por las siglas en inglés) de Seguridad Cibernética Nacional desarrollado por el Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford evalúa la madurez de la seguridad cibernética de un país en 5 dimensiones principales: 1. Política y Estrategia; 2. Cultura y Sociedad; 3. Educación; 4. Marcos legales; y 5. Tecnologías.

20 Cisco. (2017). *Informe de ciberseguridad anual de Cisco 2017*. Recuperado de https://www.cisco.com/c/dam/m/digital/1226019/Cisco_2017_ACR_es-xl.pdf

que las velocidades de banda ancha, en concreto, están creciendo a una velocidad significativamente mayor que otras variables de redes que se muestran en la misma. Así mismo, las mayores velocidades y el aumento de dispositivos conectados generan un crecimiento de tráfico exponencial, por lo que las empresas luchan por potenciar sus medidas e infraestructuras de seguridad a una velocidad similar.

Gráfica 3 Madurez de la seguridad y tasas de crecimiento



Fuente: Cisco, Informe de ciberseguridad anual de 2017

Por tanto, es inevitable que toda esta revolución en materia de acceso a Internet llegue acompañada del incremento en el nivel de amenazas y la diversificación en las modalidades de ataque en las redes. A continuación, se muestran diversas amenazas y vulnerabilidades en las redes, así como algunos métodos de ataque y el impacto económico que los mismos generan en las empresas.

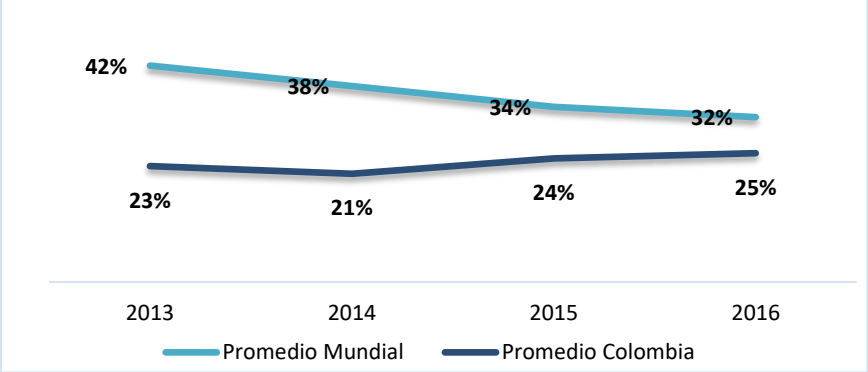
2.1. Reportes de amenazas globales

Organizaciones expertas en seguridad digital monitorean anualmente los niveles de riesgo de incidentes informáticos. Este es el caso de Kaspersky Lab, quienes realizan un análisis de amenazas en línea por país y han encontrado que los incidentes agrupan un conjunto de amenazas con código dañino[21],

21 Nota: Software que realiza funciones no deseadas, no solicitadas o perjudiciales en un sistema infectado.

ransomware[22] y cryptoware, e incluyen incidentes de phishing[23] y spearphising[24] entre otros incidentes. Los datos son obtenidos de los usuarios (corporativos y consumidores) de Kaspersky, y se integran para obtener el nivel de amenaza online, es decir, el porcentaje de usuarios que anualmente fueron infectados por lo menos una vez. Los resultados para Colombia de los últimos tres años revelan que, mientras la media mundial para este tipo de amenazas viene en constante disminución, en Colombia se han registrado aumentos de hasta 12% año a año[25], ver Gráfica 4.

Gráfica 4 Porcentaje de usuarios infectados online



Fuente: Kaspersky Lab

Ahora bien, los reportes regionales de seguridad digital[26] coinciden en afirmar que la mayor parte de los ataques reportados no son sofisticados o avanzados. Si bien es cierto que en algunas áreas los cibercriminales demuestran un alto grado de sofisticación en sus herramientas, tácticas y procesos, la mayoría de los incidentes tienen éxito por la falta de conciencia y malas prácticas de los usuarios finales.

22 Nota: Consiste en el secuestro del dispositivo (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

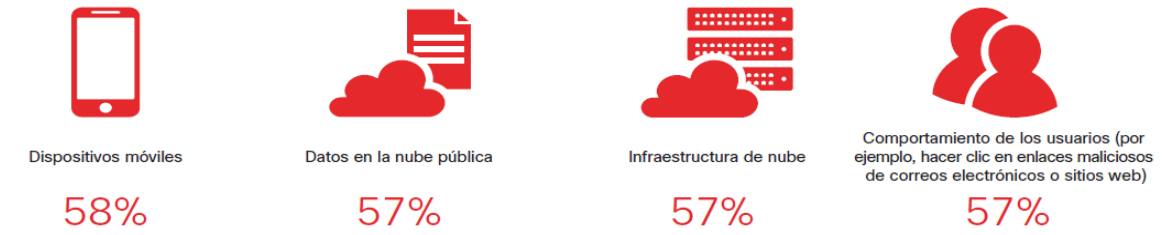
23 Nota: Correos electrónicos que suplantan destinatarios de buena reputación con el fin de inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito.

24 Nota: Spear phishing es una estafa focalizada por correo electrónico cuyo único propósito es obtener acceso no autorizado a datos confidenciales. A diferencia de las estafas por phishing, que pueden lanzar ataques amplios y dispersos, el spear phishing se centra en un grupo u organización específicos. La intención es robar propiedad intelectual, datos financieros, secretos comerciales o militares y otros datos confidenciales.

25 Kaspersky Lab. (2013, 2014, 2015 y 2016). *Security Bulletins*. Recuperado de http://media.kaspersky.com/pdf/KSB_2013_EN.pdf, https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf, https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf, https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf

26 Nota: Referente a la Tricotomía del delito, en donde se estipula que, a mayor volumen de ataque se realiza a víctimas con bajos niveles de seguridad con métodos poco sofisticados explotando vulnerabilidades ampliamente documentadas. IOCTA 2016 (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency de EUROPOL.

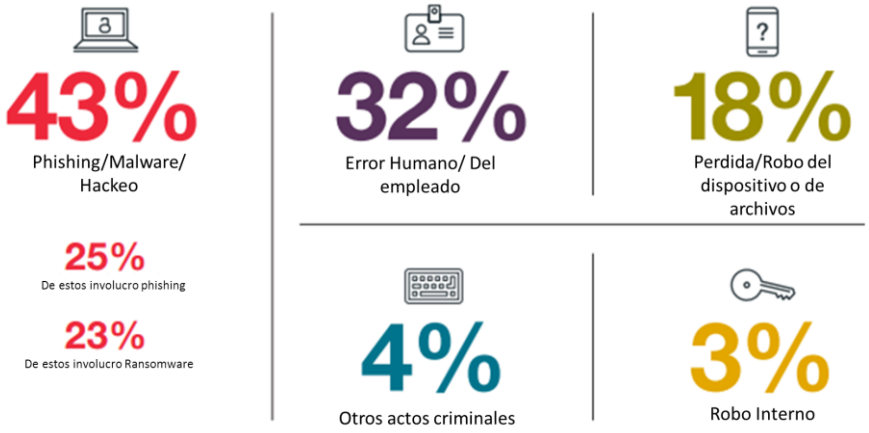
Ilustración 3 Mayores fuentes de preocupación de los profesionales de la seguridad en relación con los ciberataques



Fuente: Cisco, Informe de ciberseguridad anual de 2017 - Estudio comparativo sobre capacidades de seguridad de Cisco 2017

La firma norteamericana especializada en seguridad digital, BakerHostetler, realiza anualmente un análisis de las causas de infección para los incidentes gestionados en el sector privado. En el reporte de 2017, se evidencia que el 32% de los incidentes tienen origen directo en error humano. Si suman los casos de phishing, el error humano representa el 43% del total de incidentes gestionados.

Ilustración 4 Causas de Incidentes de seguridad digital en el sector privado



Fuente: BakerHostetler, Data Security Incident Response Report, 2017

Otro método de ataque son los archivos binarios sospechosos[27] de Windows y las aplicaciones potencialmente indeseadas (PUA) los cuales encabezaron la lista de métodos de ataque en la Web en 2016 (Cisco, 2017), ver Ilustración 5. Los archivos binarios sospechosos de Windows contienen amenazas, como spyware[28] y adware[29]. Las extensiones maliciosas de navegador son un ejemplo de PUA.

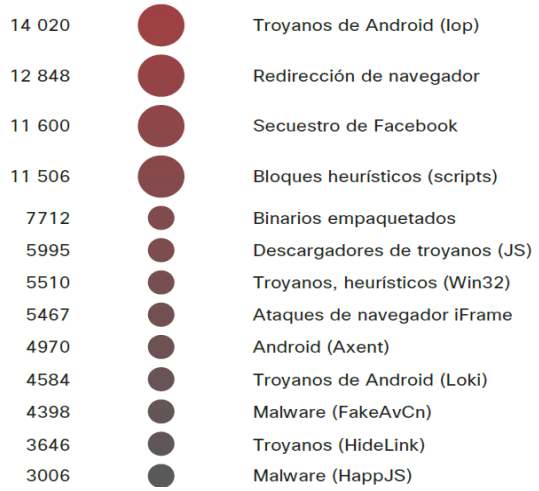
Ilustración 5 Malware[30] más frecuente

27 Nota: Los archivos binarios son archivos que contienen información en formas diferentes al texto plano, en muchas ocasiones están destinados para su uso por parte del sistema operativo o por otras aplicaciones y pueden no ser leíbles directamente por los humanos, Definición del *Linux Information Project*.

28 Nota: Es una categoría de programas maliciosos para la recolección no autorizada de la actividad y datos del usuario. Esta categoría incluye los programas que registran en un archivo las teclas pulsadas en un teclado y el envío de estos archivos a los cibercriminales, la recopilación de mensajes de correo electrónico para bases de datos de spam, etc.

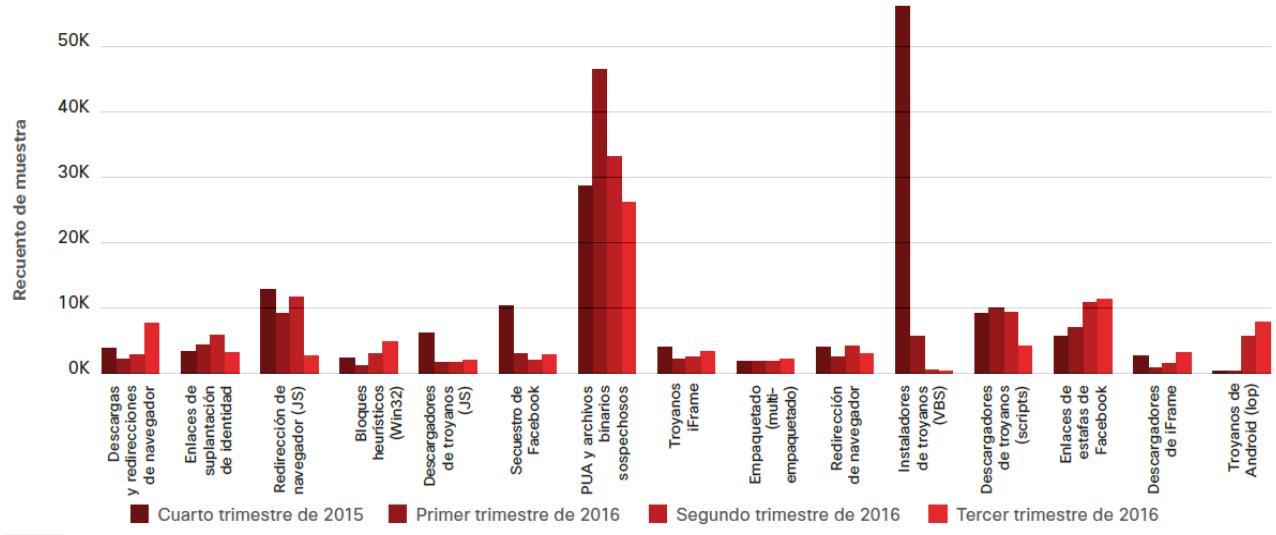
29 Nota: Adware es el nombre que se da a los programas diseñados para mostrar publicidad en su computadora, redirigir sus solicitudes de búsqueda a sitios web de publicidad y recopilar datos de "marketing" acerca de usted (como los tipos de sitios web que visita) de manera de poder mostrar avisos personalizados https://latam.kaspersky.com/resource-center/threats/adware

30 Tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.



Fuente: Cisco, Informe de ciberseguridad anual de 2017

Gráfica 5 Malware más frecuente (evolución)



Fuente: Cisco, Informe de ciberseguridad anual de 2017

> *"Desde finales de 2015 los adversarios han cambiado la fase de reconocimiento de ataques basados en la Web, es así como cada vez más amenazas buscan los navegadores y los plugins vulnerables. Según los investigadores de Cisco, este cambio es coherente con la dependencia cada vez mayor de los adversarios en el malware, ya que cada vez es más difícil abarcar un número de usuarios a través de los vectores de ataque en la Web tradicionales".* (Cisco, Informe de Ciberseguridad anual de 2017).

Por otro lado, en el reporte de seguridad digital de Symantec de 2016[31] se identificó que el correo electrónico continúa siendo un medio importante de amenaza para los ciberatacantes y ha tenido un resurgimiento como vector de ataque[(32)]. Durante ese periodo, 1 de cada 131 correos electrónicos enviados fue malicioso, la cifra más alta en los últimos 5 años. El reporte atribuye este incremento al hecho que la entrega a través de email no depende de vulnerabilidades, sino que utiliza el engaño para que la víctima abra archivos adjuntos, enlaces o entregue credenciales. Toda la familia de ataques de *phishing y spearphishing* se apoyan en los malos hábitos de los usuarios. Asimismo, el correo electrónico fue el vector original favorito para la distribución de ransomware.

> *"La tendencia de camuflar los envíos maliciosos masivos como correspondencia de negocios ha venido creciendo. Ahora los spammers no se limitan a imitar el estilo de las cartas de negocios, sino que con frecuencia usan los datos reales de compañías existentes, copian sus firmas y logotipos, y hasta los temas de los mensajes puede corresponder al perfil de la compañía".* Kaspersky Lab. (2017). Spam y Phishing en el segundo trimestre de 2017. Recuperado de https://securelist.lat/spam-and-phishing-in-q2-2017/85433/

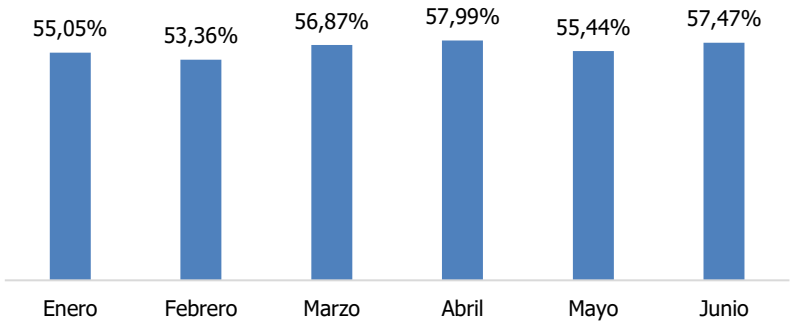
En línea con los ataques por medio del correo electrónico, los ciberpiratas siguen actuando a través de lo que se conoce como "*spam*" o correo basura. En el informe trimestral 2017 sobre spam que publica Kaspersky Lab, se explica que el envío de archivos con contraseña persigue dos objetivos al mismo tiempo, el primero, es ingeniería social: en el mensaje los delincuentes hacen ahínco en que son datos confidenciales (por ejemplo, cuentas) y están protegidos adicionalmente por contraseñas, y segundo, el antivirus no puede hacer un análisis completo de los archivos mientras no los descomprima. Como se puede observar en cifras, más de la mitad del tráfico de correos corresponden a spam.

---

31 Symantec Corporation. (2017). *Internet security threat report*. Recuperado de https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq

32 Nota: Un vector de ataque es el medio o método que utiliza una amenaza para atacar un sistema.

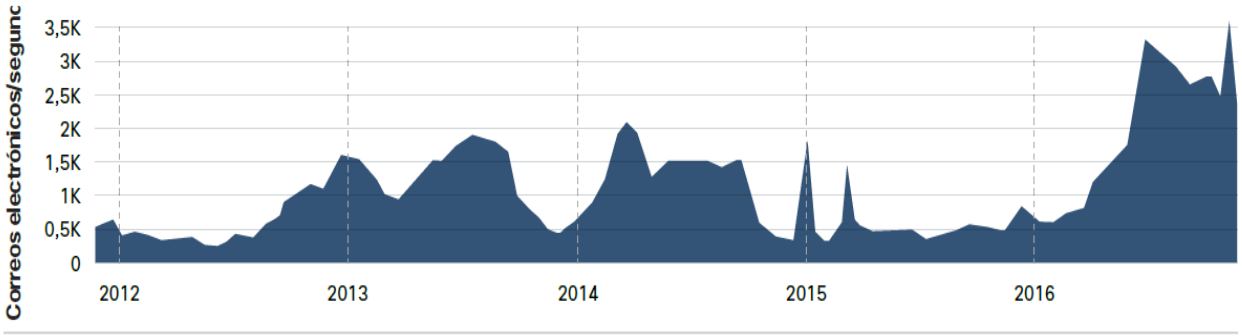
Gráfica 6 Porcentaje de spam en el tráfico de correo - 2017



Fuente: Kaspersky Lab. Elaboración: CRC

Así mismo, la gran cantidad de spam que ingresa vía correo electrónico genera una gran preocupación por parte de los profesionales de la seguridad. Así, en la Gráfica 7 se observa en un periodo de cinco años de Composite Blocking List (CBL), es decir *una "lista negra" basada en DNS de las infecciones informáticas sospechosas de envío de spam*, un significativo aumento en el volumen total de spam durante el año 2016, los investigadores de amenazas atribuyen este comportamiento a la botnet[33] Necurs[34].

Gráfica 7 Volumen Total de Spam



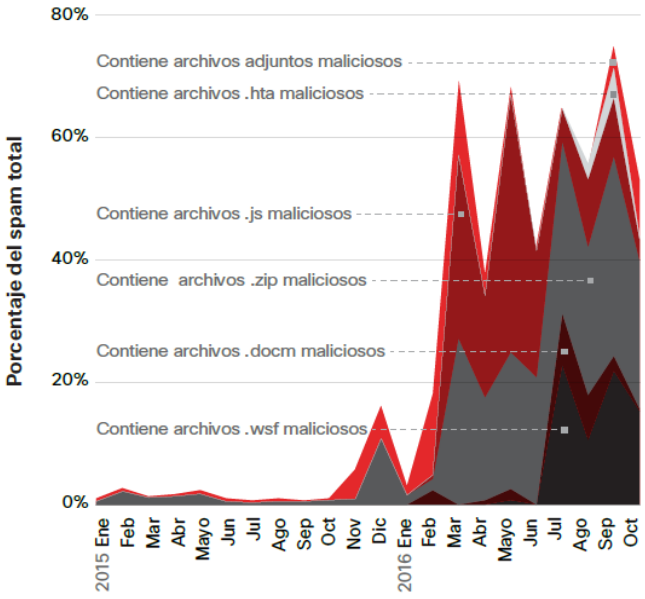
Fuente: Cisco, Informe de ciberseguridad anual de 2017 - Composite Blocking List (CBL)

33 Nota: La palabra Botnet se forma a partir de las palabras 'robot' y red 'net'. Los ciberdelincuentes usan virus y troyanos especiales para infringir la seguridad de las computadoras de varios usuarios, tomar el control de cada computadora y organizar todas las máquinas infectadas en una red de "bots" que el delincuente puede administrar a distancia, tomado de: https://usa.kaspersky.com/resource-center/threats/botnet-attacks

34 Nota: Necurs es uno de los principales vectores del ransomware Locky. También distribuye amenazas como el troyano bancario Dridex.

"Los operadores de spam malicioso experimentaron con el uso de archivos .docm, JavaScript, .wsf y .hta entre el 2015 y el 2016, ver Gráfica 8*. Y, en línea con lo anterior, muchos de estos tipos de archivos están relacionados con el spam enviado por la botnet Necurs. Los patrones con archivos .wsf durante 2016 proporcionan un ejemplo de cómo los adversarios evolucionan sus tácticas de spam malicioso con el transcurso del tiempo".* (Cisco, 2017, Informe de Ciberseguridad anual de 2017).

Gráfica 8 Porcentaje de spam total que contiene archivos adjuntos maliciosos



Fuente: Cisco, Informe de ciberseguridad anual de 2017

Ahora bien, respecto a las alertas principales de brotes de amenazas, en la Gráfica 9 se observa los mensajes de spam y suplantación de identidad presenciados que los ciberdelincuentes actualizaban de forma repetida en 2016 con el objetivo de cruzar los controles y reglas de seguridad del correo electrónico:

Gráfica 9 Alertas principales de brotes de amenazas

Versión	Identificador de publicación	Nombre y URL de publicación	Resumen de mensajes	Tipo de Archivo Adjunto	Idioma	Fecha de publicación más reciente
96	35656	RuleID4626	Factura, pago	.zip	Alemán, inglés	25/04/2016
87	34577	RuleID10277	Pedido de compra	.zip	Alemán, inglés	02/06/2016
82	36916	RuleID4400KVR	Pedido de compra	.zip	Inglés	01/02/2016
74	38971	RuleID15448	Pedido de compra, pago, recepción	.zip, .gz	Inglés	08/08/2016
72	41513	RuleID18688	Pedido, pago, seminario	.zip	Inglés	01/09/2016
70	40056	RuleID6396	Pedido de compra, pago, recepción	.rar	Inglés	07/06/2016
66	34796	RuleID5118	Pedido de producto	.zip	Alemán, inglés	29/09/2016
64	39317	RuleID4626 (continuación)	Factura, pago, envío	.zip	Inglés, alemán, Español	28/01/2016
64	36917	RuleID4961KVR	Confirmación, pago/ transferencia, pedido, envío	.zip	Inglés	08/07/2016
63	37179	RuleID13288	Aviso de entrega, comparecencia ante el tribunal, factura	.zip	Inglés, Español	21/07/2016
61	38095	RuleID858KVR	Envío, presupuesto, pago	.zip	Inglés	01/08/2016
58	39150	RuleID4961KVR	Solicitud de presupuesto, pedido de producto	.zip	inglés, Alemán, Varios idiomas	25/01/2016
47	41886	RuleID4961	Transferencia, envío, facturación	.zip	Inglés, alemán, Español	22/02/2016

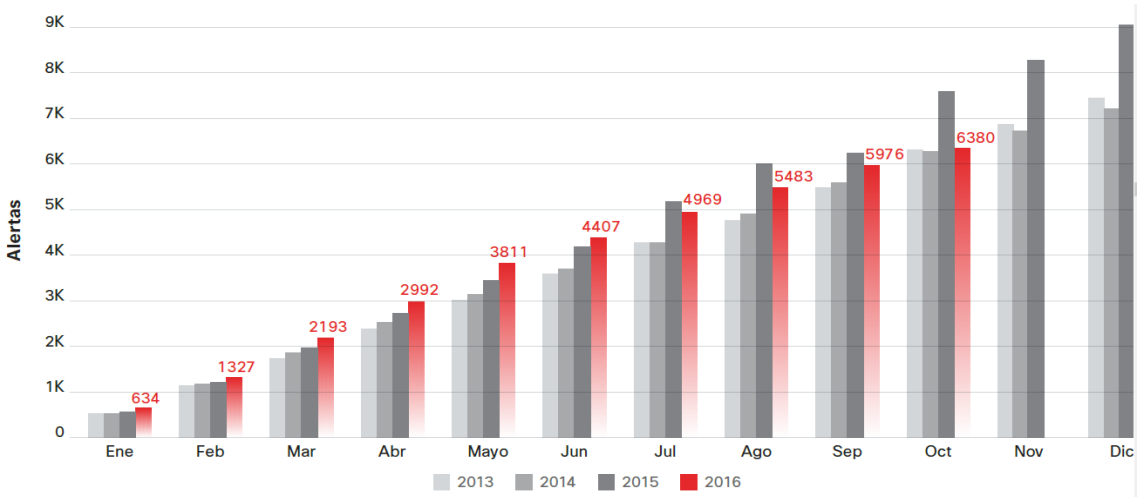
Fuente: Cisco, Informe de ciberseguridad anual de 2017

Por otro lado, software como el adware ha cobrado mucha relevancia, al punto de lograr que 75% de organizaciones se vean afectadas por infecciones de este tipo de software. Investigaciones como la de Cisco, revelan que los ciberdelincuentes utilizan el adware para:

- Inyectar publicidad, lo que puede provocar infecciones o una mayor exposición a los exploit kits (Los exploits son un subconjunto de malware. Estos programas maliciosos contienen datos o códigos ejecutables que son capaces de aprovecharse de una o más vulnerabilidades en el software local o remoto de la computadora)
- Cambiar la configuración del navegador y el sistema operativo para debilitar la seguridad
- Fracturar el antivirus u otros productos de seguridad
- Obtener el control completo del host para poder instalar otro software malicioso
- Realizar un seguimiento de los usuarios según su ubicación, identidad, servicios utilizados y lugares visitados habitualmente
- Extraer información como datos personales, credenciales e información de infraestructura (por ejemplo, las páginas de ventas internas de una empresa). (Cisco, 2017).

Finalmente, se observa que solo a partir de la segunda mitad de 2016 (ver Gráfica 10) las vulnerabilidades divulgadas por proveedores, como los de Cisco, descendieron significativamente en contraste con 2015. La National Vulnerability Database (base de datos de vulnerabilidades de Estados Unidos) muestra una dinámica similar.

Gráfica 10 Número total de alertas acumuladas anuales



Fuente: Cisco, Informe de ciberseguridad anual de 2017

2.2. Amenazas y Vulnerabilidades en Colombia

Al indagar sobre las diferentes formas de ataques cibernéticos en el país y sobre la defensa ante amenazas de los ciberpiratas, se encontraron dos investigaciones que reflejan el estado actual de esta problemática en Colombia. Por un lado, se encuentra el estudio *"Impacto de los incidentes de seguridad digital en Colombia 2017*[35]*"*, publicación auspiciada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC), la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID). Por otro lado, el Centro Cibernético Policial (CCP) de Colombia publica anualmente el informe *"Amenazas del Cibercrimen en Colombia*[36]*".*

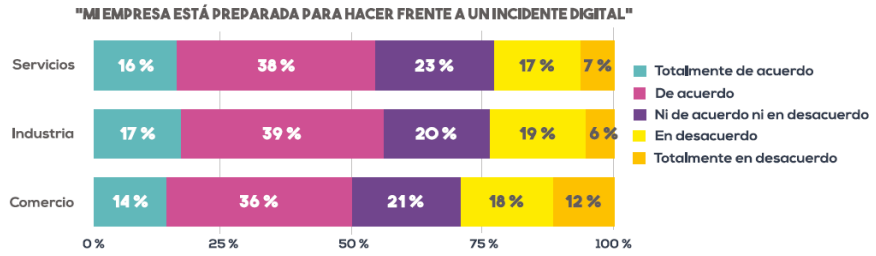
[35] MinTIC, OEA y BID. (2017). Recuperado de https://publications.iadb.org/bitstream/handle/11319/8552/Impacto_de_los_incidentes_de_seguridad_digital.pdf?sequence=1&isAllowed=y

[36] Centro Cibernético Policial. (2017). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

María Paz y Paz, Secretaria de Seguridad Multidimensional de la OEA: *"Las amenazas de ciberseguridad son ahora una parte de nuestra realidad cotidiana. Las naciones soberanas deben considerar ahora su desarrollo y sus inversiones económicas en el marco de un mundo digital. Según cálculos del sector, el gasto mundial en productos y servicios de seguridad de la información llegará a USD $86.400 millones en 2017, un incremento del 7% desde 2016, con un gasto esperado de USD $93.000 millones en 2018. Más alarmante es el hecho de que se prevé que el gasto mundial en productos y servicios de seguridad digital exceda USD $1 billón en los próximos cinco años. 2017-2021"*

Específicamente, el estudio[37] ***"Impacto de los incidentes de seguridad digital en Colombia 2017"***, expone información sobre las amenazas para la seguridad digital en el país, lo cual permite entrever los ataques que sufren tanto el sector público como el privado, así como su nivel de preparación para defenderse de dichos ataques (ver Gráfica 11). Una de las primeras indagaciones de la encuesta tuvo el objetivo de conocer si las organizaciones colombianas creen que están preparadas para hacer frente a un incidente[38] digital, un promedio simple del 37% de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) respondieron que estaban preparadas para manejar un incidente digital.

Gráfica 11 Nivel de preparación para hacer frente a un incidente digital por sector económico



Número de observaciones: 486

Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

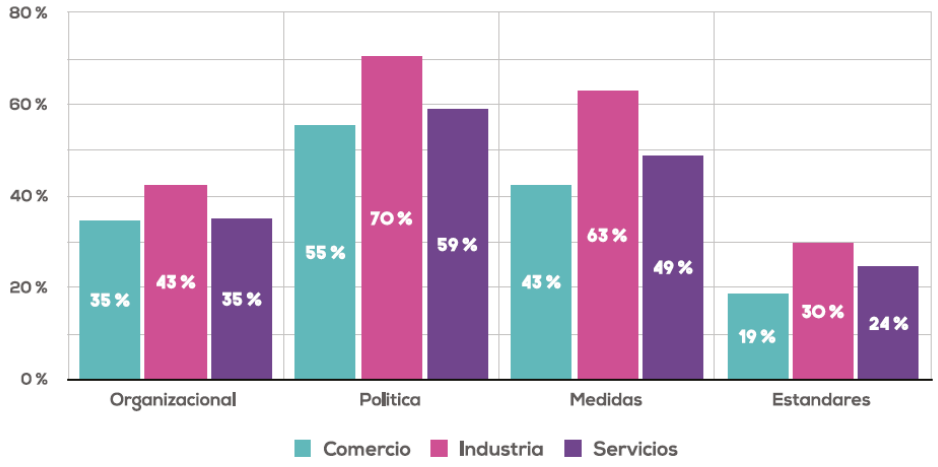
37 Nota: "*Las entidades colombianas que participaron del estudio presentan, en su mayoría, un alto nivel de conectividad. De las empresas entrevistadas, 65% indicaron que entre el 81% y el 100% de su fuerza laboral contaba con acceso a Internet. En el sector público, 69% de las entidades participantes indicaron que entre el 81% y el 100% de sus empleados tenían acceso a Internet en el trabajo".*

38 «incidente»: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

*"Un aspecto importante de la preparación cibernética son las **medidas implementadas**, ya sea que se trate de políticas, medidas técnicas o normas. Con el fin de entender estos ejemplos, se enumeran a continuación:*
1. Organizacional (ej. área, departamento dedicado a la seguridad digital, jefe de seguridad de la información, roles asociados a la seguridad de la información, funciones en torno a la seguridad de la información)
2. Política (ej. política de acceso al sistema, política de actualización de contraseñas, concientización)
3. Medidas técnicas (ej. pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI)
4. Estándares (ej. ISO 27001, otros estándares internacionales)". (MinTIC, OEA y BID, 2017, Impacto de los incidentes de seguridad digital en Colombia 2017).

Otra pregunta enfocada en las medidas implementadas en las empresas fue: *¿Cuáles de las siguientes prácticas en seguridad digital (seguridad digital y/o seguridad de la información) son implementadas por su entidad/empresa?,* un gran número respondió que había implementado medidas de política (55% del sector Comercio, 70% del sector Industria y 59% del sector de Servicios, ver Gráfica 12), le siguen en su orden la implementación de estándares técnicos (ej. ISO 27001, otros estándares internacionales).

Gráfica 12 Prácticas en seguridad digital por sector

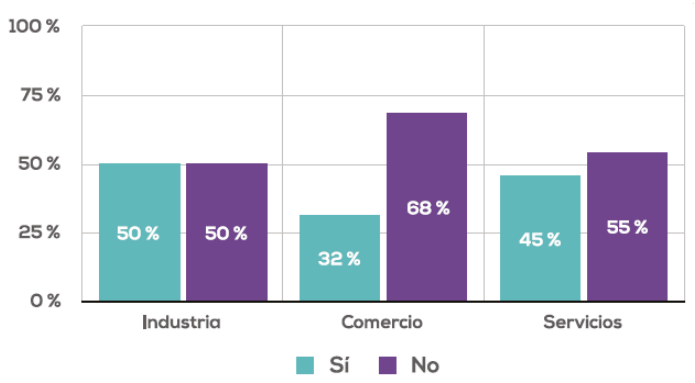


Número de observaciones: 554

Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

Por otro lado, en relación con las prácticas organizacionales, cuando se indagó sobre si las organizaciones emprendían o no la evaluación del riesgo de la seguridad digital, los resultados arrojaron que el 50% del sector Industria no lo hicieron, en contraste con el 32% y el 45% de los sectores Comercio y de Servicios que sí realizaron una evaluación del riesgo de seguridad digital, respectivamente, ver Gráfica 13.

Gráfica 13 Evaluación del riesgo cibernético por sector económico



Número de observaciones: 439

Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

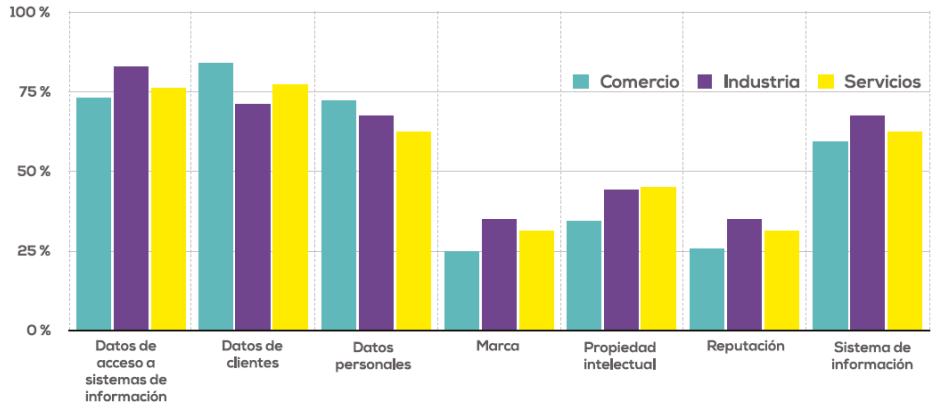
"Según lo establecido por el Marco de Seguridad Digital del Instituto Nacional de Estándares y Tecnología (NIST, por su sigla en inglés), la realización de una evaluación de riesgos típicamente incluye los siguientes seis pasos:

1. *Identificar y documentar vulnerabilidades de los Activos.*
2. *Identificar y documentar las amenazas internas y externas.*
3. *Adquirir información sobre amenazas y vulnerabilidades de fuentes externas.*
4. *Identificar posibles impactos comerciales y probabilidades.*
5. *Determinar el riesgo empresarial revisando amenazas, vulnerabilidades, probabilidades e impactos.*
6. *Identificar y priorizar las respuestas de riesgo."*

Con el propósito de conocer la valoración que tienen las empresas respecto al cuidado de la información comercial y de datos personales, la encuesta de la OEA realizó la siguiente pregunta*: ¿A la hora de protegerse frente a incidentes digitales, amenazas cibernéticas y/o ataques cibernéticos, cuáles de estos datos y/o activos de información son priorizados por su entidad/empresa?*, un gran número argumentó

que darían prioridad a Datos de acceso a sistemas de información (por ejemplo: contraseñas, tokens, credenciales) y Datos de clientes, ver Gráfica 14.

Gráfica 14 Datos y Activos priorizados por las empresas (2016)

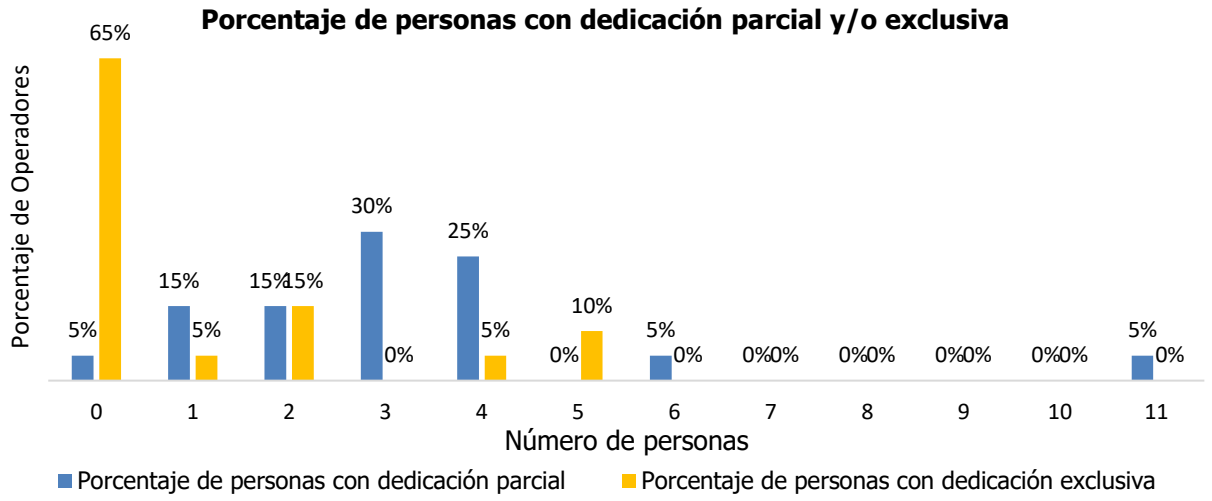


Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

Por otro lado, respecto a la pregunta *¿Tiene su entidad/empresa un área, cargo (s) o rol(es) dedicado(s) a la seguridad digital (seguridad digital y/o de seguridad de la información)?,* con un porcentaje del 54, el sector Industria respondió que cuentan con un equipo de dedicación exclusiva, frente al 45% y el 42% de las empresas de los sectores de Servicios y Comercio, respectivamente. En la misma línea, encontraron que la falta de personal con dedicación exclusiva al área y la falta de presupuesto son los principales determinantes que afectan la capacidad de abordar la seguridad digital.

En particular, la encuesta realizada por la CRC a los proveedores de Internet en Colombia revela que solo un 30% de los operadores tienen un equipo de respuesta a incidentes. Ahora bien, para aquellos que cuentan con un equipo de respuesta, la encuesta arrojó que el 65% de los operadores no dedica ninguna persona exclusivamente al tratamiento de incidentes informáticos. Por su lado, el 30% de los operadores dedica 3 personas en promedio, de forma parcial, a la gestión de incidentes de seguridad informática (ver Gráfica 15). *Para mayor información sobre las áreas dedicadas a la seguridad digital en Colombia ver ANEXO 1. ENCUESTA: DIAGNÓSTICO SEGURIDAD DIGITAL CRC*

Gráfica 15 Miembros del equipo CSIRT responsables de la gestión de incidentes de seguridad informática



Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

Por último, y con el objetivo de identificar los ataques a los cuales se ven expuestas las organizaciones en Colombia, el estudio de la OEA interrogó sobre los tipos de incidentes o amenazas cibernéticas que han experimentado las empresas en el país durante 2016, a lo cual, por ejemplo, el sector servicios respondió que el malware y el phishing se encontraban entre los tipos de incidentes más comunes, donde el 50% de los que contestaron argumentaron un incremento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio.

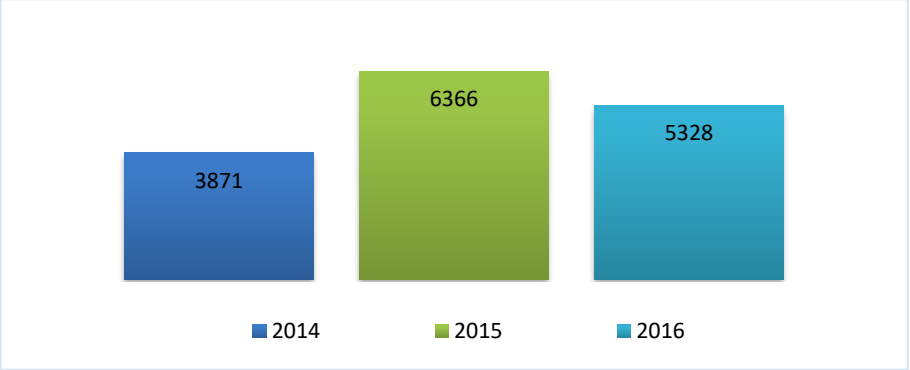
Ahora bien, al comparar la información de la encuesta de la OEA con el informe ***"Amenazas del Cibercrimen en Colombia 2016 – 2017"***[39], del CCP, también se corrobora que el número de denuncias cibernéticas sigue en aumento, así como el número de ataques de malware. A continuación se describen las principales cifras del documento del CCP, las cuales muestran el estado del arte de la ciberdelincuencia en Colombia.

El informe de amenazas del cibercrimen en Colombia de 2017, publicado por el Centro Cibernético Policial (CCP). Revela que este organismo recibió un total de 15.565 denuncias de incidentes informáticos en el país durante el periodo enero 2014 - marzo 2017. A su vez, entre el año 2014 y 2015 se presentó un incremento del 64% en el número de incidentes denunciados. Si bien para el periodo

[39] Ibid. [36]

de 2016 se registró una disminución del 16% (ver Gráfica 16), éste se atribuye principalmente a un cambio en las modalidades de cibercrimen, pues mientras en el 2014 el 92% de las denuncias presentadas afectaban a los ciudadanos y solo el 8% correspondía a denuncias del sector empresarial y de gobierno, las denuncias para 2016 muestran que el 66% de las denuncias afectaron a los ciudadanos y el 34% restante corresponde al sector empresarial y gobierno. Lo anterior evidencia la tendencia de los delincuentes en los últimos años de atacar entidades privadas y públicas que generan mayores retornos que los ataques a ciudadanos del común.

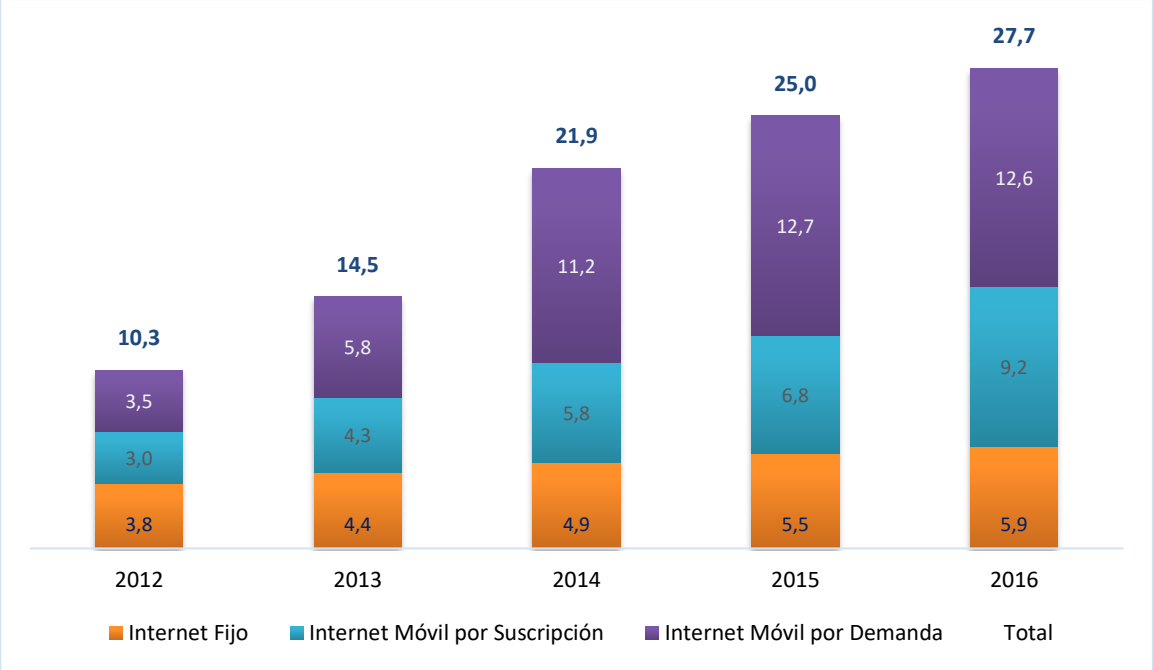
Gráfica 16 Denuncias de incidentes informáticos recibidos por el CCP



Fuente: Estadísticas del Centro Cibernético Policial

Al indagar por las posibles causas del incremento en el nivel de amenazas y la diversificación en las modalidades de ataque en Colombia, debe recordarse que durante los últimos cinco años, Colombia ha sido protagonista de una revolución en materia de acceso a internet, registrando una tasa de crecimiento promedio anual de 12% para las conexiones fijas y de 38% para conexiones móviles (ver Gráfica 17). Esta tendencia ha estado acompañada de un crecimiento en el uso de servicios soportados en Internet. La Encuesta de Calidad de Vida -ECV- realizada por el DANE muestra la evolución de los usos dados al Internet por parte de los colombianos, y aunque el mayor porcentaje de uso se atribuye a las redes sociales, la mensajería y la obtención de información, los colombianos también utilizan Internet para realizar trámites con organismos gubernamentales, comprar bienes y servicios, y utilizar servicios de banca electrónica.

Gráfica 17 Evolución de suscripciones a Internet en Colombia (Millones de conexiones)



Fuente: Colombia TIC. Elaboración CRC.

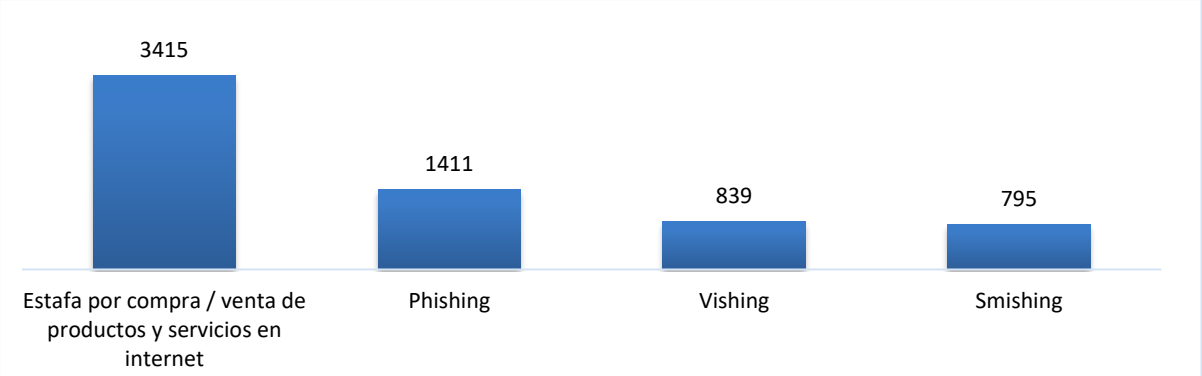
En particular, el estudio sobre comercio electrónico[40] realizado por la CRC en 2016 y publicado en abril de 2017 da cuenta de un acelerado ritmo de crecimiento para este tipo de transacciones. Según el estudio el 76.4% de los más de 33 millones de ciudadanos mayores de 18 años en Colombia, es decir tres de cada cuatro personas, están conectados a Internet.

Sin duda, la confianza en el entorno digital determina en muchas ocasiones la disponibilidad de los usuarios a utilizar Internet para realizar transacciones en línea. Así, el 59,4% de las personas que no realizan actividades de comercio electrónico adujeron la desconfianza como principal razón para no hacerlo, bien sea en el momento de entregar sus datos personales o financieros, o en el momento del pago.

Esta tendencia es coherente con los hallazgos del CCP que identificaron los incidentes ligados al comercio electrónico como la principal afectación a usuarios finales durante el 2016 (ver Gráfica 18).

[40] Comisión de Regulación de Comunicaciones. (2017). *El Comercio Electrónico en Colombia, Análisis Integral y Perspectiva Regulatoria*. Recuperado de https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf

Gráfica 18 Incidentes digitales reportados al CCP por los usuarios finales - 2016



Fuente: CCP, Amenazas del Cibercrimen en Colombia 2016 – 2017

Finalmente, debe anotarse que este incremento en la penetración, sumado a la diversificación en el uso de internet, eleva el nivel de riesgo de amenazas cibernéticas, puesto que incrementa la superficie de ataque[41] disponible para vulnerabilidades e incidentes digitales.

Problemática suplantación de SIM cards – Autenticación de dos factores a través de número celular

De otro lado, como se indicó previamente en cuanto a incidentes, las transacciones de comercio electrónico tienen una alta incidencia y es aquí donde prácticas que refuercen la seguridad en las transacciones en línea revisten la mayor importancia.

Por ejemplo, en el sector bancario el método de autenticación de dos factores corresponde a buenas prácticas en materia de seguridad en banca online. En este caso no basta con que mediante una conexión se dispongan transacciones (pagos, transferencias), sino que requiere una segunda confirmación, ya sea por una segunda clave generada en el mismo banco, o por un factor externo tal como la generación y envío de una clave de único uso (OTP) a un correo electrónico o a un número móvil registrado (ver Ilustración 6).

41 Nota: La superficie de ataque de un sistema se define como aquella parte del sistema que se encuentra expuesta al acceso o modificación por parte de usuarios no autorizados, más información en: https://www.owasp.org/index.php?title=Attack_Surface_Analysis_Cheat_Sheet&oldid=156006

Ilustración 6 Autenticación de dos factores a través de SMS en portales y servicios de Internet

Es importante reconocer que el uso de mensajes de texto SMS al número celular como método de autenticación de dos factores se ha convertido en una medida de seguridad estándar en numerosos portales y plataformas en Internet, por lo que eventuales protocolos inadecuados son un factor de riesgo para los servicios del entorno digital.

Con el objetivo de indagar sobre el estado de la suplantación de SIM cards en los operadores en Colombia, la encuesta de diagnóstico realizada por la CRC a los PRST de servicios móviles en Colombia revela que los operadores tramitan, dependiendo de su base de usuarios, entre 4.000 y 80.000 trámites de reposición de SIM card mensualmente. Este procedimiento es el punto al cual un potencial ciberdelincuente interesado en sobrepasar la autenticación de dos factores a través del número celular podría recurrir. Sin embargo, a la pregunta, *¿Cuántos reportes de fraude de suplantación de SIM card se tramitaron en promedio mensualmente?* los PRSTM manifestaron recibir un número muy bajo de reportes de fraude, entre 0 y 170 reportes mensuales.

Teniendo en cuenta que todos los PRSTM manifestaron, además, realizar una verificación documental y algunos incluso verificación contra centrales de riesgo para la reposición de SIM card, es posible formular la hipótesis que para la suplantación de tarjetas SIM los ciberdelincuentes cuentan ya con un insumo importante de datos personales de la víctima, por lo que antes de evaluar potenciales modificaciones a los procedimientos de entrega de SIM cards es necesario identificar los puntos de vulneración de datos personales de las víctimas, en primera instancia.

2.3. Impactos económicos de los ataques sobre ciberseguridad

Los efectos de los incidentes de seguridad digital han sido ampliamente estudiados a nivel global y local. Así, informes como el de ***Ciberseguridad anual de 2017*** de Cisco, ***Impacto de los incidentes de seguridad digital en Colombia 2017*** del MinTIC, la OEA y el BID, y por último, el del CCP de Colombia, ***Amenazas del Cibercrimen en Colombia 2016 – 2017***, dejan entrever los costos y pérdidas económicas que arrojan los ciberataques en las organizaciones. Por ejemplo, en el reporte de 2017[42] que Cisco realiza anualmente sobre ciberseguridad, se evidencia que las brechas de seguridad digital en las organizaciones implican pérdidas económicas directas, así como costos indirectos en tiempo y clientes, además de pérdidas económicas por indisponibilidad de servicios soportados en línea.

De acuerdo con algunos de los resultados del informe en mención, el 29% de los profesionales de seguridad consultados manifestaron que sus organizaciones sufrieron una pérdida en ganancias como resultado de los ataques; de ese grupo, el 38% dijo que esa pérdida de ganancias fue del 20% o más (ver Ilustración 7).

Ilustración 7 Porcentaje de la pérdida de ingresos organizativa como resultado de un ataque

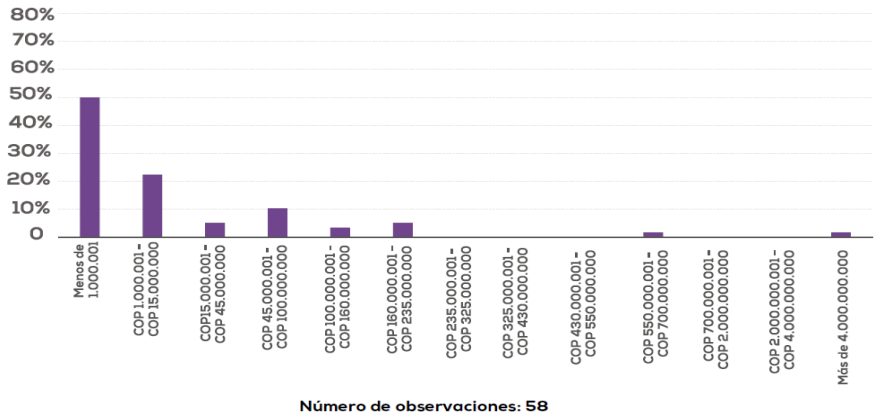
Fuente: Informe de ciberseguridad anual de Cisco 2017 - Estudio comparativo sobre capacidades de seguridad de Cisco 2017

[42] Cisco. (2017). Anual Cybersecurity Report. Recuperado de: http://www.cisco.com/c/dam/m/digital/1226019/Cisco_2017_ACR_es-xl.pdf

> ***Costos del Cibercrimen****: El Cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año, el 16% del costo total mundial del delito.* Fuente: CCP (2017), Amenazas del Cibercrimen en Colombia 2016-2017.

Específicamente para el caso colombiano, los resultados de la encuesta, ***Impacto de los incidentes de seguridad digital en Colombia 2017*** del MinTIC, la OEA y el BID, "indican que existe una relación significativa y positiva entre el costo y el número de incidentes. Según sus resultados, se estima que el incremento de una unidad en el número de incidentes aumenta en aproximadamente $500 mil pesos colombianos el costo incurrido por las empresas en Colombia como resultado de incidentes digitales. Es importante tener en cuenta que este valor es una estimación a partir de la información reportada y que algunos incidentes pueden tener valores más bajos, mientras otros más altos"

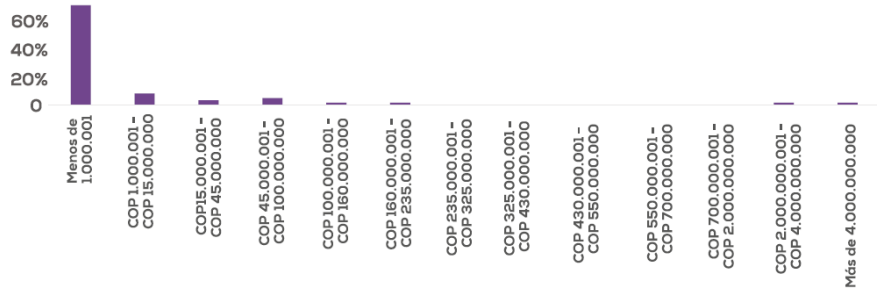
Gráfica 19 Costos de interrupción de las operaciones incurridos por las empresas que estimaron el impacto de los incidentes digitales (2016)



Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

Respecto a otros costos, como los de interrupción de las operaciones normales de la organización, la encuesta de la OEA arrojó que el 50% presentaron un costo más pequeño que $1.000.001, 22% arrojaron un costo entre $1.000.001 y $15.000.000 (ver Gráfica 19). Por otro lado, en cuanto a costos relacionados con sanciones, multas y gastos legales, más de 75% de las empresas arrojaron un costo menor a un $1.000.001, en promedio 12% tuvieron un costo entre $1.000.001 y COP $15.000.000 (ver Gráfica 20).

Gráfica 20 Costos de sanciones, multas y gastos legales incurridos por las empresas que estimaron el impacto de los incidentes digitales (2016)

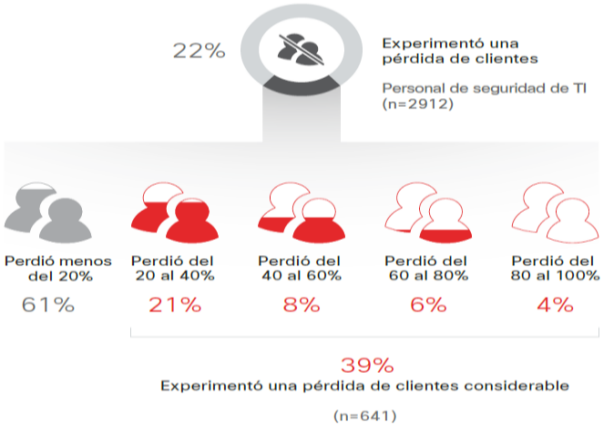


Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

***Costos del Cibercrimen**: La principal problemática radica en que las empresas no reconocen ser víctimas por miedo a perder clientes. El Ciberfraude en Colombia está generando pérdidas por $1 billón de pesos.* Fuente: CCP (2017). Amenazas del Cibercrimen en Colombia 2016-2017.

Ahora bien, los ataques en línea también resultaron en pérdidas de clientes, ya que un 22% de las organizaciones manifestaron un impacto en el número de clientes y de ese grupo el 39% manifestaron haber perdido más del 20% de sus usuarios (ver Ilustración 8).

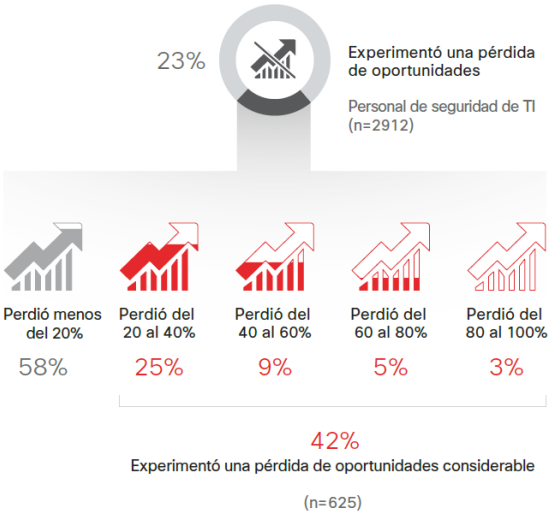
Ilustración 8 Porcentaje de clientes perdidos por empresa debido a ataques



Fuente: Informe de ciberseguridad anual de Cisco 2017 - Estudio comparativo sobre capacidades de seguridad de Cisco 2017

Finalmente, y no menos importante, los incidentes de seguridad digital también tienen costos indirectos, que pueden seguir acumulándose incluso después de que el daño inmediato ha sido reparado (ver Ilustración 9). Muchos de estos costos derivan de la pérdida de reputación o daño a la marca de una empresa, y los mercados financieros pueden reaccionar negativamente y afectar la valoración de las compañías. Algunos de estos factores de costo son fácilmente cuantificables, pero otros aspectos como la pérdida de confianza son intangibles y difíciles de medir.

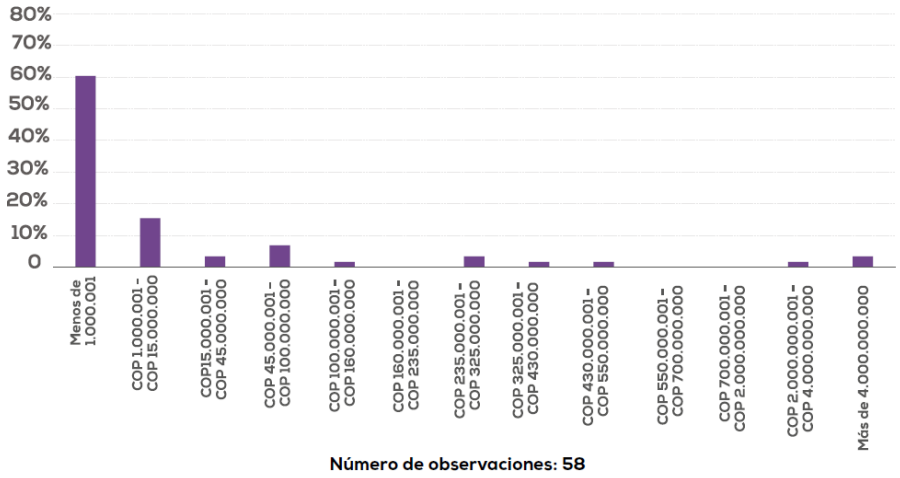
Ilustración 9 Porcentaje de oportunidades empresariales pérdidas como resultado de un ataque



Fuente: Informe de ciberseguridad anual de Cisco 2017 - Estudio comparativo sobre capacidades de seguridad de Cisco 2017

La encuesta de la OEA indagó para Colombia sobre los costos relacionados con daños a la reputación, de lo cual se obtuvo que el 60% de las empresas tuvieron un costo menor a un $1.000.001, aproximadamente 16% arrojaron un costo entre $1.000.001 y $15.000.000 (ver Gráfica 21).

Gráfica 21 Costos de daños a la reputación incurridos por las empresas que estimaron el impacto de los incidentes digitales (2016)



Fuente: Impacto de los incidentes de seguridad digital en Colombia 2017

3. CONTEXTO INTERNACIONAL DE MARCOS REGULATORIOS PARA LA GESTIÓN DE RIESGOS SEGURIDAD DIGITAL

A continuación se realizará una descripción de las experiencias de la Unión Europa, de la República Popular China, Brasil y Estados Unidos, y se revisará su normatividad sectorial de comunicaciones en materia de seguridad y privacidad, las agencias encargadas de la seguridad digital y los estándares adoptados.

3.1. Unión Europea

La Unión Europea (UE) trabaja desde hace muchos años en una estrategia de seguridad digital coherente; particularmente en 2013, la UE estableció una Estrategia de Ciberseguridad[43] que definió la línea de trabajo que debían adoptar los estados miembros para mejorar la seguridad digital. Sus principales objetivos y principios están orientados a fomentar un ecosistema cibernético fiable, seguro y abierto.

[43] JOIN. (2013). *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Recuperado de http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do

Sin embargo, en septiembre de 2017 la Comisión Europea introdujo una serie de propuestas orientadas a actualizar la política de seguridad digital de la región. Principalmente, se propone el fortalecimiento de la Agencia de Seguridad de la Red y de la Información de la Unión Europea (ENISA), la creación de un marco de certificación de ciberseguridad para productos en toda la UE, un plan de acción para responder a incidentes y crisis de ciberseguridad a gran escala y un Centro Europeo de Investigación y Competencia en Seguridad Cibernética.

La propuesta también incluye una nueva Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo para proporcionar una respuesta penal más eficaz a los ciberataques, así como un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas y medidas para fortalecer la cooperación internacional en materia de ciberseguridad[44].

El paquete de medidas propuestas se centra en tres áreas clave:

- Reforzar la capacidad de resistencia de la UE a los ciberataques y reforzar la capacidad de ciberseguridad de la UE
- Creación de una respuesta efectiva del derecho penal a la ciberdelincuencia
- Fortalecimiento de la estabilidad mundial mediante la cooperación internacional

Si bien estos elementos son importantes en la estrategia general de la UE, resulta de mayor relevancia en el contexto del presente estudio analizar aquellas medidas que atañen específicamente al sector de las tecnologías de la información y las comunicaciones. En esta misma línea es importante retomar el marco normativo para las comunicaciones electrónicas de la UE, el cual es definido por la Comisión como: *"(...) una serie de normas que se aplican en todos los Estados miembros de la UE. para fomentar la competencia, mejorar el funcionamiento del mercado y garantizar los derechos básicos de los usuarios"*[45]*;* actualmente está compuesto por cinco directivas y dos regulaciones.

Específicamente en materia de seguridad digital, la Directiva 2009/1401 CE[46] introdujo un capítulo nuevo *"Seguridad e Integridad"* en la forma de modificaciones al Art. 13 bis de la Directiva 2002/21/CE

---

44 Nota: La UE ha emitido un comunicado explicando el paquete de medidas propuestas, disponible aquí: http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm

45 Comisión Europea. (2017). Telcoms Rules. Recuperado de https://ec.europa.eu/digital-single-market/telecoms-rules

46 Directiva 2009/140/CE del Parlamento Europeo y del Consejo, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociad os, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0140&from=en

(Directiva Marco). Estas modificaciones implementan un conjunto de obligaciones en materia de seguridad e integridad de las redes y servicios de comunicaciones. El artículo obliga a los estados miembros de la UE a garantizar que *"los proveedores de servicios de telecomunicaciones adopten las medidas técnicas y organizativas adecuadas para gestionar adecuadamente los riesgos existentes para la seguridad de sus redes y servicios*" y "*adopten todas las medidas oportunas para garantizar la integridad de sus redes a fin de asegurar la continuidad de la prestación de los servicios que utilizan esas redes*".

Un análisis detallado del artículo 13 bis revela el uso de tres definiciones fundamentales: *"incidentes de seguridad*", *"violaciones de seguridad"* y *"pérdidas de integridad"*:

- El párrafo 1 exige que se tomen medidas "*para evitar y reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y las redes interconectadas"*
- El párrafo 2 exige a los estados miembros garantizar que los proveedores tomen "l*as medidas oportunas para garantizar la integridad de sus redes a fin de asegurar la continuidad de la prestación de los servicios"*
- El párrafo 3 exige que se *"notifiquen a la autoridad nacional de reglamentación competente las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios"*

Finalmente, se obliga a las agencias de regulación de comunicaciones de cada país miembro a remitir un reporte anual de incidentes a ENISA y a la Comisión Europea (CE).

El Art. 13 bis debía reglamentarse a nivel nacional por lo Estados miembros antes de 2011. Sin embargo, el calendario y el proceso de transposición varió considerablemente de un país a otro. Hoy en día, la mayoría de los países aplican las disposiciones del art. 13 bis. De una manera u otra, el Art. 13a también designó a ENISA, junto con la CE, como órganos responsables de la recopilación de las notificaciones recibidas y de las medidas adoptadas en los Estados miembros. Además de este mandato específico, de acuerdo con la Directiva la ENISA debería contribuir también a *"armonizar medidas de seguridad técnicas y organizativas adecuadas proporcionando asesoramiento experto"* y *"promover el intercambio de mejores prácticas".*

Como respuesta a los requisitos de la directiva, en 2010, ENISA, los Ministerios y las Agencias Nacionales de Regulación (NRA) de los Estados miembros, iniciaron una serie de reuniones (talleres, conferencias telefónicas, etc.) con el fin de lograr una aplicación armonizada del art. 13 bis de la Directiva marco. Como resultado de estas reuniones, se creó un grupo de expertos de las ANR, *ahora "Article 13a Expert*

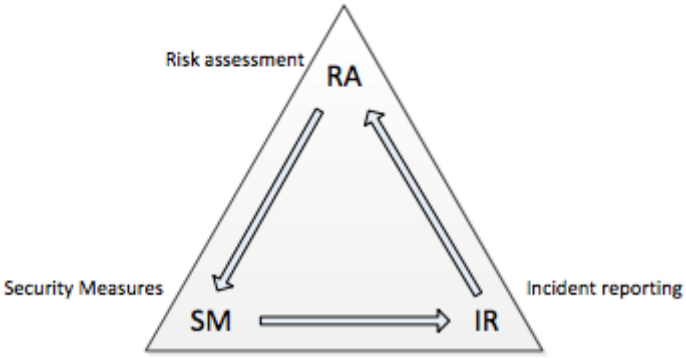
Group"[47]. A través de este grupo se llegó a un acuerdo sobre tres documentos técnicos no vinculantes que proporcionan orientación a las ANR de los Estados miembros de la UE.

El artículo 13 bis, define tres procesos de seguridad de la información para los operadores:

1. Evaluar los riesgos.
2. Tomar las medidas de seguridad apropiadas.
3. Informar sobre incidentes de seguridad significativos.

Los tres procesos se representan en la Ilustración 10:

Ilustración 10 Procesos definidos en el Artículo 13 bis



Fuente: ENISA, grupo de trabajo artículo 13a

A través del trabajo del grupo de expertos, los países miembros llegaron a un acuerdo sobre tres documentos técnicos no vinculantes que proporcionan orientación a las ANR de los Estados miembros de la UE sobre la aplicación del artículo 13 bis:

1. **Guía Técnica de reporte de Incidentes**[48]: define un marco de reporte de información para toda la UE y explica los diferentes enfoques para establecer un proceso nacional de presentación de informes de incidentes.

47 Nota: Las publicaciones del grupo de trabajo pueden consultarse en: https://resilience.enisa.europa.eu/article-13

48 ENISA. (2013). *Technical Guideline on Incident Reporting.* Recuperado de https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

2. **Guía Técnica de Medidas de Seguridad**[49]: presenta de manera general las diferentes medidas de seguridad que podrían ser consideradas por las ANR al evaluar el cumplimiento de las obligaciones. Estas medidas se derivaron de las normas internacionales existentes, principalmente tomando como marco la norma ISO 27001/2.

3. **Guía Técnica de Amenazas y Activos**[50]: proporciona un diccionario de amenazas y activos que tiene como objetivo apoyar el marco de informes de incidentes y apoyar la revisión de la evaluación de riesgos por parte de los proveedores.

En materia de denuncia de incidentes, el artículo 13a establece que no todos son materia de reporte. El artículo obliga a reportar incidentes cuando se presente *"violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios*".

El umbral a partir del cual inicia la obligación de reporte por parte de los operadores a las Agencias Nacionales de Regulación fue dejado a discreción de cada país miembro. Sin embargo, para el reporte anual a ENISA y a la CE el grupo de expertos del art 13a estableció una serie de umbrales recomendados(51).

En conclusión, es posible identificar el enfoque de la unión europea en tres elementos principales: i) continuidad del servicio, ii) reporte de incidentes y iii) cooperación internacional. Adicionalmente, es importante mencionar que el documento de directrices técnicas sobre medidas seguridad desarrollado por ENISA, incluye también las previsiones de la directiva de privacidad en línea (artículo 4), e-privacy Directive (2002/58/EC), por lo que el control incluye un elemento de protección de los usuarios[52].

3.2 República Popular de China

Según la Constitución de la República Popular China, RPC (revisada en 2004), la libertad y la privacidad de las comunicaciones entre los ciudadanos de la RPC están protegidas por la ley. Ninguna organización

---

49 ENISA. (2014). *Technical Guideline on Security measures for Article 4 and Article 13a.* Recuperado de https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article13a/TechnicalGuidelineonSecuritymeasuresforArticle4andArticle13a_version_1_0.pdf

50 ENISA. (2015). *Guideline for Threats and Assets*. Recuperado de https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

51 Nota: El umbral absoluto es de 60 Millones de minutos de usuarios, o 1 Millón de horas de usuario, aunque hay umbrales específicos de acuerdo con la base de usuarios del servicio, más información en [48] Technical Guideline on Incident Reporting

52 ENISA. (2012). *Shortlisting network and information security standards and good practices*. Recuperado de https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

o individuo puede, por cualquier motivo, infringir la libertad y la privacidad de las comunicaciones de los ciudadanos, excepto cuando se ven involucradas las necesidades de seguridad nacional o la investigación de delitos. En respuesta a estas necesidades, las instituciones de seguridad, y las autoridades judiciales, pueden censurar las comunicaciones de acuerdo con los procedimientos prescritos por la ley. Así, la Ley de contraespionaje de la RPC (2014) establece que cuando el trabajo de contraespionaje lo requiere, las autoridades de seguridad nacional pueden inspeccionar los instrumentos de comunicación electrónica, electrodomésticos, otros equipos similares e instalaciones pertenecientes a cualquier organización o individuo. Además, el Reglamento de Telecomunicaciones también establece que las autoridades de seguridad o las fiscalías pueden llevar a cabo un examen del contenido de las telecomunicaciones de conformidad con la ley[53].

En la Ley de Seguridad del Estado de la RPC (2015), se establece que el Estado debe garantizar la seguridad y la capacidad de control de las tecnologías básicas de red e información, infraestructura crítica y sistemas de información y datos en áreas clave. Para ello, el gobierno ha publicado una ley de Ciberseguridad (2016).

Antes de promulgar la Ley de Ciberseguridad, China ya tenía algunas leyes y reglamentos relacionados con la seguridad de la información, como las medidas administrativas para la prevención y el tratamiento de virus informáticos y las medidas administrativas para la protección de la seguridad de la información. Sin embargo, la Ley de Ciberseguridad, demuestra el alto grado de interés de China en la seguridad digital. La mencionada Ley fue adoptada por el Congreso Nacional del Pueblo (NPC) en noviembre de 2016 después de un año de procedimientos legislativos, y entró en vigor el 1 de junio de 2017.

Los principales aspectos incluidos en la Ley son[54]:

- Protección de la información personal y la privacidad individual.
- Estandarización de los mecanismos para la recopilación y el uso de información personal.
- Requerimientos más allá de la "seguridad de los datos": se estipulan requerimientos para la "protección individual de la privacidad".
- Definiciones claras de operadores de redes y requisitos de seguridad.
- Las instituciones financieras más grandes pueden ser consideradas "operadores de red".
- Se imponen mayores requisitos a la protección de la infraestructura crítica.
- Se específica el alcance de la infraestructura de información crítica.

53 ICLG, China Telecoms. (2017). *Media & Internet Laws & Regulations.* Recuperado de http://www.kwm.com/~/media/library/Files/Knowledge/Insights/au/2016/10/12/iclg-telecoms-media-internet-2017-china.ashx?la=en

54 KPMG. (2017). *Overview of China's Cybersecurity Law*. Recuperado de https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

- Restricciones a la transferencia de información fuera de China.
- Se estipula que los datos confidenciales deben almacenarse en el país.
- Las penas por violar la Ley están claramente establecidas e incluyen la suspensión de actividades comerciales.
- Una acción ilegal grave puede llevar al cierre de negocios o la revocación de licencias.
- La multa máxima puede alcanzar 1.000.000 de RMB.

Específicamente el Artículo 10[55] trata sobre los requerimientos de seguridad que deben cumplir los operadores de red; el artículo especifica que, al crear y operar redes o proporcionar servicios a través de redes, se deben tomar medidas técnicas y de otro tipo, necesarias para salvaguardar las operaciones de red, responder de manera efectiva a los incidentes de seguridad cibernética y prevenir el cibercrimen. Así mismo, establece que las medidas también deben mantener la integridad, confidencialidad y accesibilidad de los datos de la red.

De otra parte, el artículo 21[56] establece que el estado adoptará un sistema escalonado para la protección de la ciberseguridad. En dicho sistema los operadores de red deben seguir ciertos procedimientos de seguridad para proteger las redes contra interferencias, destrucción o acceso no autorizado, y para evitar que se filtren, manipulen o roben datos de la red.

Adicionalmente, el artículo 22[57] establece que los proveedores de productos o servicios de red no deben instalar programas maliciosos, y al descubrir un defecto de seguridad, vulnerabilidad u otro riesgo en su producto o servicio, los proveedores de la red deben tomar medidas correctivas de inmediato, informar a los usuarios e informar el problema a los departamentos pertinentes. Este artículo cubre también a los proveedores de servicios y productos de red, quienes deben realizar el mantenimiento de seguridad para sus productos y servicios durante todo el período establecido en los acuerdos entre las partes.

Otros artículos (23 y 35) estipulan que los proveedores solo pueden vender equipos, productos o servicios críticos de red obteniendo certificaciones de seguridad de las autoridades nacionales.

Finalmente, los operadores de infraestructura de información crítica deben evaluar la seguridad cibernética y otros riesgos potenciales al menos una vez al año, ya sea por su cuenta o con ayuda de proveedores de servicios de seguridad de red. Los resultados de la evaluación y las medidas de mejora deben ser reportados a departamentos de protección de infraestructura de información crítica.

55 Nota: Los artículos completos se pueden consultar en: http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en
56 Idem
57 Idem

3.3 Estados Unidos de Norte América

La Federal Communications Commission (FCC), como agencia reguladora de las comunicaciones de los Estados Unidos de Norte América, ha reconocido que la seguridad digital es una de sus prioridades[58]; por esta razón, las normas de la Comisión incluyen la obligación de los Proveedores de Servicios de Internet (ISP) de tomar medidas para proteger sus redes de dispositivos dañinos interconectados. Estas normas establecen que los proveedores no sólo tienen la libertad de tomar medidas para proteger a los consumidores de daños, sino que tienen la responsabilidad de hacerlo.

Para la FCC, una gestión razonable de la red debe incluir prácticas para la seguridad de la red y la integridad del servicio, incluyendo "*el tratamiento del tráfico dañino para la red",* como los ataques de denegación de servicio[59]. Las acciones orientadas a mejorar la seguridad son lideradas en la FCC por la Oficina de seguridad pública y seguridad Nacional - Public Safety & Homeland Security Bureau (PSHSB)[60]. Un análisis de la actividad de esta oficina revela que, aunque las iniciativas son numerosas, rara vez los esfuerzos de la FCC en materia de seguridad de la información se traducen en regulación; en contraste, la Comisión ha trabajado estrechamente con sus Comités Asesores Federales (FAC), así como con otras partes interesadas, para fomentar estándares y mejores prácticas para la reducción del riesgo cibernético[61].

> *"En los últimos años, la Comisión ha avanzado en un nuevo paradigma para la ciberseguridad el cual reconoce que las normas prescriptivas nunca podrían esperar seguir el ritmo de una cuestión tan cambiante".* (FCC, 2017, White Paper: Cybersecurity Risk Reduction).

58 FCC. (2017). *White Paper: Cybersecurity Risk Reduction*. Recuperado de https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf

59 FCC. (2016). *Protecting and Promoting the Open Internet*. Recuperado de https://apps.fcc.gov/edocs_public/attachmatch/DA-16-271A1_Rcd.pdf

60 Public Safety & Homeland Security Bureau (PSHSB), https://www.fcc.gov/public-safety-and-homeland-security

61 Nota: Por ejemplo, el Consejo Asesor de tecnología (TAC) ha examinado cómo incorporar los principios de "seguridad por diseño" en los estándares emergentes para 5G, y el Consejo de Seguridad, Confiabilidad e Interoperabilidad de las Comunicaciones (CSRIC) ha trabajado cómo mejorar la gestión del riesgo de seguridad digital en la cadena de valor del servicio de internet, cómo abordar los riesgos asociados con protocolos *"legacy"* como SS7 y en promover mejores prácticas de seguridad en redes y dispositivos que utilizan Wi-Fi. Además, frecuentemente establece compromisos voluntarios, en consonancia con las recomendaciones del Marco del NIST y del CSRIC, en las que los proveedores colaborarán con la Comisión para abordar los riesgos de seguridad digital en sus redes y entorno de servicios.

La estrategia de la FCC se basa en esfuerzos voluntarios de los ISP con parámetros acordados mutuamente, junto con supervisión del regulador y un mayor énfasis en la rendición de cuentas asegurando que las compañías estén mitigando su riesgo cibernético. Las acciones clave de la FCC son:

- **Promoción de las mejores prácticas:** la FCC trabaja directamente con la industria y socios externos para desarrollar un repositorio de estándares y mejores prácticas para la gestión del riesgo cibernético.
- **La ciberseguridad como acción preventiva y no reactiva:** la Comisión promueve esquemas de *"security by design"* o esquemas para incorporar la gestión de riesgos de seguridad digital durante la fase de desarrollo de nuevos productos y servicios.
- **Concientización:** fortalecimiento de requisitos de reporte de fallas de red y violación de datos.
- **Mejorar el intercambio de información:** adoptar el intercambio de información sobre amenazas cibernéticas en tiempo real con los socios y promover el intercambio entre los operadores privados.
- **Establecer la ciberseguridad como parte integral del Interés Público:** identificar la ciberseguridad como una consideración de las revisiones de fusiones.

Estas acciones clave se evidencian en el trabajo que realiza el Consejo de Seguridad de Comunicaciones, Confiabilidad e Interoperabilidad (CSRIC), el cual es un consejo "multistakeholder" con participación del sector privado que proporciona recomendaciones a la FCC para asegurar, entre otras cosas, la seguridad y fiabilidad de los sistemas de comunicaciones, incluyendo las telecomunicaciones, los medios de comunicación y la seguridad pública. Los miembros de CSRIC se enfocan en una variedad de asuntos de seguridad pública y asuntos relacionados con la seguridad nacional, incluyendo:

1. La confiabilidad y seguridad de los sistemas e infraestructura de comunicaciones, particularmente los sistemas móviles;
2. 911, Enhanced 911 (E911) y Next Generation 911 (NG911); y
3. Alertas de emergencia.

Es posible consultar las mejores prácticas desarrolladas y promovidas por el CSRIC a través de una herramienta dedicada de consulta[62]. Si bien las temáticas a desarrollar por el CSRIC varían anualmente de acuerdo con las necesidades convenidas por la FCC, es interesante apreciar la variedad de temáticas desarrolladas anualmente por el CSRIC (ver Ilustración 11).

62 Nota: CSRIC Best Practices: https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data

Ilustración 11 Grupos de trabajo del consejo de Seguridad de Comunicaciones, Confiabilidad e Interoperabilidad 2016

Communications Security, Reliability, and Interoperability Council (CSRIC) V Working Groups			
Working Group 1 **Evolving 911 Services** **Co-Chairs:** Susan Sherwood & Jeff Cohen **FCC Liaisons:** Tim May & John Healy	**Working Group 2** **Wireless Emergency Alert** **Co-Chairs:** Francisco Sánchez & Farrokh Khatibi **FCC Liaisons:** Chris Anderson, James Wiley & Gregory Cooke	**Working Group 3** **Emergency Alert System** **Co-Chairs:** Steven Johnson & Kelly Williams **FCC Liaison:** Gregory Cooke	**Working Group 4A** **Communications Infrastructure Resiliency** **Co-Chairs:** Kent Bressie & Catherine Creese **FCC Liaison:** Jerry Stanshine & Michael Connelly
Working Group 4B **Network Timing Single Source Risk Reduction** **Chair:** Jennifer Manner **FCC Liaison:** Emil Cherian	**Working Group 5** **Cybersecurity Information Sharing** **Co-Chairs:** Rod Rasmussen, Christopher Boyer, Brian Allen **FCC Liaisons:** Greg Intoccia & Vern Mosely	**Working Group 6** **Secure Hardware & Software** **Co-Chairs:** Brian Scarpelli & Joel Molinoff **FCC Liaisons:** Steven McKinnon & Emily Talaga	**Working Group 7** **Cybersecurity Workforce** **Co-Chairs:** Bill Boni & Drew Morin **FCC Liaison:** Erika Olsen
Working Group 8 **Priority Services** **Co-Chairs:** William Reidway & Thomas Anderson **FCC Liaisons:** Tim Perrier & Ken Burnley	**Working Group 9** **Wi-Fi Security** **Chair:** Brian Daly **FCC Liaisons:** Peter Shroyer & Kurian Jacob	**Working Group 10** **Legacy Systems Risk Reduction** **Co-Chairs:** John Kimmins & Danny McPherson **FCC Liaison: Steven McKinnon**	

Fuente: Communications Security, Reliability and Interoperability Council V, FCC.

Finalmente, es importante mencionar que la FCC mide también el impacto de los incidentes de seguridad utilizando varios indicadores. Además, ha establecido un proceso de notificación de incidentes que proporciona directrices a los operadores de telecomunicaciones en los Estados Unidos sobre qué informar y cuándo notificar los incidentes. Para facilitar el proceso de notificación de incidentes, la FCC también ha establecido valores de umbral. La FCC solicita a los operadores de telecomunicaciones que informen[63] (dependiendo de la falla, el reporte debe realizarse dentro de los 120 minutos después de la detección):

63 Reporting Requirements for Disruptions to Communications, Disponible en: https://www.ecfr.gov/cgi-bin/text-idx?SID=617740ce7d789a296ccb55edda008c40&mc=true&node=pt47.1.4&rgn=div5#se47.1.4

1. La fecha y hora de inicio de la interrupción.
2. Una breve descripción del problema, los efectos del servicio y el área geográfica afectada por el corte.
3. También se hace una distinción en los informes "inicial" y "final", que los proveedores deben reportar el mismo incidente más de una vez (una vez inicialmente y al momento de resolverse). Los requisitos de notificación de interrupciones se clasifican en función del servicio afectado.
4. Los servicios incluidos en el reporte son servicios de cable, instalaciones IXP, interrupciones de las comunicaciones por satélite, sistema de señalización, servicios inalámbricos y proveedores de servicios de VOIP interconectados

Estos reportes son utilizados por la Oficina de Seguridad Pública y Seguridad Nacional de la FCC para adelantar planes directamente con los proveedores de servicio o informar a la ciudadanía y el sector sobre interrupciones de los servicios.

3.4 Brasil

Los protocolos de seguridad vigentes en Brasil cubren las infraestructuras críticas y situaciones de emergencia. En esta materia, desde el 2010 Brasil tiene una "Guía de referencia para la seguridad de las Infraestructuras Críticas de la Información"[64], mediante la cual las instituciones responsables de estas infraestructuras nacionales están orientadas a realizar, como mínimo: (i) mapeo de sus activos de información para la identificación de aquellos que son críticos; (ii) gestión de riesgos con identificación de posibles amenazas y vulnerabilidades; y (iii) establecimiento de un método de generación de alerta de seguridad de las infraestructuras críticas de la información.

En 2015 se publicó la Estrategia de Seguridad de la Información y Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018[65] que reitera la importancia de la protección de las infraestructuras críticas.

Adicionalmente, los operadores deben proteger los datos personales utilizando "técnicas alineadas con estándares internacionales y mejores prácticas" (Ley 12965 de 2014); los requisitos de seguridad específicos (por ejemplo, normas de seguridad o protocolos) para los operadores no están regulados; sin embargo, los operadores deben informar a los clientes sobre los mecanismos de seguridad que implican las prácticas de gestión del tráfico (Ley 12965 de 2014).

64 http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf
65 Para mayor información, ver: http://www.gsi.gov.br/arquivos/4_estrategia_de_sic.pdf

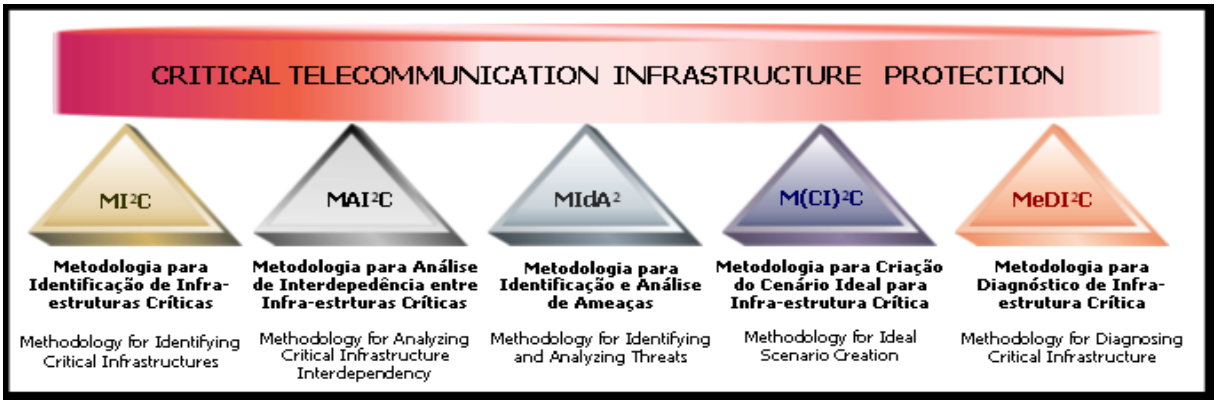
Así mismo, el gobierno requiere protocolos de seguridad específicos como cliente corporativo. Los servicios prestados a las agencias gubernamentales deben cumplir con los requisitos de seguridad establecidos por el Ministerio de Planificación y Presupuesto de acuerdo con el Decreto 8135 de 2013.

Adicionalmente, la Ordenanza Interministerial N. 16, de julio de 2008, estableció el Subgrupo Técnico de Protección de Infraestructuras Críticas de Telecomunicaciones (SGTSIC - Telecom), con el objetivo de:

1. Estudiar y proponer un método para identificar Infraestructura Crítica de Telecomunicaciones (CTI).
2. Identificar la CTI en Brasil;
3. Evaluar las vulnerabilidades de la CTI identificada y sus interrelaciones.
4. Seleccionar las causas y evaluar los riesgos que pueden afectar la seguridad de las CTI.
5. Proponer, coordinar y monitorear las medidas necesarias para asegurar la CTI.
6. Estudiar, proponer e implementar un sistema de información de CTI, que contenga datos en línea para apoyar la toma de decisiones.

La Agencia Nacional de Telecomunicaciones (Anatel), la cual hace parte del subgrupo SGTSIC, así como el Ministerio de Comunicaciones, y otros organismos y expertos, desarrollaron una metodología de protección de infraestructuras críticas de telecomunicaciones la cual culminó con la creación del SIEC, Sistema de Segurança das Infraestruturas Críticas.

Ilustración 12 Modelo CTIP (Critical Infraestructure Protection) desarrollado por ANATEL y CPqD



Fuente: ANATEL

El Proyecto SIEC fue creado con el propósito de proveer a la Agencia de un sistema informatizado y metodologías que le permitieran la gestión de riesgos relacionados con la seguridad de las infraestructuras críticas de telecomunicaciones y monitoreo de las redes.

Específicamente, ANATEL desarrolló un cuestionario que se aplica a los prestadores de servicios de comunicaciones para identificar las infraestructuras críticas de las redes de los operadores, permitiendo identificar información y datos sobre la infraestructura de las estaciones, medidas de seguridad, energía, capacidad y otros datos.

A partir del SIEC, ANATEL desarrolló procesos semestralmente para lograr[66]:

- Identificar las principales estaciones núcleo (core) de las grandes empresas;
- Generar cuestionarios para que los operadores respondan vía web y sirvan de insumo para la elaboración de informes de identificación de amenazas y vulnerabilidades, calculando el índice de riesgos de cada operador.
- Generar planes de tratamiento para mitigar las amenazas y reducir los riesgos que puedan afectar la continuidad en la prestación de los servicios por estas estaciones.

Para el monitoreo de las redes ANATEL desarrolló un módulo de redes que permite el monitoreo de interrupciones, indicadores de calidad y capacidad, así como la construcción visual de las topologías de red, para simular crecimientos de tráfico y estimar impactos en caso de interrupción de un elemento de red (ver Ilustración 13).

Ilustración 13 Centro de monitoreo de infraestructuras críticas ANATEL

Fuente: http://www.anatel.gov.br/setorregulado/destaques/351-central-de-monitoramento

66 Información disponible en la página del SIEC - ANATEL: http://www.anatel.gov.br/setorregulado/destaques/351-central-de-monitoramento

El sistema y la metodología de identificación de infraestructuras críticas de comunicaciones, fue probado durante la Copa Mundial de Fútbol FIFA 2014 y los juegos olímpicos de Río 2016, donde la resiliencia de las comunicaciones era un factor determinante para el éxito de estos eventos y era una de las razones por las cuales se desarrolló el SIEC.

3.5 Resumen tendencias del benchmarking internacional

Como se pudo observar, los Estados están cada vez más interesados en proteger las redes y servicios de telecomunicaciones por su creciente impacto económico y social. A continuación, se presenta un resumen de las principales medidas adoptadas a nivel internacional que fueron analizadas:

Ilustración 14 Resumen medidas de seguridad benchmarking internacional

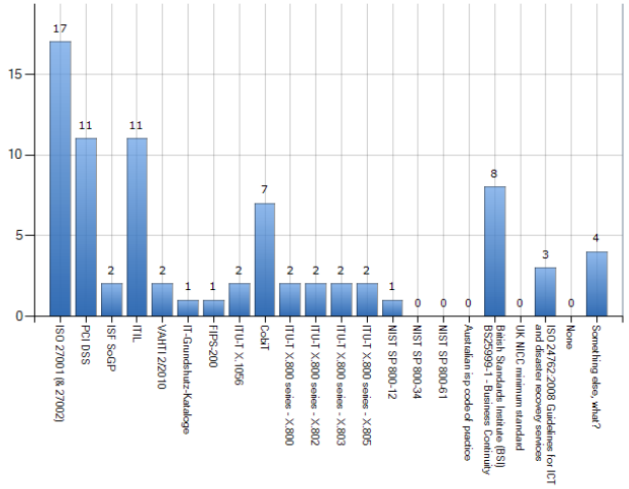
Medidas para la protección de Infra estructura crítica	Modelos para la gestión de riesgos	Reporte de incidentes de seguridad	Certificación de productos
• Diferenciación entre proveedores de infraestructura crítica, infraestructura de telecomunicaciones y proveedores de servicios digitales • Solo la infraestructura efectivamente crítica de comunicaciones e información está sujeta a obligaciones de monitoreo y registro.	• Uso de guías técnicas sobre gestión de riesgo y medidas de seguridad. (Unión Europea) • Mejores prácticas de caracter voluntario desarrolladas en grupos de trabajo con la industria (EE.UU.)	• Los incidentes que se deben reportar son aquellos significativos, definidos a través de umbrales de afectación en la base de usuarios. • Reporte de incidentes a entidades de seguridad de la información.	• Los proveedores sólo pueden vender equipos, productos o servicios críticos de red obteniendo certificaciones de seguridad de las autoridades nacionales (República popular de China, Propuesta Europa).

4. EVALUACIÓN DE ESTÁNDARES Y MEJORES PRÁCTICAS DE SEGURIDAD DIGITAL

Con el objetivo de identificar las mejores oportunidades de actualización del marco regulatorio para la seguridad de las redes y servicios de comunicaciones en Colombia, se revisaron los principales estándares y mejores prácticas de seguridad digital disponible. Si se tiene en cuenta la gran cantidad de estándares disponibles[67], es importante seleccionar aquellos que han sido reconocidos y adoptados por la industria antes de realizar un análisis detallado.

Al respecto, existen investigaciones que han indagado sobre los niveles de adopción de estándares internacionales tanto en Europa como en Estados Unidos. Para el caso específico de la Unión Europea, la Agencia Europea para la Seguridad de las Redes y la Información – ENISA, en 2012, durante el desarrollo de la guía técnica para el cumplimiento del artículo 13 bis, determinó que los estándares de mayor uso entre operadores de telecomunicaciones y compañías de seguridad de la información es el estándar ISO/IEC 27001/2, seguido del estándar PCI DSS (Payment Card Industry Data Security Standard) de uso obligatorio para pagos electrónicos (ver Gráfica 22).

Gráfica 22 Estándares con mayor adopción en Europa

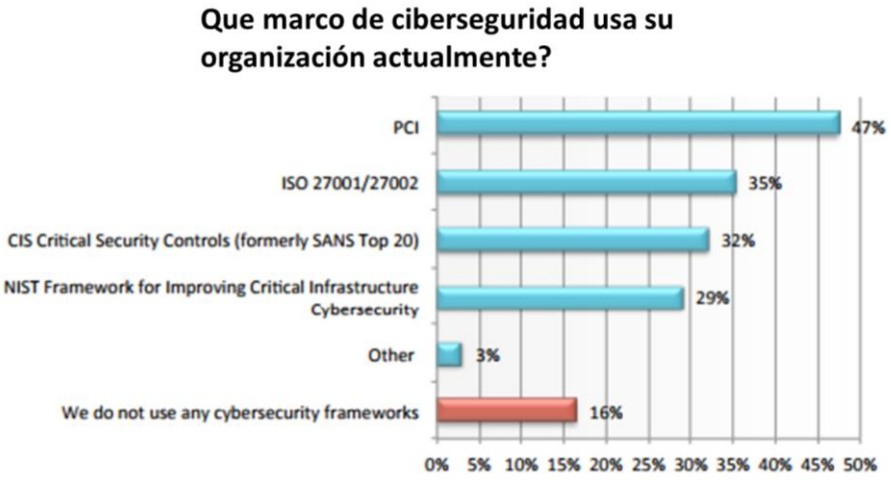


Fuente: ENISA

[67] Para el desarrollo de los requerimientos mínimos del Artículo 13 bis, en Europa se identificaron más 50 estándares y buenas prácticas relevantes en materia de ciberseguridad, Anexo 1 - Guidance on the security measures Article 13ª, ENISA, disponible en: https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

De manera similar, en Estados Unidos de América, un reciente estudio sobre el uso de marcos de ciberseguridad y protección de infraestructuras críticas reveló que el estándar con mayor adopción en una muestra multisectorial, es el estándar PCI DSS, seguido de ISO/IEC 270001/2[68] (ver Gráfica 23).

Gráfica 23 Adopción de estándares de seguridad en Estados Unidos



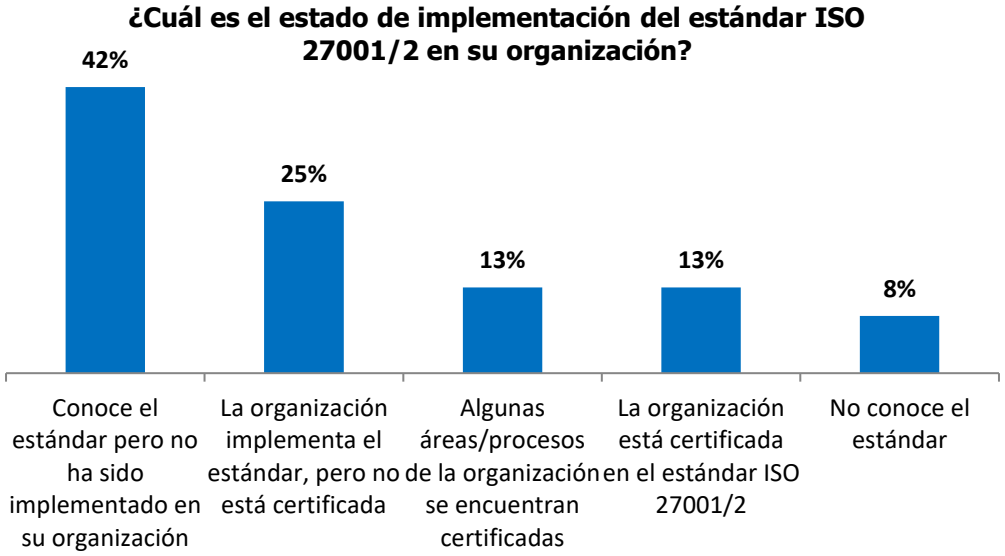
Fuente: Dimensional Research (2016), Trends in Security Framework Adoption

La alta adopción de estos estándares puede ser atribuida no solo a exigencias de cumplimiento por parte de socios de negocio (como es el caso de PCI), sino también al valor agregado que el uso de estos estándares da a las organizaciones, tanto en términos de estandarización del lenguaje de seguridad, como en incrementos de eficiencia en los esfuerzos de protección. Por tanto, el uso de normas acordadas internacionalmente (como la norma ISO/IEC 27001/2) como base para la seguridad de la red, promueven la convergencia de aplicaciones y pueden ser más rentables que desarrollar programas individuales de seguridad. La estandarización y el uso de perfiles estandarizados facilitan la interoperabilidad y la reutilización de soluciones y productos, lo que significa que la seguridad puede introducirse de manera más rápida, más consistente y con un menor costo dentro de las operaciones de las compañías. Es así como las soluciones de seguridad de red estandarizadas benefician tanto a los proveedores de productos y servicios de seguridad, como a las firmas interesadas en proteger sus activos de información, a través de una economía de escala en el desarrollo de productos y la interoperabilidad de componentes.

[68] Dimensional Research. (2016). *Trends in Security Framework Adoption*. Recuperado de https://static.tenable.com/marketing/tenable-csf-report.pdf

De acuerdo con la encuesta diseñada por la CRC para realizar este diagnóstico de seguridad digital, en Colombia la mayor parte de los ISP no implementan el estándar (42%, ver Gráfica 24). Sin embargo, al centrar el análisis únicamente en los 7 operadores que representan el 90% de los accesos a Internet en Colombia, se encuentra que más del 80% de los operadores con más de 100.000 suscriptores implementan el estándar ISO 27001/2.

Gráfica 24 Implementación del estándar ISO 27001/2 en proveedores de servicios de comunicaciones



Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

Si bien el estándar ISO/IEC 27001/2 tiene altas tasas de adopción entre los proveedores de redes y servicios de telecomunicaciones en el mundo, las empresas de telecomunicaciones han manifestado que las normas de la UIT y del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), son normas de ingeniería que definitivamente tienen valor en el sector. La ISO se considera una mejor práctica, pero no es específica para el sector de las telecomunicaciones. El ambiente de riesgo en la vertical de telecomunicaciones difiere significativamente, por lo que requieren modificaciones a la hora de aplicar la norma ISO 27001[69].

[69] ENISA. (2012). *Shortlisting network and information security standards and good practices.* Recuperado de https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

Por lo anterior, se considera conveniente centrarse en los estándares y recomendaciones desarrolladas por la UIT en colaboración con ISO/IEC sobre la mejor práctica 27001 para el análisis de estándares y mejores prácticas.

Adicionalmente, al final de esta sección, se documentan cuatro tecnologías fundamentales de Internet, que pueden ser enmarcadas en cualquiera de las mejores prácticas y que son identificadas por Internet Society, en su programa para la difusión de mejores prácticas en internet "*Deploy 360*"[70] desde donde busca promover la implementación de tecnologías clave para la seguridad digital en Internet (ver Ilustración 15).

Ilustración 15 Líneas de acción del programa Deploy 360

Fuente: Programa Deploy360, Internet Society

4.1 Sistemas de gestión de seguridad de la información (ITU-T X.1051)

Desde el año 2003, la UIT ha trabajado con la Organización Internacional de Estandarización -ISO- para desarrollar una recomendación alrededor de la gestión de seguridad de la información e integridad de servicios basado en la serie ISO 27000, que reconozca el entorno específico de riesgos del sector de las telecomunicaciones.

[70] Nota: para más información ver http://www.internetsociety.org/deploy360/

La gestión de seguridad de la información reconoce que la información es un activo esencial para el desarrollo de los procesos de negocio de una organización. Por esta razón, independientemente de la forma, funcionalidad, o de los medios por los cuales se comparte o almacena la misma, esta siempre debe estar adecuadamente protegida.

Adicionalmente, cuando las empresas cuentan con infraestructura para que clientes finales procesen información que pueden incluir datos personales, confidenciales y comerciales sensibles, se debe garantizar un nivel adecuado de protección, es decir, debe establecerse un Sistema de Gestión de Seguridad de la Información Efectiva (ISMS)[71].

Respecto a lo anterior, la especificación para ISMS más reconocida en el mundo es la definida en la serie de normas ISO/IEC 27000. Esta serie define estándares, requisitos, códigos de práctica, y guías de implementación para sistemas de ISMS. La UIT trabajó conjuntamente con ISO en el desarrollo de la Recomendación UIT-T X.1051 - Código de prácticas en materia de controles de seguridad de la información basados en la norma ISO/CEI 27002 para organizaciones de telecomunicaciones. Esta recomendación es un desarrollo específico para el sector de telecomunicaciones basado en la serie ISO 27000.

Ahora bien, la Recomendación UIT-T X.1051 establece directrices y principios generales para definir, implementar, mantener y mejorar la gestión de la seguridad de la información en empresas de telecomunicaciones y proporciona una base de implementación para la gestión de seguridad de la información orientada a garantizar la confidencialidad, integridad y disponibilidad de las instalaciones y servicios de telecomunicaciones.

La versión específica para el sector de las telecomunicaciones incluye los siguientes temas:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Gestión de activos.
- Control de acceso.
- Cifrado.
- Seguridad física y ambiental.
- Seguridad de operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.

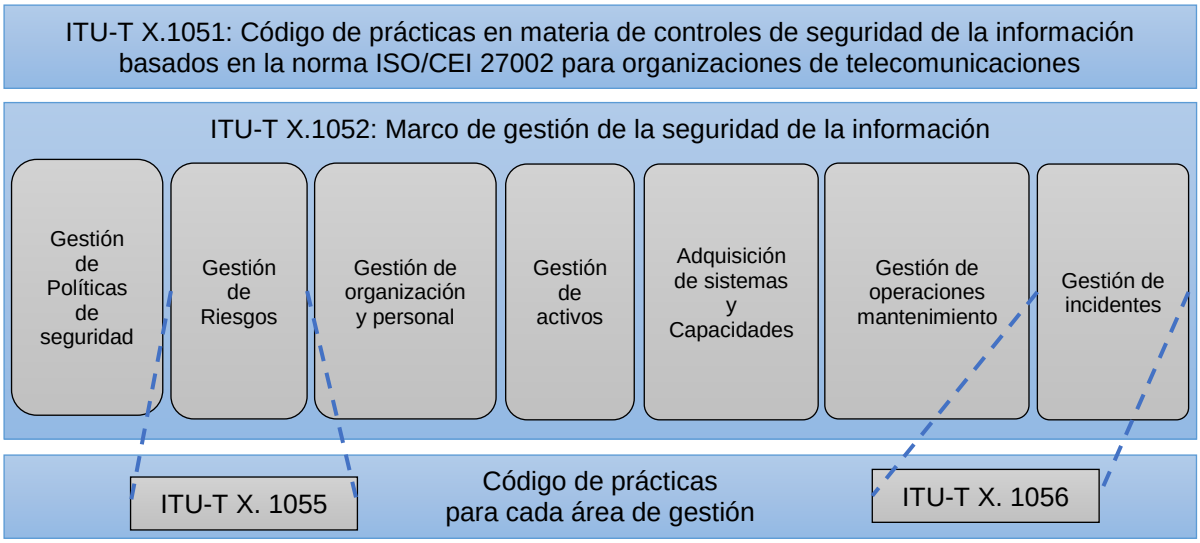
[71] Information security management system (ISMS), ITU-T X.1051. (2016), *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

- Relaciones con proveedores.
- Gestión de incidentes de seguridad de información.
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio.
- Cumplimiento.

4.1.1 Marco de gestión de la seguridad de la información

En concreto, la Recomendación UIT-T X.1051 define las categorías de controles de seguridad para telecomunicaciones. Por su parte, la Recomendación UIT-T X.1052 estipula las actividades principales que deben llevarse a cabo para la implementación de controles de seguridad definidos en la Recomendación UIT-T X.1051, y otras que proporcionan guías específicas para las áreas definidas de seguridad de la información (Recomendaciones UIT-T X.1055, UIT-T X.1056 y UIT-T X.1057).

Ilustración 16 Relación entre la Recomendación UIT-T X.1052 y otras recomendaciones de gestión de la seguridad de la información



Fuente: Security in Telecommunications and Information Technology (2015) – ITU

Así, según la Recomendación ITU-T X.1052, las empresas de telecomunicaciones deben determinar el alcance de su ISMS, incluyendo qué activos de información deben ser cubiertos. Esta definición, junto con la de directrices para la implementación del sistema gestión de la seguridad de la información, deben llevarse a cabo antes de evaluar los riesgos para los activos de información y definir el proceso de control del riesgo. Adicionalmente, según la recomendación, es necesario establecer la estructura y

la forma de la organización de seguridad de la información como base para la implementación del control de riesgos. Uno de los principales aspectos destacados por la recomendación, es que las actividades que controlan los riesgos de las organizaciones no deben aislarse de las operaciones de negocio. Las operaciones de la organización usualmente descritas en una serie de procedimientos deben integrar las actividades de control de riesgos como una parte integral y pertinente.

El sistema ISMS describe las principales actividades de gestión de la seguridad de la información en el sector de telecomunicaciones desde tres aspectos:

a. **Impulsar en la organización la implementación de la gestión de la seguridad de la información:** incluyendo áreas de gestión, como la de gestión de la organización y el personal, y gestión de activos.
b. **Definir y mejorar continuamente el ISMS:** incluyendo áreas de gestión como la gestión de riesgos y la gestión de políticas.
c. **Actividades operativas específicas de la organización:** definiendo áreas de gestión tales como gestión de desarrollo y adquisición de sistemas, de operaciones y mantenimiento y de incidentes.

4.1.2 Gestión de Riesgos - UIT-T X.1055

En cuanto a la gestión de riesgos (proceso de evaluación y cuantificación del riesgo y la adopción de medidas para garantizar que el riesgo marginal esté por debajo de un nivel aceptable predeterminado), este tema es tratado en la Recomendación UIT-T X.1055, que identifica los procesos y técnicas que pueden utilizarse para evaluar los requisitos y riesgos de seguridad de las telecomunicaciones, y para ayudar a seleccionar, implementar y actualizar los controles apropiados para mantener el nivel requerido de seguridad.

Específicamente, la Recomendación UIT-T X.1055 proporciona los criterios para evaluar y seleccionar las metodologías apropiadas para una organización de telecomunicaciones. Sin embargo, no propone ninguna metodología específica.

Ilustración 17 Proceso de gestión de riesgos de la recomendación UIT-T X.1055

Fuente: Security in Telecommunications and Information Technology (2015) - ITU

Por último, es importante mencionar que los perfiles de riesgo se utilizan para guiar el proceso general de gestión de riesgos. Específicamente, se usan para ayudar tanto al proceso de toma de decisiones, como para priorizar los riesgos en términos de su criticidad. Así mismo, el perfil de riesgo se utiliza para determinar la asignación de recursos y controles. La Recomendación UIT-T X.1055 proporciona orientación en el desarrollo de perfiles de riesgo e incluye una plantilla y algunos ejemplos de perfil de riesgo. En concreto, el análisis de riesgos en redes de próxima generación (NGN) se trata en el suplemento Y.19 de la serie ITU-T Y.2200.

4.1.3 Gestión de activos - UIT-T X.1057

Ahora bien, activos como las instalaciones de información y comunicación dentro del alcance del ISMS son considerados de mayor valor que el resto de los activos. Lo anterior sucede porque incidentes que involucran tales activos pueden afectar negativamente no solo a los usuarios, sino también al negocio de la organización. Por lo tanto, se debe considerar que los activos tienen prioridades de alta protección.

Es así como la mayoría de las organizaciones se esfuerzan por encontrar métodos para identificar los activos que deben tener mayores prioridades de protección. El objetivo de la gestión de activos es identificar y proteger los componentes más críticos de la organización a fin de minimizar el riesgo. Al determinar la importancia de los activos, los servicios principales y el valor de la empresa deben considerarse teniendo en cuenta:

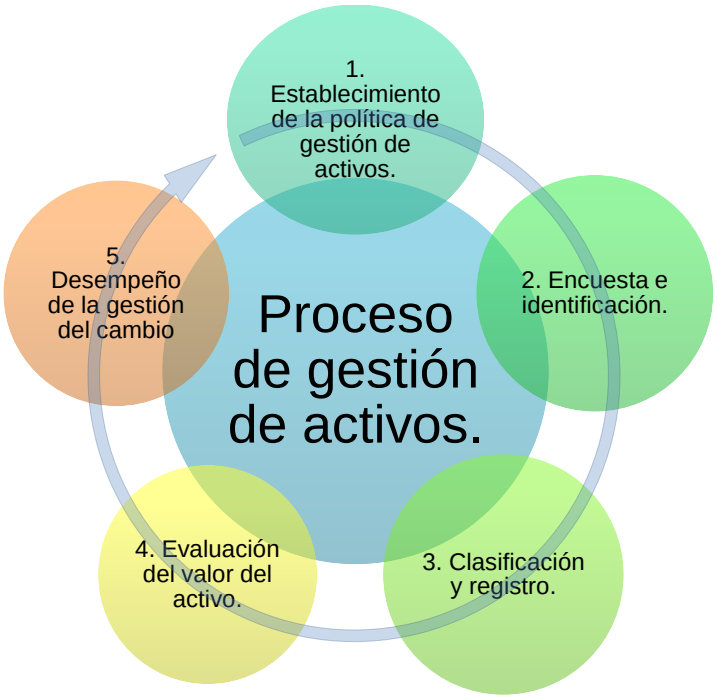
- El impacto potencial en el servicio y el alcance de los servicios que afecta a cada activo.
- La posible pérdida de ganancias y el grado de posible pérdida financiera.
- El impacto potencial de la pérdida de clientes.
- El daño potencial a la imagen de la organización.

Por su lado, las empresas de telecomunicaciones tienen objetivos particularmente altos para operar y administrar sus diversos activos, para proporcionar servicios al cliente y para apoyar directa o indirectamente su negocio. Por tanto, para la protección de activos, es fundamental que las organizaciones de telecomunicaciones se aseguren de que las operaciones y los servicios de la empresa no se vean comprometidos.

Para ello, la Recomendación UIT-T X.1057 proporciona una descripción general de los procesos y métodos que deben abordarse para identificar, clasificar, evaluar y mantener los activos que poseen las organizaciones de telecomunicaciones.

En concreto, la gestión de activos de seguridad de la información se refiere a las medidas apropiadas de manejo y protección considerando el valor del activo según lo determine cada organización. Por tanto, para gestionar los diversos activos de una organización de forma sistemática y segura, debe adoptarse un proceso de gestión de activos del ciclo de vida que cubra la adquisición o generación del activo, así como la modificación y eliminación o destrucción del activo según normas y estándares predeterminados.

Ilustración 18 Proceso de gestión de activos UIT-T X.1057



Fuente: Security in Telecommunications and Information Technology (2015) - ITU

Finalmente, la Recomendación UIT-T X.1057 proporciona directrices de actividades detalladas en cada proceso que cubren: i) establecimiento de la política de gestión de activos, ii) encuesta e identificación, iii) clasificación y registro, iv) evaluación del valor del activo, y v) rendimiento de la gestión del cambio. La UIT-T X.1057 también describe los activos específicos de telecomunicaciones.

4.2 Recomendaciones Internet Society para ISP

Adicional a las recomendaciones incluidas previamente, se considera importante referenciar mejores prácticas a nivel técnico que favorecen un entorno digital seguro en las redes y servicios. En este sentido, se observa que el programa Deploy360 de Internet Society busca ayudar a las organizaciones a acelerar la implementación de nuevos estándares y tecnologías de Internet.

El programa fue planteado para cerrar la brecha entre el desarrollo de protocolos y estándares desarrollados por el Grupo de Trabajo de Ingeniería de Internet (IETF) y crear protocolos basados en estándares abiertos y su implementación en la industria de comunicaciones. Actualmente, el programa cubre cuatro tecnologías fundamentales para la seguridad en Internet. Esta sección documenta la

importancia de cuatro tecnologías (IPV6, DNSSEC, Aseguramiento del BGP, y Prevención de la falsificación de direcciones IP), su nivel de adopción en Colombia y las perspectivas en el futuro próximo.

4.2.1 IPv6

Todos los dispositivos terminales con conexión a Internet requieren una dirección IP numérica para comunicarse con otros dispositivos. En el esquema de direccionamiento original, llamado IPv4, está agotando el bloque de direcciones disponibles[72]. Ante la escasez de direcciones IPv4, los ISP han recurrido a protocolos de red que permiten agrupar usuarios a través de una misma dirección pública. IPv6 es la norma de dirección de Protocolo de Internet (IP) de próxima generación destinada a complementar y reemplazar a IPv4. El agotamiento de direcciones IPv4 compromete la identificación unívoca de las fuentes de tráfico y puede dificultar las investigaciones y el filtrado para manejo de incidentes debido al uso compartido de direcciones IPv4.

La práctica generalizada de colocar a múltiples usuarios, a veces miles de ellos, tras una misma dirección de IP hace que sea técnicamente muy difícil investigar un comportamiento malicioso en línea. La Unión Europea, por ejemplo, ha identificado que en algunos casos de delitos graves como los abusos sexuales infantiles, es incluso necesario investigar a cientos de usuarios con el fin de identificar a un agente malicioso[73].

Por ello, la UE fomentará la adopción del nuevo protocolo (IPv6), que permite la asignación de un único usuario por dirección IP, lo que supone una gran ventaja para los servicios policiales y las investigaciones de ciberseguridad. Como primer paso para fomentar dicha adopción, la Comisión Europea incorporará el requisito de pasar al IPv6 en todas sus políticas, incluidos los requisitos en materia de contratación y financiación de proyectos e investigaciones, además de fomentar el uso de los materiales de formación necesarios. Así mismo, los Estados miembros han sido llamados a considerar la posibilidad de establecer acuerdos voluntarios con los proveedores de servicios de Internet para impulsar la adopción de IPv6.

A nivel mundial, Bélgica es el país líder[74] en porcentaje de adopción del IPv6 como resultado de la cooperación de los sectores público y privado. Las partes interesadas pertinentes consideraron la

---

72 Un fenómeno conocido como "IP Exhaustion" o Agotamiento de IP, más información en: https://www.apnic.net/community/ipv4-exhaustion/graphical-information/

73 Comisión Europea. (2017). *Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*. Recuperado de http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=ES

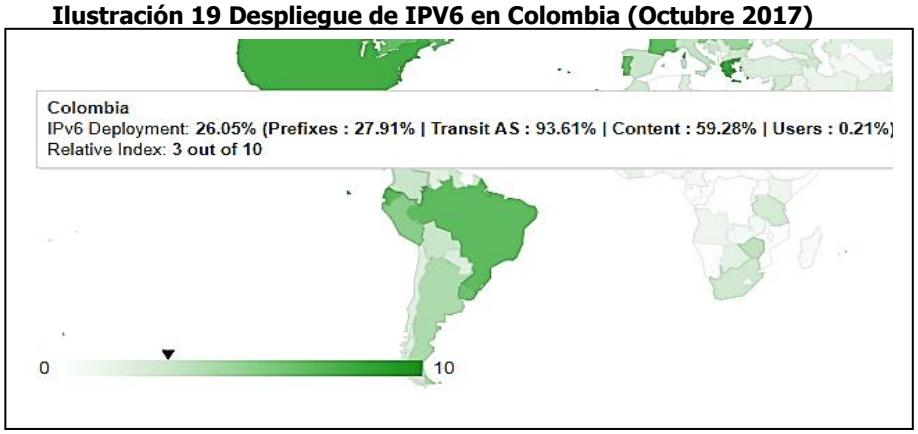
74 Monitoreo de adopción mundial de IPV6 por CISCO: http://6lab.cisco.com/stats/index.php?option=all

posibilidad de limitar el uso de una dirección IP a un máximo de 16 usuarios como parte de una medida voluntaria de autorregulación, lo que incentivó la transición al IPv6[75].

Adicionalmente, IPv6 integra como componente obligatorio en su especificación el framework IPsec[76] proporcionando capacidades de autenticación y cifrado directamente desde el protocolo de comunicaciones y de consecuencia mejorando significativamente las capacidades de seguridad de las redes que lo implementan.

Globalmente, diversas organizaciones monitorean el despliegue de IPv6. CISCO presenta una métrica completa que agrupa cuatro variables para su construcción: (i): los prefijos IPv6 asignados por el registro regional de internet LACNIC[77], (ii) el porcentaje de tránsito en el Sistema autónomo[(78)] con IPv6 habilitado en el país, (iii) páginas web (contenido) con IPv6 en las 500 más transitadas del país, y (iv), el porcentaje de conexiones de los usuarios a Google con dirección IPv6 habilitada.

Ilustración 19 Despliegue de IPV6 en Colombia (Octubre 2017)



Fuente: CISCO 6Lab, http://6lab.cisco.com/stats/search.php

Por su lado, Colombia tiene un índice compuesto de despliegue de IPv6 de 3.0 sobre 10 (ver Ilustración 19), muy por detrás de los líderes de la región después de Ecuador (7.0), Brasil (6.9) y Perú (5.4). Un análisis detallado de los indicadores del país (

75 CONSULTATION ON QUESTION OF THE BIPT BOARD OF 11 OCTOBER 2016 CONCERNING THE TERMS OF USE OF IPV4 / CGN, Disponible en: http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf

76 Guidelines for Specifying the Use of IPsec Version 2, IETF, Best Current Practice 146.

77 LACNIC es el Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe. Es uno de los 5 Registros Regionales de Internet en el mundo.

78 Nota: El sistema autónomo (AS) es una colección de prefijos de enrutamiento IP bajo el control de los operadores en representación de una o más entidades que presentan una política de enrutamiento claramente definida en Internet.

Tabla **1**), muestra que los peores resultados se dan en el usuario final donde solo un 0.21% de los usuarios establecieron conexiones a través de direcciones IPv6.

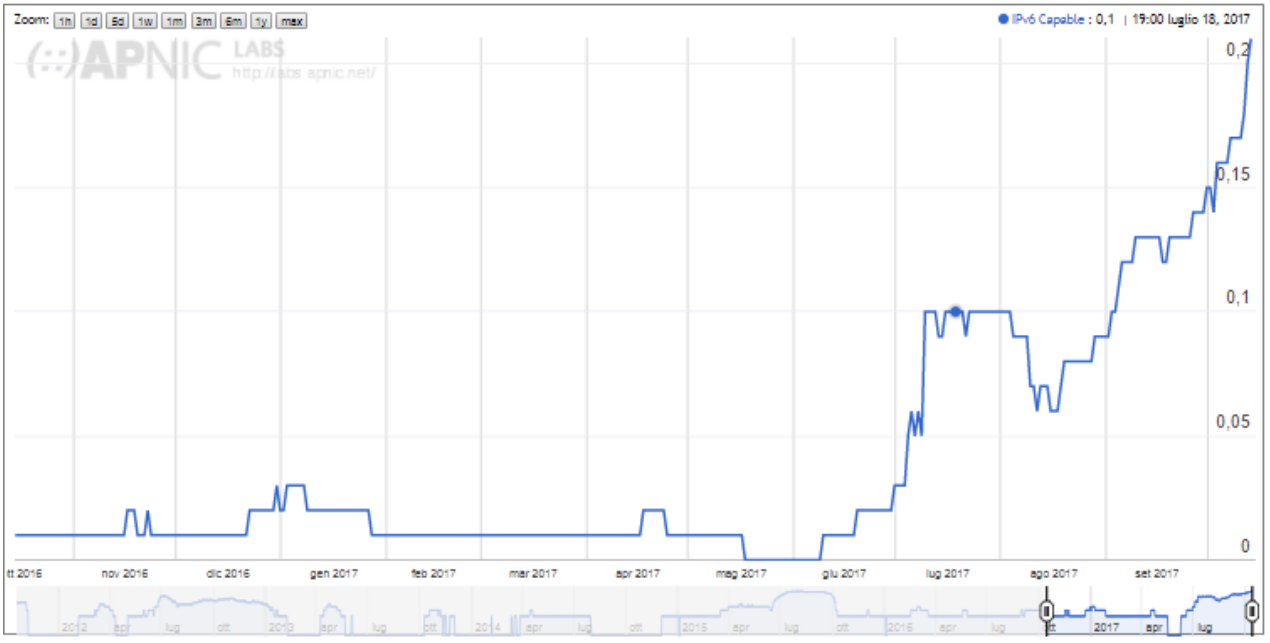
Tabla 1 Indicadores de despliegue IPV6 en Colombia (octubre 2017)

Indicador IPV6	
Prefijos	27.9%
Transito AS	93.6%
Contenido	59.2%
Usuarios	0.21%
Índice relativo	3.0/10

Fuente: CISCO 6Lab.

Analizando los datos específicos para la variable de usuarios recolectados por APNIC (Asia Pacific Network Information Centre), los resultados arrojan que el 0,21% representa un incremento significativo (+2000%) respecto a los niveles de 2016 (0.01%). Sin embargo, un análisis de los ASN muestreados por APNIC, revela que de los operadores con mayor número de accesos en Colombia, solo DirecTV ha desplegado moderadamente IPv6 en sus redes.

Ilustración 20 Porcentaje de uso de IPv6 en usuarios finales en Colombia



Fuente: APNIC Labs (octubre 2017)

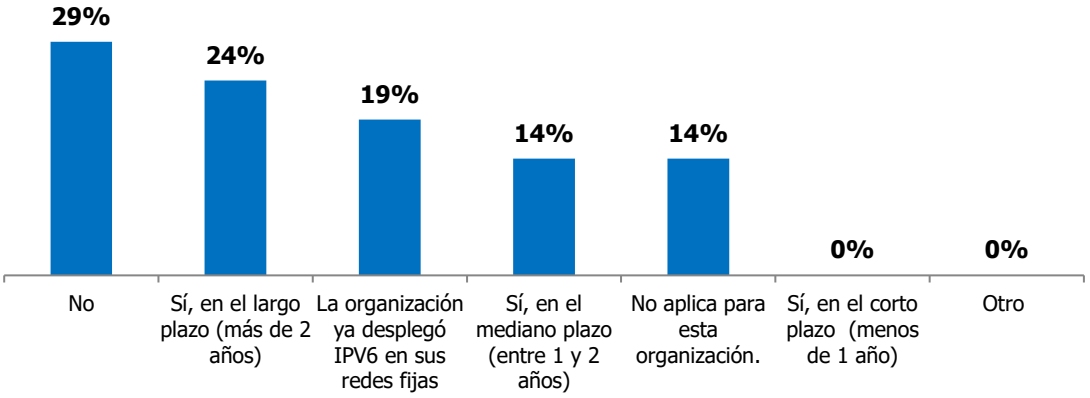
Tabla 2. Uso de IPv6 por prefijos de enrutamiento de operadores

ASN	Nombre de AS	IPV6	Muestras
AS10620	Telmex Colombia S.A.	0.00%	609.731
AS13489	EPM Telecomunicaciones S.A. E.S.P.	0.01%	498.689
AS3816	COLOMBIA TELECOMUNICACIONES S.A. E.S.P.	0.01%	454.149
AS14080	Telmex Colombia S.A.	0.01%	258.871
AS19429	ETB - Colombia	0.02%	222.063
AS26611	COMCEL S.A.	0.00%	86.381
AS262186	TV AZTECA SUCURSAL COLOMBIA	0.01%	69.064
AS27695	EDATEL S.A. E.S.P.	0.00%	60.244
AS262928	DIRECTV COLOMBIA LTDA.	6.77%	57.489
AS8163	Metrotel S.A. ESP	0.00%	42.903
AS22368	TELEBUCARAMANGA S.A. E.S.P.	0.00%	39.486
AS27831	Colombia Móvil	0.00%	32.407
AS10299	EMPRESAS MUNICIPALES DE CALI E.I.C.E. E.S.P.	0.00%	31.445
AS3549	LVLT-3549 - Level 3 Communications, Inc.	0.00%	20.278
AS18678	INTERNEXA S.A. E.S.P.	0.00%	18.247
AS27951	Media Commerce Partners S.A.	0.07%	16.757
AS23520	COLUMBUS-NETWORKS - Columbus Networks USA, Inc.	0.21%	11.635
AS18747	IFX18747 - IFX Corporation	0.08%	7.205
AS263210	HV TELEVISION S.A.S	0.00%	6.461
AS27837	Dialnet de Colombia S.A. E.S.P.	0.00%	5.499
AS22698	AVANTEL SAS	0.00%	4.720
AS27845	Empresa de Recursos Tecnológicos S.A E.S.P.	0.00%	4.534

Fuente: APNIC Labs (octubre 2017)

De otra parte, la encuesta realizada por la CRC a los proveedores de Internet en Colombia revela que ninguno de los ISPs planea desplegar IPv6 en el corto plazo, y el 29% de los ISPs no tiene ningún plan para desplegar IPv6 en redes fijas (ver Gráfica 25). Si se centra el análisis únicamente en los 7 ISPs con mayor número de suscriptores, la situación es positiva, pues 3 de los 7 mayores ISPs de Colombia manifiestan contar con planes para desplegar IPv6 en el mediano plazo (entre 1 y 2 años).

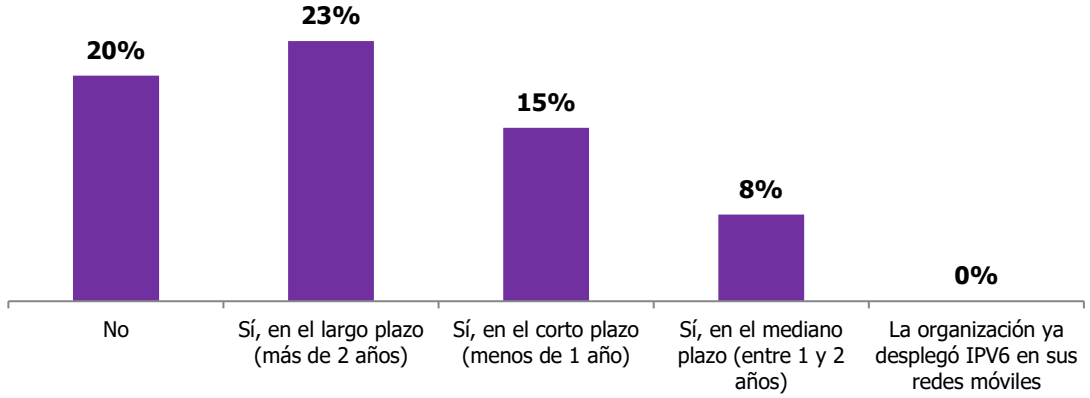
Gráfica 25 ¿Cuenta su organización con un plan de transición a IPV6 en sus redes fijas?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

La situación para las redes móviles es similar. La mayor parte de los operadores tiene planes de despliegue de IPv6 en el largo plazo o no planea desplegar IPv6 ni siquiera en el largo plazo (ver Gráfica 26).

Gráfica 26 ¿Cuenta su organización con un plan de transición a IPV6 en sus redes móviles?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

Frente a la situación del IPv6 en los operadores colombianos, la encuesta también indagó aspectos relacionados con el nivel de preparación. Así, los resultados revelan que un 32% de los operadores aún no han solicitado direccionamiento IPv6 a LACNIC (a pesar de que todos los siete operadores con mayor participación en el mercado han solicitado ya direccionamiento IPv6).

Como parte de un plan de transición, los operadores deben identificar los elementos de red que requerirían mejoras. Sin embargo, al indagar sobre el estado de este inventario en los operadores se evidencia que el 50% de los mismos tienen identificados los elementos que requerirían cambios, el porcentaje es aún mayor entre los operadores con más de 100.000 suscriptores, en donde más del 80% contaría con el inventario de equipos de red que requieren mejoras.

Otro aspecto importante es la preparación del personal de la organización para la transición a IPv6. En este punto, el 45% de los operadores manifestaron tener un nivel de preparación aceptable, y solo el 32% manifestaron sentirse bien preparados para la transición.

Finalmente, la encuesta indagó sobre las pruebas y ensayos realizadas por los ISPs. En este aspecto se evidenció que el 50% de los ISPs han realizado pruebas de despliegue IPv6 para clientes externos o internos. *Para mayor información sobre el diagnóstico de IPv6 ver Anexo I. Encuesta: Diagnóstico Seguridad Digital CRC.*

Iniciativa de IPv6 MINTIC – Resolución 2710 de 2017

Por otro lado, y respecto a la adopción de IPv6, en octubre de 2017 el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 2710 de 2017 "Por la cual se establecen lineamientos para la adopción del protocolo IPv6"[79]. En esta Resolución se establece que la infraestructura de comunicaciones de todas las entidades estatales debe operar nativamente con el protocolo IPv6.

Específicamente, la Resolución en mención tiene por objeto "*formular medidas para la adopción del protocolo IPv6 en Colombia por parte de los obligados de que trata el artículo siguiente; así mismo, establecer medidas para los proveedores de redes y servicios de telecomunicaciones para que cursen tráfico y ofrezcan conectividad y servicios en IPv6 a las entidades objeto de esta resolución*" y establece que los proveedores de redes y servicios de telecomunicaciones que presten el servicio de acceso a Internet, deben tener preparada su conexión troncal de acceso a Internet, de forma, que permita enrutar los prefijos de IPv6 nativos de las entidades estatales.

Para alcanzar este objetivo el MinTIC desarrolló dos guías: i) "Guía de transición de IPv4 a IPv6 para Colombia"[80], y ii) "Guía para el aseguramiento del Protocolo IPv6"[81]. Asimismo, la resolución establece

[79] Imprenta Nacional de Colombia. (2017). *Diario Oficial N. 50376, 4 de octubre de 2017*. Recuperado de http://jacevedo.imprenta.gov.co/tempDownloads/50D3761508334567108.pdf

[80] MinTIC. (2016). *Seguridad y privacidad de la información.* Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

[81] MinTIC. (2016). *Seguridad y privacidad de la información.* Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

que la contratación estatal, de infraestructura y servicios de comunicaciones, iniciada a partir de la vigencia de la misma, debe dar soporte nativo IPv6.

El plazo para la transición establecido en la Resolución para entidades del orden nacional es hasta el 31 de diciembre de 2019, y para entidades territoriales, hasta el 31 de diciembre de 2020.

Como consecuencia de esta resolución se espera que los operadores encuentren incentivos adicionales para realizar las modificaciones a sus redes, impulsando así la adopción general del protocolo IPv6 en Colombia.

4.2.2 DNSSEC

Las extensiones de seguridad del DNS[82], Security Extensions desarrolladas por la Internet Engineering Task Force (IETF) también conocidas como DNSSEC, son una herramienta para asegurar que la conexión a un sitio web o servicio es auténtica. Antes de conectarse a un sitio web, el navegador tiene que recuperar la dirección IP del sitio mediante el sistema de DNS. Sin embargo, es posible que un atacante intercepte las consultas al DNS y proporcione información falsa que haga que el navegador se conecte a un sitio web falso donde potencialmente los usuarios podrían proporcionar información personal (credenciales, mensajes, passwords, etc.). DNSSEC provee un nivel de seguridad adicional donde el navegador web puede verificar la información del DNS y asegurarse que no ha sido modificada.

Para los usuarios, la implementación de DNSSEC por parte de los ISPs y los proveedores de contenidos, implica un nivel de riesgo menor de convertirse en una víctima de fraude cuando, por ejemplo, accede a servicios bancarios en línea o compras por Internet porque existe más seguridad para el usuario que se está comunicando con el banco o la tienda adecuada y no con una página alterada.

No obstante, es importante tener en cuenta que DNSSEC no detiene todos los tipos de fraude. La función solo está diseñada para prevenir ataques en los que el atacante manipula las respuestas a las consultas DNS para lograr su objetivo. Existen muchas vulnerabilidades diferentes y problemas de seguridad en Internet que DNSSEC no resuelve, por ejemplo, ataques como la denegación de servicio distribuida (DDOS).

Cuando se trata de phishing (páginas que son similares o idénticas a las originales para engañar a las contraseñas y datos personales) y pharming (redirección de una consulta DNS a un servidor incorrecto)

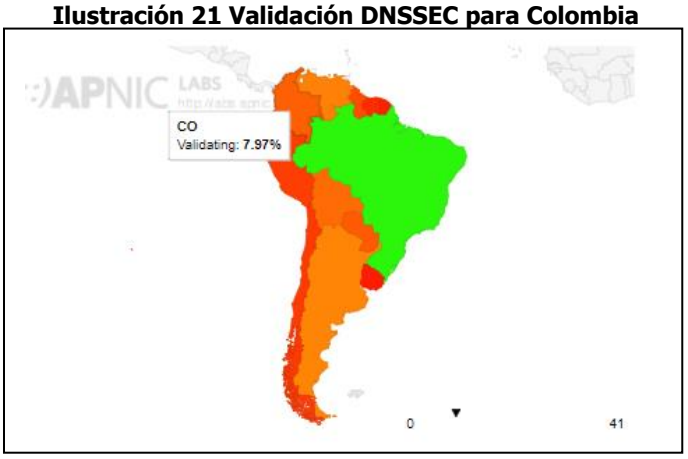
82 DNS: Domain Name Resolver, el sistema de nombres de dominio tiene como una de sus funciones "traducir" las direcciones inteligibles para las personas (www.ejemplo.com) en identificadores numéricos asociados con los equipos conectados a la red (direcciones IP), esta traducción es fundamental para poder enrutar y localizar los contenidos solicitados.

y otros ataques similares contra DNS, DNSSEC brinda un nivel adicional de protección. Sin embargo, DNSSEC no protege contra ataques en otras capas.

Teniendo en cuenta que el reporte del Centro Cibernético Policial identifica el phishing y las estafas por Internet como la mayor fuente de denuncias por parte de la ciudadanía en materia de seguridad digital, resulta importante evaluar el estado de adopción en Colombia.

En la actualidad la única fuente de estadísticas de validación DNSSEC es la producida por el equipo de Geoff Huston's team en APNIC. Al revisar las estadísticas de mayo a marzo de 2017 se tiene que para Colombia:

Ilustración 21 Validación DNSSEC para Colombia



Fuente: APNIC - https://stats.labs.apnic.net/dnssec

Solo el 7,97% de las conexiones fueron validadas, lejos del líder regional, Brasil, donde se realiza un 40% de validaciones DNSSEC. Un análisis detallado de los identificadores asignados a los operadores presentes en la muestra de APNIC:

Tabla 3 Distribución de validación DNSSEC por ASN

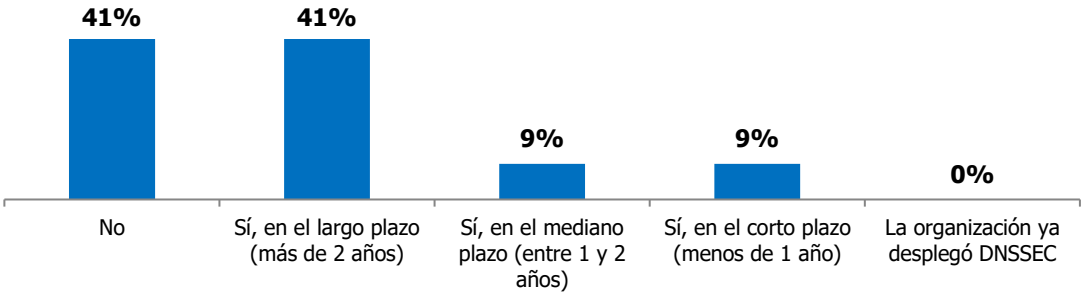
ASN	AS Name	% Validación	Muestras
AS10620	Telmex Colombia S.A.	2.36%	564.337
AS13489	EPM Telecomunicaciones S.A. E.S.P.	4.63%	453.766
AS3816	COLOMBIA TELECOMUNICACIONES S.A. E.S.P.	1.59%	414.504
AS14080	Telmex Colombia S.A.	5.52%	239.155
AS19429	ETB - Colombia	2.60%	207.211
AS26611	COMCEL S.A.	0.47%	71.738
AS262186	TV AZTECA SUCURSAL COLOMBIA	40.04%	62.200
AS27695	EDATEL S.A. E.S.P.	2.62%	53.741
AS262928	DIRECTV COLOMBIA LTDA.	97.90%	51.785
AS8163	Metrotel S.A. E.S.P.	5.12%	38.307
AS22368	TELEBUCARAMANGA S.A. E.S.P.	5.08%	36.478
AS10299	EMPRESAS MUNICIPALES DE CALI E.I.C.E. E.S.P.	9.76%	28.535
AS27831	Colombia Móvil	0.06%	27.069
AS3549	LVLT-3549 - Level 3 Communications, Inc.	44.63%	18.651
AS18678	INTERNEXA S.A. E.S.P.	37.72%	16.849
AS27951	Media Commerce Partners S.A.	31.11%	15.374
AS23520	COLUMBUS-NETWORKS - Columbus Networks USA, Inc.	28.89%	11.198

Fuente: https://stats.labs.apnic.net/dnssec

Se observa que la mayor parte de los ISP no tienen altas tasas de validación, y con excepción de DIRECTV, la mayor parte de los operadores no realizan validaciones de DNS. Teniendo en cuenta el potencial de DNSSEC para mitigar numerosas modalidades de Malware/Phishing y otras vulnerabilidades, resulta importante evaluar la evolución del despliegue de DNSSEC dentro de los operadores colombianos.

De otra parte, la encuesta realizada por la CRC a los proveedores de Internet en Colombia revela que el 41% de los ISP no tiene planes de desplegar DNSSEC en sus redes, y solo el 9% planea un despliegue del protocolo a largo plazo (ver Gráfica 27).

Gráfica 27 ¿Planea su organización ofrecer soporte DNSSEC en sus redes?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

La encuesta de la CRC también indagó acerca de las capacidades de los servidores de DNS de los ISP, y reveló que el 77% de los ISPs tendrían infraestructura capaz de soportar DNSSEC. Sin embargo, más allá de las capacidades de los servidores, un despliegue de DNSSEC requiere la modificación de una configuración crítica de red como lo es el protocolo DNS por lo que se necesitan esfuerzos significativos de configuración. *Para mayor información sobre el diagnóstico de DNSSEC ver Anexo I. Encuesta: Diagnóstico Seguridad Digital CRC.*

4.2.3 Aseguramiento del BGP

El Border Gateway Protocol (BGP) es el protocolo utilizado para intercambiar información de enrutamiento entre redes para el funcionamiento del Internet en general. Es el lenguaje que utilizan los enrutadores para determinar cómo y dónde enviar los paquetes de un enrutador a otro hasta llegar al destino final. El BGP ha sido muy exitoso y sigue siendo un protocolo fundamental para el funcionamiento de Internet.

A pesar de lo anterior, el protocolo BGP no fue diseñado con mecanismos de seguridad en su incepción y depende en gran medida de la confianza entre los operadores de red, y en que los mismos aseguren sus sistemas correctamente y no envíen datos incorrectos. El problema emerge por el hecho de que atacantes potencialmente podrían modificar las tablas de enrutamiento usadas por BGP.

Por ejemplo, en febrero de 2008 se presentó una caída global de YouTube que duró alrededor de dos horas, cuando un ISP Pakistaní publicó sus propios servidores en el BGP como destino global del tráfico de YouTube[83].

Existen diferentes medidas que pueden ayudar a proteger el BGP, muchas de las cuales se describen en la RFC 7454, *"BGP Operations and Security"* publicada por IETF en 2015 y que se conoce como mejor práctica BCP 194.

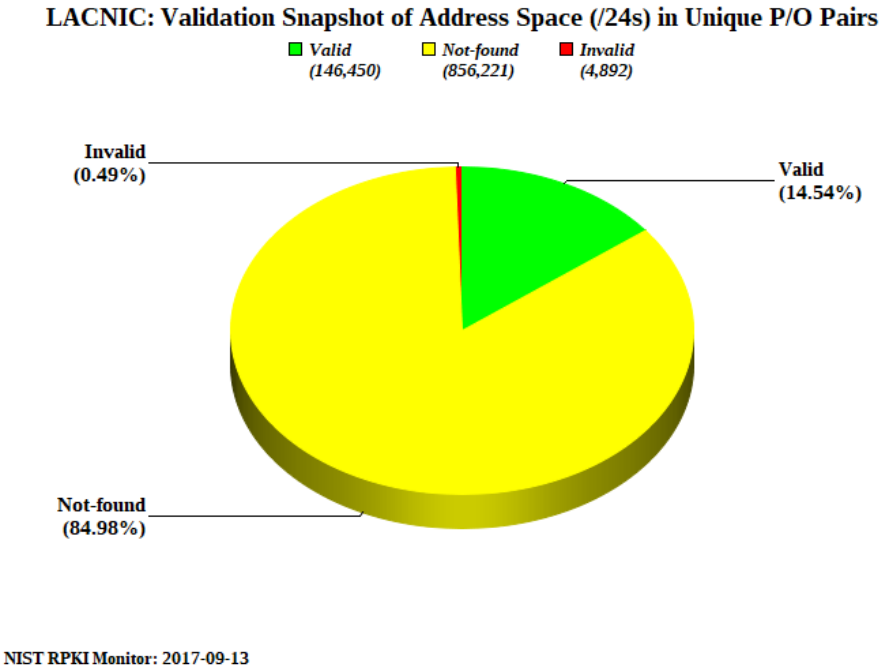
Una de las principales medidas de protección del BGP, es el sistema de infraestructura de claves públicas de recursos (RPKI). Este sistema es un framework de infraestructura de claves públicas especializado en proteger la infraestructura de enrutamiento de Internet. El RPKI puede ser utilizado por los titulares legítimos de los recursos para controlar el funcionamiento de los protocolos de enrutamiento de Internet y evitar los ataques de tipo route hijacking[84].

83 https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/

84 El secuestro de ruta es la adquisición ilegítima de grupos de direcciones IP a través de la corrupción de las tablas de enrutamiento de Internet mantenidas por el Border Gateway Protocol (BGP)

Debido a la complejidad de la infraestructura de enrutamiento global, no existen muchas estadísticas sobre su resiliencia. Sin embargo, el Instituto Nacional de Estándares y Tecnología Estadounidense (NIST) mantiene un monitoreo del despliegue de RPKI a nivel global.

Gráfica 28 Resultados de Validación RPKI para la región LACNIC, octubre 2017

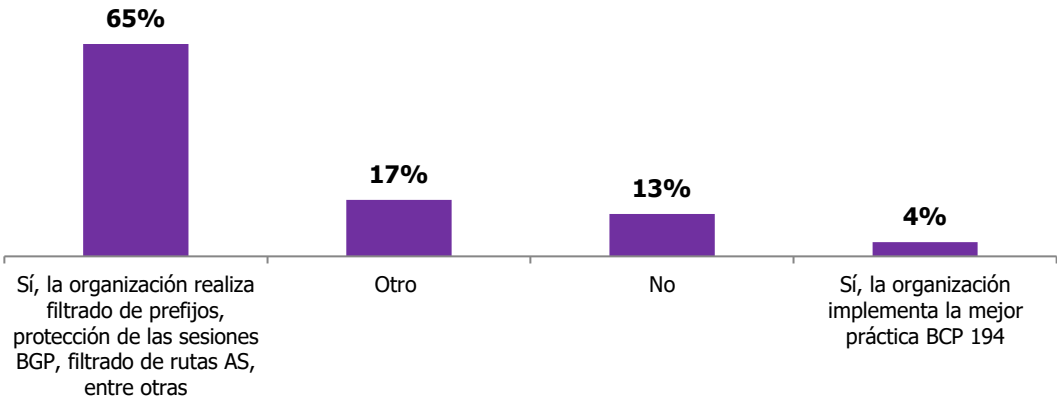


Fuente: NIST, https://rpki-monitor.antd.nist.gov/index.php?p=4&s=0.

Los resultados de Latin America & Caribbean Network Information Centre (LACNIC), región en donde se encuentra el espacio de direccionamiento de Colombia, revelan la baja adopción de validaciones RPKI en la región. Dada la importancia central de BGP en el funcionamiento global de Internet se considera pertinente evaluar el estado de implementación de las mejores prácticas contenidas en BCP-194 dentro de los operadores colombianos.

Específicamente, la encuesta realizada por la CRC en 2017 a los proveedores de Internet en Colombia revela que si bien solo 4% de los operadores adopta la Best Current Practice BCP-194, el 65% de los ISP adopta medidas para la protección del BGP (ver Gráfica 29). *Para mayor información sobre protección del BGP por parte de los operadores en Colombia ver ANEXO 1. ENCUESTA: DIAGNÓSTICO SEGURIDAD DIGITAL CRC*

Gráfica 29 ¿Las redes provistas por su organización implementan medidas de aseguramiento del BGP?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

4.2.4 Prevención de la falsificación de direcciones IP (Antispoofing)

El spoofing de IP es la práctica de falsificar porciones del "*header*" o cabecera de los paquetes del protocolo de Internet (IP). Debido a que la mayor parte del tráfico, aplicaciones y servidores de Internet utilizan IP, la suplantación de IP tiene importantes implicaciones de seguridad.

Ahora bien, para la suplantación de direcciones de origen IP, una parte decisiva en los ataques distribuidos de denegación de servicio – DDoS. Para este tipo de ataques, usualmente los atacantes usan malwares y "bots" que se ejecutan en computadores "desprevenidos" para así enviar una gran cantidad de solicitudes a un servidor de destino. Las solicitudes suelen tener direcciones IP de origen falsas o "spoofed" y, por lo tanto, cuando el servidor intenta responder a estas solicitudes, se atasca esperando iniciar conexiones a destinos que no existen. Adicionalmente, a la hora de investigar los incidentes, las direcciones IP de origen falsas (ya sea IPv4 o IPv6) también hacen que sea extremadamente difícil localizar de dónde provienen las fuentes de los ataques.

Un mecanismo que puede ser implementado por los operadores de red para mitigar los efectos de los ataques de DDoS es la implementación de tecnologías anti-spoofing. Una solución que parece ser viable es no permitir que los paquetes abandonen la red de los ISP con destino al resto de Internet si los mismos tienen una dirección IP falsa. En particular, en el borde de Internet (dentro de la red del ISP)

es posible saber con precisión qué gama de direcciones IP están en su red y sólo permitir direcciones "legítimas" como direcciones de origen para los paquetes salientes. La implementación es más complicada en las redes más grandes, pero este enfoque en general se denomina a menudo filtrado de ingreso, y es una Best Current Practice (BCP) de la IETF, BCP-38[85]. También se conoce este método como "Ingress Filtering" o "validación de dirección de origen".

El proyecto "Spoofer" del Centro para el Análisis Aplicado de los Datos de Internet (CAIDA, por sus siglas en inglés) de la Universidad de San Diego en California, analiza la capacidad de las redes globales para enviar y recibir paquetes con direcciones IP falsificadas[86]. Los resultados para Colombia, si bien se realizaron únicamente para 69 bloques de IP, revelan que dentro de la muestra analizada, un 14.5% permite falsificación (ver Tabla 4).

Tabla 4 Resultado de pruebas de Spoofing por país

Country	Client IP blocks	Spoofing IP blocks	Blocking IP blocks		Inconsistent IP blocks
			Non-NAT	NAT	
usa (United States)	7100	398 (5.6%)	1164 (16.4%)	5531 (77.9%)	7 (0.1%)
jpn (Japan)	260	10 (3.8%)	22 (8.5%)	228 (87.7%)	0 (0.0%)
col (Colombia)	69	10 (14.5%)	0 (0.0%)	59 (85.5%)	0 (0.0%)

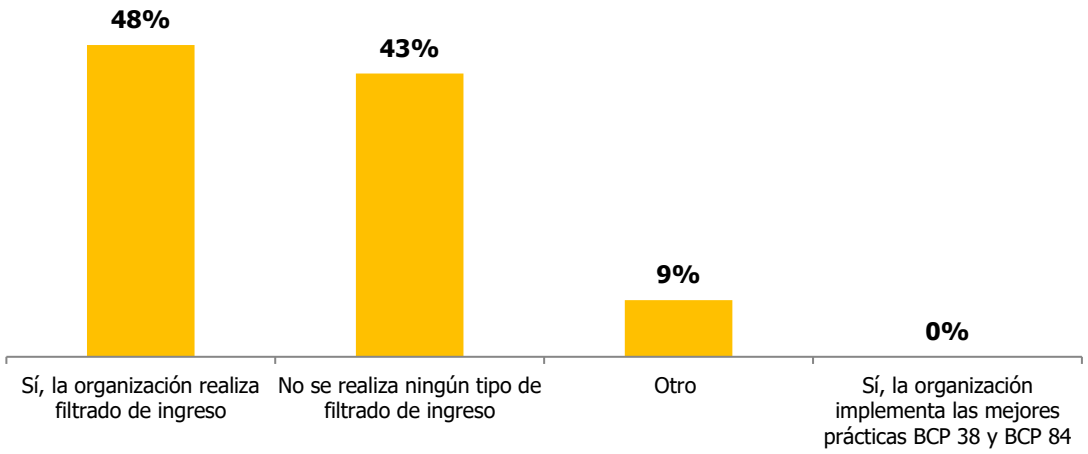
Fuente: Proyecto CAIDA, Universidad de San Diego, California

Teniendo en cuenta el rol del filtrado de ingreso en la prevención y mitigación de ataques DDoS, se consideró pertinente evaluar el estado de implementación de las mejores prácticas contenidas en BCP-38 dentro de los operadores colombianos.

La encuesta realizada por la CRC a los proveedores de Internet en Colombia revela que si bien ninguno de los operadores adopta la Best Current Practice BCP-38, el 48% de los ISP realizaría filtrado de ingreso en sus redes (ver Gráfica 30). Posiblemente el efecto del protocolo NAT (Network Adress Translation) de bloquear o rechazar direcciones que no se encuentren en el rango de traducción esperado, incentive que en la práctica se tenga un mayor porcentaje de seguridad en el forjado de direcciones IP en Colombia. *Para mayor información sobre la falsificación de direcciones IP en Colombia ver ANEXO 1. ENCUESTA: DIAGNÓSTICO SEGURIDAD DIGITAL CRC*

85 Mas información disponible en: http://www.bcp38.info/index.php/Main_Page
86 Proyecto CAIDA: https://www.caida.org/projects/spoofer/

Gráfica 30 ¿Realiza su organización algún tipo de filtrado de ingreso?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

5. EVALUACIÓN DEL ESTADO DE IMPLEMENTACIÓN DE MODELOS DE SEGURIDAD EN LOS PRST

A partir de la información resultante de la encuesta, y de un análisis de las previsiones vigentes, se examinarán los modelos de seguridad adoptados por los PRST en Colombia.

5.1 Previsiones vigentes

A partir de lo señalado en la Resolución CRT 2258 de 2009 - *"Aspectos regulatorios asociados a la ciberseguridad"*, se establecieron las características generales para garantizar la seguridad de la red y la integridad de los servicios. Específicamente se estableció la obligación de implementar modelos de seguridad que contribuyesen a mejorar la seguridad de las redes de acceso de los proveedores de servicio de Internet, de acuerdo con los marcos de seguridad definidos por la UIT en lo que respecta a las recomendaciones pertenecientes a las series X.800. Esta medida se integró dentro del Régimen de calidad vigente en ese momento (Resolución CRT 1740 de 2007), y actualmente se encuentra vigente dentro en el artículo 5.1.2.3 SEGURIDAD DE RED del Capítulo 1 del Título V de la Resolución compilatoria CRC 5050 de 2016.

Así mismo, a través de la Resolución CRT 2258 de 2009, se establecieron las características generales que deben cumplir los PRST en materia de inviolabilidad de las comunicaciones y privacidad de los datos personales. Estas previsiones se encuentran vigentes en los artículos 2.1.4.1. INVIOLABILIDAD DE LAS COMUNICACIONES y 2.1.4.2. SEGURIDAD DE LOS DATOS E INFORMACIÓN del Título II de la Resolución compilatoria CRC 5050 de 2016. Sin embargo, es en la Resolución CRC 5111 de 2017 "*Por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones*" se revisaron estos artículos, y dadas las evoluciones en la reglamentación del tratamiento de datos personales a partir del desarrollo de la Ley de Protección de Datos Personales (Ley 1581 de 2012), el nuevo régimen de protección a los usuarios de servicios de comunicaciones, hace referencia a las previsiones de la ley y por lo tanto, en el estudio de las obligaciones vigentes es suficiente realizar el análisis de los requerimientos de seguridad red contenidos en el título V de la Resolución compilatoria de la CRC.

5.2 Recomendaciones de la serie UIT X.800

Un análisis detallado de las previsiones del artículo 5.1.2.3 SEGURIDAD DE RED del título V de la Resolución compilatoria CRC 5050 de 2016, revela diferentes aspectos asociadas a la seguridad de la red que deben ser adoptados por los PRST.

Tabla 5 Previsiones de seguridad de red en el Título V de la Resolución compilatoria de la CRC 5050 de 2016

Elementos del Artículo 5.1.2.3 SEGURIDAD DE RED	Implicaciones
"Los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio"	El alcance de las previsiones es para los PRST que ofrecen servicio de Internet.
"Deberán informar en su página Web sobre las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing, malware entre otras"	Los PRST deben dedicar una sección en sus páginas web donde informen las acciones adoptadas para prevenir el spam, phishing, malware.
"implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de	Los ISP deben adoptar modelos de seguridad conforme a las recomendaciones de seguridad de la UIT.

seguridad definidos por la UIT en lo relativo a las recomendaciones pertenecientes a las series X.800 dictadas por este organismo"	
1) Autenticación: Verificación de identidad tanto de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida (Recomendaciones UIT X.805 y UIT X.811).	Los ISP deben adoptar mecanismos para garantizar la identidad de las entidades[87] involucradas. Las entidades incluyen no sólo humanos, sino también dispositivos, servicios y aplicaciones.
2) Acceso: Prevenir la utilización no autorizada de un recurso. El control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones (Recomendaciones UIT X.805 y UIT X.812).	Los ISP deben adoptar mecanismos para prevenir el uso no autorizado de los recursos, incluyendo la prevención del uso de un recurso de una manera no autorizada. El control de acceso garantiza que sólo el personal o dispositivos autorizados tengan acceso a elementos de red, información almacenada, flujos de información, servicios y aplicaciones.
3) Servicio de No repudio: Es aquél que tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. (Recomendaciones UIT X.805 y X.813).	Los ISP deben tener la capacidad de evitar que las entidades posteriormente nieguen falsamente que realizaron (o no realizaron) una acción/comunicación. El no repudio tiene el objetivo de contar con pruebas que más tarde puedan utilizarse para contrarrestar afirmaciones falsas.
4) Principio de Confidencialidad de datos: Proteger y garantizar que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados (Recomendaciones UIT X.805 y X.814).	Los ISP deben garantizar que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizadas. El propósito del servicio de confidencialidad es proteger la información de divulgaciones no autorizadas.

87 Nota: Una entidad puede ser un humano, organización, hardware o pieza de software – ITU X.842 - §3

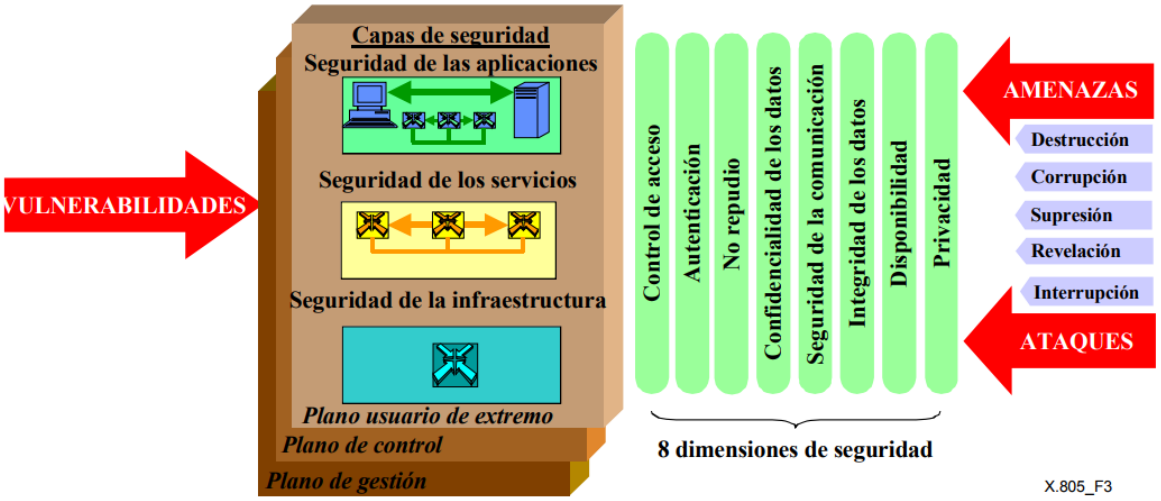
5) Principio de Integridad de datos: Garantizar la exactitud y la veracidad de los datos, protegiendo los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señalar o informar estas acciones no autorizadas (Recomendaciones X.805 y X.815).	Los ISP deben garantizar que los datos involucrados en el servicio no han sido alterados sin autorización. En general, un servicio de integridad se ocupa de la necesidad de garantizar que los datos no están corruptos o, si están corruptor, que el usuario lo sabe.
6) Principio de Disponibilidad: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones (Recomendación X.805).	Los ISP deben garantizar que no se niegue el acceso autorizado a elementos de red, información almacenada, flujos de información, servicios y aplicaciones por eventos que afecten la red.
Los proveedores de redes y servicios de telecomunicaciones a través de redes móviles, además de las soluciones de seguridad antes descritas, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122.	Para los servicios móviles, los PRST deben adoptar modelos de seguridad acordes con el marco de comunicaciones móviles seguras extremo a extremo.

Los marcos de seguridad descritos en las recomendaciones de la serie X.800 de la UIT fueron desarrollados para definir las descripciones generales de los servicios de seguridad. Estos estándares abordan todos los aspectos de cómo se deben aplicar los servicios de seguridad en el contexto de una arquitectura específica. Los marcos se centran en proporcionar protección para los sistemas, los objetos dentro de los sistemas y la interacción entre los sistemas. Sin embargo, estos estándares no abordan la metodología para construir los mecanismos y los servicios de seguridad.

5.2.1 Elementos de la recomendación de arquitectura UIT-T X.805

Respecto a la arquitectura de la Recomendación UIT-T X.805, la cual se define en términos de tres conceptos principales: capas de seguridad, planos y dimensiones, para una red de extremo a extremo, se toma un enfoque jerárquico al dividir los requisitos de seguridad en capas y planos para que cubra la seguridad de extremo a extremo al diseñar medidas de seguridad en cada una de las dimensiones para abordar las amenazas específicas. En la Ilustración 22 se observan los elementos de esta arquitectura.

Ilustración 22 Aplicación de las dimensiones de seguridad a las capas de seguridad[88]



Fuente: UIT-T X.805

Ahora bien, una dimensión de seguridad es un conjunto de medidas diseñadas para abordar un aspecto particular de la seguridad de la red. Los servicios básicos de la Recomendación UIT-T X.800 (Control de acceso, autenticación, confidencialidad de datos, integridad de datos y no repudio, ya presentes en las previsiones de seguridad vigentes de la CRC) se reflejan en las funcionalidades de las dimensiones de seguridad correspondientes de la Recomendación UIT-T X.805 (como se muestra en Figura). Además, la Recomendación UIT-T X.805 agrega tres dimensiones (seguridad de comunicación, disponibilidad y privacidad) que no estaban en la Recomendación UIT-T X.800:

- Dimensión Seguridad de la Comunicación: garantiza que la información fluya solo entre los puntos finales autorizados, es decir, que la información no se desvíe o intercepte a medida que fluye entre estos puntos finales.
- Dimensión Disponibilidad: (ya incluida en las previsiones vigentes de la CRC) garantiza que no se niegue el acceso autorizado a los elementos de la red, la información almacenada, los flujos de información, los servicios y las aplicaciones debido a eventos que afectan a la red.
- Dimensión de Privacidad: proporciona la protección de la información que podría derivarse de la observación de actividades de la red. Los ejemplos incluyen sitios web que un usuario ha visitado, la ubicación geográfica de un usuario y las direcciones IP y los nombres DNS de los dispositivos en una red de proveedores de servicios.

[88] Rec. UIT-T X.805 (10/2003), Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

Estas dimensiones no se limitan a la red, sino que también se extienden a las aplicaciones y la información del usuario final. Las dimensiones de seguridad se aplican a los proveedores de servicios o empresas que ofrecen servicios de seguridad a sus clientes. Para proporcionar una solución de seguridad de extremo a extremo, las dimensiones deben aplicarse a una jerarquía de equipos de red y agrupaciones de instalaciones, que se denominan capas de seguridad. Un plano de seguridad representa un cierto tipo de actividad de red protegida por dimensiones de seguridad. Cada plano de seguridad representa un tipo de actividad de red protegida.

Es así como los planos de seguridad desarrollan las necesidades de seguridad específicas asociadas con las actividades de gestión de red, las actividades de señalización o control de la red, y las actividades de los usuarios finales. Según la recomendación, las redes deben diseñarse de tal manera que los eventos en un plano de seguridad estén aislados de los otros planos. Los planos de seguridad son:

- El plano de gestión: dedicado a las operaciones, la administración, el mantenimiento, y el aprovisionamiento de un usuario o una red.
- El plano de control: asociado con los aspectos de señalización para configurar (y modificar) la comunicación de extremo a extremo a través de la red, independientemente del medio o la tecnología utilizada en la red.
- El plano del usuario final: que trata la seguridad del acceso y el uso de la red por parte de los suscriptores. Este plano también trata de proteger los flujos de datos del usuario final.

Finalmente, la recomendación define capas de seguridad, las cuales abordan los requisitos que son aplicables a los elementos y sistemas de la red y a los servicios y aplicaciones. Una de las ventajas de definir estas capas, es permitir la reutilización de servicios de seguridad en diferentes aplicaciones para proporcionar seguridad de extremo a extremo. Las vulnerabilidades en cada capa son diferentes y, por lo tanto, las medidas que se deben adoptar en cada una son distintas. Las tres capas definidas en la recomendación son:

- La capa Infraestructura: representa los componentes fundamentales de las redes, sus servicios y aplicaciones. Los ejemplos de componentes que pertenecen a esta capa incluyen elementos de red individuales, como enrutadores, conmutadores y servidores, así como los enlaces de comunicación entre ellos.
- La capa Servicios: asociada a los servicios de red ofrecidos a los clientes. Estos servicios abarcan desde ofertas básicas de conectividad, como servicios de líneas arrendadas, hasta servicios de valor agregado, como mensajería instantánea.

- La capa de Aplicaciones: define los requisitos de las aplicaciones basadas en red utilizadas por los clientes. Estas aplicaciones pueden ser tan simples como el correo electrónico o tan sofisticadas como, por ejemplo, el streaming de vídeo, donde se utilizan transferencias de vídeo de alta definición, o un programa de contabilidad.

En este orden de ideas, la arquitectura de la Recomendación UIT-T X.805 ha sido usada para guiar el desarrollo de políticas de seguridad, arquitecturas tecnológicas y planes de respuesta y recuperación de incidentes. Esta arquitectura también puede ser utilizada para evaluar el nivel de seguridad de una organización. Una vez que se implementa un programa de seguridad, debe conservarse para mantenerse actualizado en el entorno de amenazas en constante cambio.

Si bien las recomendaciones de arquitectura de seguridad de la serie UIT-T X.800, y en particular los elementos definidos en la recomendación UIT-T X.805 contienen los aspectos y requisitos funcionales que deben ser desarrollados para contar con un entorno de red seguro, resulta importante reconocer que a partir de su desarrollo la UIT ha trabajado en desarrollar estándares y recomendaciones adicionales, incluyendo aquellas relacionadas con los sistemas de gestión de seguridad de la información, como los descritos en el Capítulo 6, y que se encuentran más alineados con el objetivo de lograr una adecuada gestión de los riesgos de seguridad digital planteados en la política nacional de seguridad digital.

5.3 Estado de implementación

Para evaluar el estado de implementación de los modelos de seguridad previstos en la normatividad vigente, la encuesta de diagnóstico realizada por la CRC indagó cada uno de los aspectos mencionados tanto en el Título de Calidad como en el Título de Régimen de Protección al Usuario.

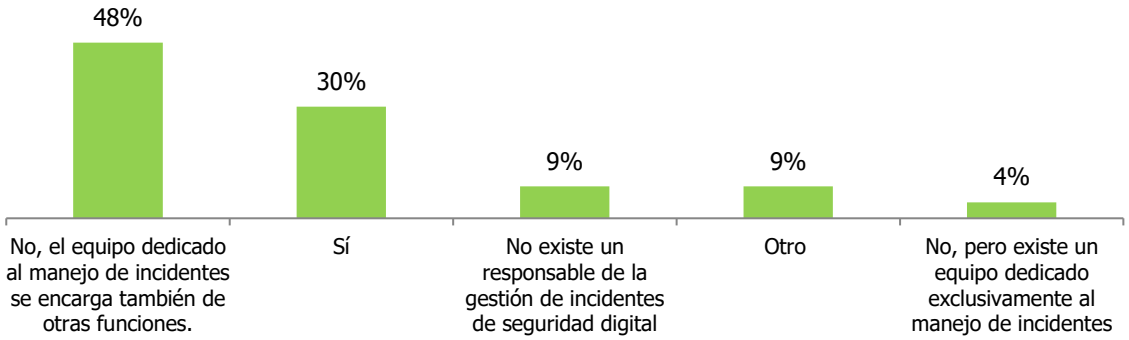
5.3.1 Tratamiento de incidentes de seguridad de la información

Uno de los primeros resultados de la encuesta de la CRC arrojó que el 100% de los ISP con más de 100.000 suscriptores cuenta con un proceso formal de tratamiento de incidentes de seguridad de la información y con un Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT por sus siglas en inglés (Computer Security Incident Response Team)[89]. El proceso formal por lo general involucra las fases de reporte, clasificación, atención y acciones correctivas. Por lo menos uno de los operadores manifestó contar con un centro de operaciones de seguridad.

[89] Nota: Los CSIRT también son conocidos como CERT o Computer Emergency Response Team.

A nivel general, sin embargo, se encontró que solo un 30% de los operadores tiene un equipo de respuesta a incidentes (ver Gráfica 31), asimismo al indagar sobre el número de personas que componen el equipo de respuesta a incidentes se encontró que el 65% de los operadores no dedica ninguna persona exclusivamente al tratamiento de incidentes informáticos. Los operadores que manifestaron no contar con un proceso de gestión de incidentes (9%) son una minoría. *Para mayor información sobre los equipos de respuesta a incidentes en Colombia ver ANEXO 1. ENCUESTA: DIAGNÓSTICO SEGURIDAD DIGITAL CRC*

Gráfica 31 ¿Cuenta su organización con un equipo de respuesta a incidentes de seguridad informática CSIRT?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

5.3.2 Autenticación y Acceso (UIT-T X.811 y UIT-T X.812):

La autenticación y acceso son servicios de seguridad que verifican la identidad tanto de usuarios como de aplicaciones para permitir el acceso a los servicios de comunicaciones solo a entidades autorizadas. Las medidas adoptadas por los operadores para cumplir con las recomendaciones pueden tratarse al mismo tiempo, porque las soluciones disponibles suelen integrar los procesos de autenticación y acceso.

Respecto a la autenticación de usuarios, dispositivos y aplicaciones, existen numerosas alternativas que dependen del servicio en cuestión. La encuesta diagnóstica de la CRC revela que los requisitos de autenticación en los servicios móviles se encuentran estandarizados a través de la gestión de servidores

HSS[90] o HLR[91], por tanto el uso de SIM cards y SMART cards proporciona los servicios de seguridad de acceso y autenticación en servicios móviles en el 100% de ISP que prestan servicios de datos móviles.

Para el servicio de Internet fijo, los ISP utilizan servidores autenticación, autorización y contabilidad AAA (Authentication, Authorization, Accounting) con protocolo RADIUS[92] o DIAMETER[93]. El 52% de los encuestados mencionó explícitamente utilizar servidores AAA para el proceso de autenticación.

5.3.2 No rechazo / No repudio (UIT-T X.813):

El servicio de no rechazo consiste en la generación, verificación y registro de evidencia de las comunicaciones cursadas. En un entorno OSI[94], el servicio de no rechazo tiene dos modalidades: no rechazo con prueba de origen que se utiliza para hacer frente a la falsa negación del envío de datos o sus contenidos por parte de un emisor, y no rechazo con prueba de entrega que se utiliza para hacer frente a la falsa negación de que no ha recibido los datos o sus contenidos por parte de un receptor.

Teniendo en cuenta que la recomendación incluye para el no rechazo:

- El identificador distintivo del originador.
- Los datos enviados, o una huella digital de los datos.
- El identificador distintivo del receptor.
- Los datos recibidos, o una huella digital de los datos.

Específicamente para los servicios móviles, los CDRs o (Charging Data Record)[95] proporcionan a los operadores suficiente evidencia para cumplir con las recomendaciones de no rechazo.

Para los servicios de datos fijos, las necesidades de los ISP cambian radicalmente dependiendo de la base de usuarios, tecnología de acceso, paquete de servicios, etc. Es por esto que la necesidad de un

90 Nota: Home Suscriber System: es una base de datos que contiene la información relacionada con el usuario y el suscriptor. Proporciona funciones de soporte en gestión de movilidad, configuración de llamadas y sesiones, autenticación de usuarios y autorización de acceso, más información en: http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

91 Nota: Home Location Register, más información en: http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

92 RADIUS es un protocolo cliente servidor que opera en la capa de aplicación y utiliza TCP o UDP para ejecutar las funciones de AAA, más información disponible en: http://www.untruth.org/~josh/security/radius/radius-auth.html

93 Evolución del protocolo RADIUS, más información en: https://www.ibm.com/developerworks/wireless/library/wi-diameter/

94 El modelo OSI (Open Systems Interconnection) caracteriza y estandariza las funciones de las redes de comunicaciones, https://support.microsoft.com/en-us/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

95 Información estructurada que contiene los detalles que son facturables en un evento de telecomunicaciones (llamada, SMS, uso de datos, etc.) más información en: http://www.3gpp.org/ftp/Specs/html-info/32240.htm

ISP en el mercado rural que proporciona Internet es diferente a la de un proveedor de FTTH que ofrece paquetes triple play. A pesar de esto, todos los ISPs integran dentro de sus sistemas de facturación recolección de información suficiente para garantizar la contabilidad y, en consecuencia, el no rechazo de sus servicios.

En conclusión, gracias a estándares de industria integrados dentro de la arquitectura de comunicaciones puede afirmarse que el servicio de no rechazo/no repudio se encuentra debidamente implementado en los operadores colombianos.

5.3.3 Confidencialidad de los datos (UIT-T X.814):

El objetivo del servicio de confidencialidad, de acuerdo con la Recomendación UIT-T X.814 es asegurar que la información esté a disposición solamente de aquellos que tienen autorización para acceder a la misma. Para alcanzar este objetivo, los ISPs adoptan medidas de dos tipos:

1) Impedir el acceso a los datos (Mediante la protección física de un recurso, o a través de restricciones de acceso a los contenidos y aplicaciones) para permitir que sólo las entidades autorizadas tengan acceso a los datos.

2) Utilizar técnicas de cifrado de la información para hacerla inaccesible a todos salvo a las entidades autorizadas.

En la encuesta diagnóstica realizada por la CRC, el 80% de los ISPs manifestaron contar con esquemas de control de acceso físico y lógico a los elementos de red basados en roles.

Los protocolos GSM (Global System for Mobile communications) y UMTS (Universal Mobile Telecommunications System), adicionalmente, garantizan la confidencialidad de los datos mediante el uso de llaves de cifrado secretas compartidas entre el suscriptor y la red visitada como parte del protocolo de autenticación. Es así como en la encuesta adelantada por la CRC, el 100% de los operadores móviles respondieron que garantizan la confidencialidad en el segmento inalámbrico de la comunicación debido a un estándar de industria.

Frente a las medidas de cifrado de la información, el uso del protocolo HTTPS[96] garantiza el cifrado de los contenidos, a pesar de que las redes de los operadores soportan el uso de este y otros protocolos

[96] HTTPS: Protocolo seguro de transferencia de hipertexto es el protocolo de comunicaciones que garantiza la privacidad e integridad de las comunicaciones en internet a través del uso de una capa cifrada de transporte, más información disponible en: https://tools.ietf.org/html/rfc2818

para garantizar la confidencialidad de las comunicaciones, su uso efectivo depende de los certificados obtenidos por los contenidos y aplicaciones, responsabilidad que excede a los ISPs.

Finalmente, en la encuesta diagnóstica realizada por la CRC a los ISP en Colombia, el 14% de los proveedores manifestaron además contar con sistemas de prevención de fuga de información DLP (Data Loss Prevention), entre otros sistemas para protección de la confidencialidad.

5.3.4 Integridad de datos (UIT-T X.815):

Según la Recomendación UIT-T X.815, el objetivo del servicio de integridad es proteger los datos de modificaciones no autorizadas. El servicio de integridad protege contra estas amenazas mediante la prevención o la detección de estas modificaciones.

Para el caso específico de las comunicaciones móviles, el protocolo de comunicaciones[97] establece un intercambio de llaves de cifrado que garantiza la integridad de las comunicaciones cursadas entre el dispositivo del usuario y la estación base. En consecuencia, el estándar de industria garantiza la integridad de los datos en el segmento inalámbrico de la comunicación.

En otros segmentos de la comunicación, la integridad de los datos debe ser garantizada a través del uso de herramientas de monitoreo, en general los nodos core o de núcleo de las redes de comunicaciones tienen herramientas de monitoreo continuo de la integridad de los datos a través de la medición del BER[98].

5.3.5 Disponibilidad de servicio (UIT-T X.815):

El servicio de seguridad denominado disponibilidad del servicio, tiene el objetivo de garantizar que las personas y los dispositivos autorizados puedan acceder a los servicios de comunicaciones. Esta dimensión debe, por ejemplo, contemplar medidas para proteger la red contra ataques de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo, la modificación o la supresión de información administrativa de autenticación.

La encuesta diagnóstica realizada por la CRC revela que las medidas adoptadas por los proveedores de servicios de comunicaciones están ligadas a la implementación de monitoreo y gestión de eventos a

97 Zahid Ghadialy (2004), UMTS Security: A Primer, disponible en: http://www.3g4g.co.uk/Tutorial/ZG/zg_security.html
98 BER: Bit Error Rate o tasa de error de bits se obtiene calculando la cantidad de errores de bit dividido entre el número total de bits transmitidos en un intervalo de tiempo específico, recuperado de: Digital Communications, John Proakis (2007)

través de alarmas de red. Los proveedores cuentan además con esquemas de redundancia que apuntan a maximizar el tiempo de disponibilidad de red. El 30% de los operadores manifestó implementar arquitecturas de alta disponibilidad (HA)[99].

6 CONCLUSIONES Y RECOMENDACIONES

Los análisis adelantados revelan la creciente importancia de la seguridad digital en la operación de cualquier empresa del ecosistema digital, la confianza es un habilitador tan importante como la conexión misma en las interacciones y actividades del mundo digital.

Teniendo en cuenta las múltiples partes interesadas en la gestión de la seguridad digital, se presentan a continuación una serie de propuestas y recomendaciones orientadas a mejorar la capacidad de gestionar los riesgos de seguridad digital en todo el entorno digital.

6.1 Aspectos asociados a las redes de los PRST

6.1.1 Seguridad de red

Teniendo en cuenta la evolución que han tenido los modelos de seguridad para empresas de telecomunicaciones, desde que fueron adoptados en el marco normativo colombiano por primera vez en 2009, y aun cuando las recomendaciones internacionales UIT-T de la serie X.800 corresponden a arquitecturas de seguridad que se han convertido en referencia de la industria, es importante reconocer la tendencia global y nacional de adopción de mejores prácticas de seguridad, las cuales fueron documentadas a lo largo del estudio. Es así como esta Entidad considera que existe una oportunidad para actualizar las previsiones del marco regulatorio en materia de seguridad digital, de forma que el mismo integre la visión planteada en la Política Nacional de Seguridad Digital delineada en el CONPES 3854 de 2016 "*Fortalecer las capacidades de las múltiples partes interesadas para identificar,* ***gestionar, tratar y mitigar los riesgos de seguridad digital*** *en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia*".

En este sentido, la CRC propone a todas las partes interesadas la modificación del artículo 5.1.2.3 SEGURIDAD DE RED del Capítulo 1 del Título V de la Resolución compilatoria CRC 5050 de 2016, el cual quedará de la siguiente manera:

[99] Los sistemas de alta disponibilidad implementan arquitecturas específicas para garantizar un nivel superior de disponibilidad – más información en: https://msdn.microsoft.com/en-us/library/cc750543.aspx

"Los proveedores de redes y servicios de telecomunicaciones deben utilizar los recursos técnicos y logísticos tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de los servicios de comunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, implementando para ello un Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con las características y necesidades propias de su red, siguiendo la recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1051 – Código de prácticas en materia de controles de seguridad de la información basados en la norma ISO/CEI 27002 para organizaciones de telecomunicaciones.

El SGSI implementado debe ser acorde con el marco de gestión de la seguridad de la información descrito en la recomendación UIT-T X.1052, así como las categorías de controles de seguridad para organizaciones de telecomunicaciones definidos en la Recomendación UIT-T X.1051, como lo son: gestión de activos (UIT-T X.1057), gestión de incidentes (UIT-T X1056), gestión de riesgos (UIT-T X.1055), gestión de políticas (UIT-T X.1054), gestión de organización y personal, adquisición de sistemas y capacidades, gestión de operaciones y de mantenimiento."

Lo anterior implica que los operadores deben implementar un sistema de gestión de seguridad de la información (SGSI), ajustando los procesos de los PRST para que estos permitan gestionar de manera eficiente la información, y asegurar la integridad, confidencialidad y disponibilidad de los datos.

Si bien los tiempos de implementación de la recomendación varían de acuerdo con el tamaño y el perfil de riesgos específicos de cada empresa de telecomunicaciones, para permitir un plazo adecuado de implementación de la medida, se propone la entrada en vigencia del artículo anterior el 1º de enero de 2019.

6.1.2 Información de incidentes de seguridad

Teniendo en cuenta la falta de información estadística sobre incidentes de seguridad con impacto significativo en los servicios de comunicaciones, así como la ausencia de datos sobre las causas de incidentes de seguridad, se considera importante proporcionar a las entidades encargadas de la seguridad digital en el país, a los responsables de formular políticas públicas en materia de seguridad digital, al público y a la industria en general, un análisis de los insumos necesarios para generar un reporte estadísticamente relevante de los incidentes, que pueda evidenciar la frecuencia y el impacto de los mismos en el sector de las comunicaciones en Colombia.

Esta información permitirá al sector y a las entidades encargadas de la seguridad y defensa en el entorno digital mejorar la comprensión y abordar tipos específicos de incidentes de seguridad o vulnerabilidades. Esta información también será relevante para evaluar la efectividad de las medidas de seguridad propuestas y orientar la política regulatoria del sector sobre las medidas de seguridad.

Por tanto, se propone a los proveedores de servicios de internet y telefonía, determinar, almacenar y tener a disposición de las autoridades pertinentes la información sobre los incidentes de seguridad o de pérdida de integridad de la red[100] que hayan afectado de manera significativa su base de usuarios.

Para efectos de lo anterior se entenderá **incidente de seguridad**[101] como una violación de la seguridad o una pérdida de integridad que podría tener un impacto en la operación de redes y servicios de telecomunicaciones.

La **integridad de red** se entenderá de acuerdo con las definiciones disponibles en la literatura técnica, esto es, la capacidad del sistema para mantener sus atributos especificados en términos de rendimiento y funcionalidad. En línea con la definición de la UIT:

> **Característica de integridad del servicio**[102]: capacidad de un servicio para cumplir sus objetivos sin degradaciones excesivas, una vez obtenido. La integridad del servicio está determinada principalmente por las características de transmisión de la red.

---

100 Los mantenimientos programados, previamente informados a la división de vigilancia y control del Ministerio de las Telecomunicaciones, no se entenderán como incidentes de pérdida de integridad de red.

101 ENISA. (2013). *Technical Guideline on Incident Reporting.* Recuperado de https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

102 Recomendación UIT-R M.1224, - § 4.1

Así mismo, se entenderá por **afectación significativa** aquella que cumple con los umbrales cuantitativos definidos así[103]:

Duración del incidente / Usuarios afectados	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1%-2%	NO	NO	NO	NO	SI
2%-5%	NO	NO	NO	SI	SI
5%-10%	NO	NO	SI	SI	SI
10%-15%	NO	SI	SI	SI	SI
>15%	SI	SI	SI	SI	SI

Nota: el porcentaje de usuarios de la columna uno se calculará sobre la base de usuarios del servicio específico de comunicaciones de acuerdo con el último trimestre reportado.

La información sobre el incidente de seguridad o pérdida de integridad debe incluir:

Fecha del Incidente	Servicio afectado	Número de usuarios afectados	Duración	Causa del incidente

1. **Fecha del incidente:** La fecha de inicio del incidente.
2. **Servicio afectado:** deberá indicarse uno o más de los servicios afectados por el incidente de indisponibilidad:
    a. Internet Fijo.
    b. Internet Móvil.
    c. Telefonía fija.
    d. Telefonía Móvil.
3. **Número de usuarios afectados:** Para telefonía fija e Internet fijo, deben indicarse el número de suscriptores afectados.

Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

[103] Umbrales alineados con la recomendación de la guía técnica de reporte de incidentes ENISA

4. **Duración:** en el campo duración debe indicarse el tiempo en horas de indisponibilidad del servicio.
5. **Causa del incidente:** este campo debe indicar la causa raíz del incidente de indisponibilidad del servicio, el operador deber indicar una de las siguientes categorías de causas raíz:

    a. Error humano: esta categoría debe utilizarse cuando el incidente sea causado por un error humano durante la ejecución de actividades y procedimientos de operación de la infraestructura o aplicaciones del proveedor.

    b. Error de sistema: este ítem debe utilizarse cuando el incidente sea causado por fallos de sistema, bien sea de hardware o de software.

    c. Fenómenos Naturales: este ítem se diligencia cuando el incidente se produce por daños causados por fenómenos naturales como incendios, terremotos, inundaciones, etc.

    d. Actores maliciosos: en este ítem se incluyen los incidentes son causados por la acción deliberada de un actor u organización.

    e. Fallas externas al operador: esta categoría debe utilizarse cuando la causa raíz del incidente se presenta por causas fuera del control del operador, como por ejemplo incidentes causados por actores externos durante el mantenimiento de una vía, cortes prolongados de energía causados por el proveedor de energía eléctrica, etc.

Finalmente, cuando se trate de incidentes que afecten significativamente el servicio de acuerdo con los umbrales definidos y la causa del incidente sean actores maliciosos, deberá enviarse por medios electrónicos, dentro de los 120 minutos subsecuentes a la determinación del incidente un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) que incluya los elementos descritos (fecha del incidente, servicio afectado, número de usuarios afectados, duración, causa del incidente) y una descripción del incidente, así como de las acciones llevadas a cabo por el operador para mitigar o resolver el incidente. Asimismo, se recuerda que aquellos incidentes que representen afectación de los datos personales deber ser notificados a la Delegatura para la Protección de datos Personales de la Superintendencia de Industria y Comercio, de acuerdo con lo dispuesto en la Ley de Protección de Datos Personales (Ley 1582 de 2012).

Teniendo en cuenta que hasta el momento no se tiene información sobre la frecuencia de los impactos de seguridad, se propone que los PRST efectúen la recolección de los datos, de acuerdo con los

parámetros indicados, durante el periodo de enero 1 a diciembre 31 de 2018, y en enero de 2019 los PRST deberán entregar a esta Comisión los datos recolectados con la información de 2018, lo cual permitirá revisar y analizar la pertinencia de posibles necesidades adicionales para la gestión de seguridad en las redes.

Como se mencionó anteriormente, a la fecha no existe información sobre los incidentes de seguridad en las redes de comunicaciones. Si bien el Formato 2.7 *INDICADORES DE DISPONIBILIDAD PARA LOS SERVICIOS DE TELECOMUNICACIONES PRESTADOS A TRAVÉS DE REDES FIJAS Y REDES MÓVILES,* estableció la información para determinar la disponibilidad de los elementos de red, como parte de los indicadores del Régimen de Calidad de que trata el Título V de la Resolución CRC 5050 de 2016, es importante mencionar que dicho formato está asociado a los elementos de red, y no al servicio. Aunque ligado a los incidentes de seguridad y la integridad de la red, no permite identificar las causas de los incidentes ni mucho menos determinar la pertinencia de las condiciones de seguridad frente a las condiciones de integridad de red.

6.1.3 Colaboración interinstitucional

Se recomienda a los equipos de seguridad, equipos de respuesta a incidentes informáticos (CERTs/CSIRTs) y centros de operación de seguridad (SOC) de los proveedores de servicios de comunicaciones, establecer mecanismos que permitan la coordinación de los esfuerzos de respuesta entre las partes involucradas en los incidentes, incluyendo no solo a las víctimas del incidente, sino también otras partes involucradas en el incidente, como pueden ser otros CSIRT y administradores de sistemas y redes, las autoridades nacionales de ciberseguridad y ciberdefensa (colCERT, CCP y CCOC) y la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio. Se recomienda la notificación a las partes de su posible participación (fuente de un incidente, destinatario o autoridad competente) y la facilitación del intercambio y análisis de información.

6.1.4 Mejores prácticas operacionales recomendadas por la Internet Society

Dado el potencial de las cuatro mejores prácticas operacionales identificadas por Internet Society e IETF para prevenir y contrarrestar una amplia variedad de incidentes de seguridad de la información como los ataques de denegación de servicio y el phishing, prácticas que fueron documentadas en la sección 4.2 de este documento (IPV6, DNSSEC, Aseguramiento del BGP, y prevención de la falsificación de direcciones IP), se recomienda a los operadores de comunicaciones considerar la implementación donde sea apropiado de las mejores prácticas operaciones BCP-38, BCP-194, adopción del protocolo IPv6 y adopción del protocolo DNSSEC.

Durante el análisis de información estadística de incidentes de seguridad planteado para enero de 2019 se analizarán las siguientes variables asociadas a las mejores prácticas identificadas:

Tabla 6 Indicadores despliegue mejores prácticas

Indicador	Fuente
Índice compuesto IPv6	6lab Cisco
Penetración DNSSEC	APNIC Labs
Falsificación de direcciones IP	Spoofer CAIDA

6.2 Aspectos asociados con el Ministerio de las Tecnologías de la Información y las Comunicaciones.

6.2.1 Vigilancia y control de las medidas

Teniendo en cuenta la necesidad de realizar la vigilancia y el control de la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI) en los operadores, se recuerda que la Recomendación UIT-T X.1051 es desarrollada a partir del estándar ISO/IEC 27002, el cual define numerosos *controles de seguridad* específicos sobre los cuales es posible obtener evidencias a partir de la documentación del SGSI. Se recomienda a la División de Vigilancia y Control del MINTIC desarrollar y discutir con las múltiples partes interesadas, un documento de verificación y vigilancia de los controles específicos para evaluar la efectiva implementación de los SGSI propuestos.

6.2.2 Sobre la iniciativa IPv6

En línea con el objetivo del MinTIC de promover que todas las entidades del gobierno, las empresas privadas, la academia y en general todos los colombianos se conecten a Internet usando el protocolo IPv6, ha dado un importante paso con la expedición de la Resolución 2710 de 2017. Las disposiciones de esta resolución tendrán un efecto directo en el indicador de adopción de IPv6 en usuarios finales, lo cual es positivo Sin embargo, es importante que el Ministerio continúe la actividad de promoción en el sector privado y en los PRSTs.

6.2.2 Recomendación Usuarios

En el presente estudio se observó que muchos de los incidentes digitales tienen origen directo en error humano, por lo cual es importante generar conciencia a los usuarios de telecomunicaciones respecto al uso adecuado de Internet. Así, iniciativas del Gobierno como "Ciudadanía Digital[104]" y "En TIC Confío[105]" son estrategias que abren espacios para educar al ciudadano en torno al buen uso de Internet.

Por un lado, Ciudadanía Digital ofrece 28 cursos a Colombianos mayores de 13 años que estén interesados en contenidos digitales, tres de estos cursos están relacionados con Seguridad Digital: I. Prevenir para estar seguros en digital[106], II. Experiencias digitales seguras[107] y III. Redes sociales y medios digitales, una oportunidad para los jóvenes[108]. Por otro lado, en TIC Confío ofrece a la ciudadanía herramientas para enfrentar los riesgos asociados al uso de nuevas tecnologías, como el phishing, el ciberacoso, la ciberdependencia y el abuso de menores de edad, entre otros. Esta última está dirigida a todos los ciudadanos y se realiza a través de la Cátedra Poder Digital, gratuita y de 45 minutos de duración[109].

Por lo anterior, se recomienda al MinTIC que continúe promoviendo esta clase de escenarios pedagógicos para los usuarios de telecomunicaciones y que los mismos cuenten con mayor visibilidad, de forma que se logre generar y promover la responsabilidad digital desde la ciudadanía en general.

6.3 Recomendaciones a colCERT/CCP/CCOC

La encuesta diagnóstica realizada por la CRC revela que solo el 23% de los PRSTs en Colombia, coordinan sus acciones con el colCERT.

---

104 La Ciudadanía Digital es el resultado de la transformación digital y productiva de los ciudadanos. Ante el reto de la economía digital, como país se tiene la meta de impulsar esa transformación en los próximos años. Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-channel.html

105 Estrategia de promoción de uso responsable de internet y de las nuevas tecnologías del Ministerio de Tecnologías de la Información y las Comunicaciones. Ayuda a la sociedad a desenvolverse e interactuar responsablemente con las TIC, al tiempo que promueve la cero tolerancia con la pornografía infantil y la convivencia digital. Para mayor información, ver: https://www.enticconfio.gov.co/

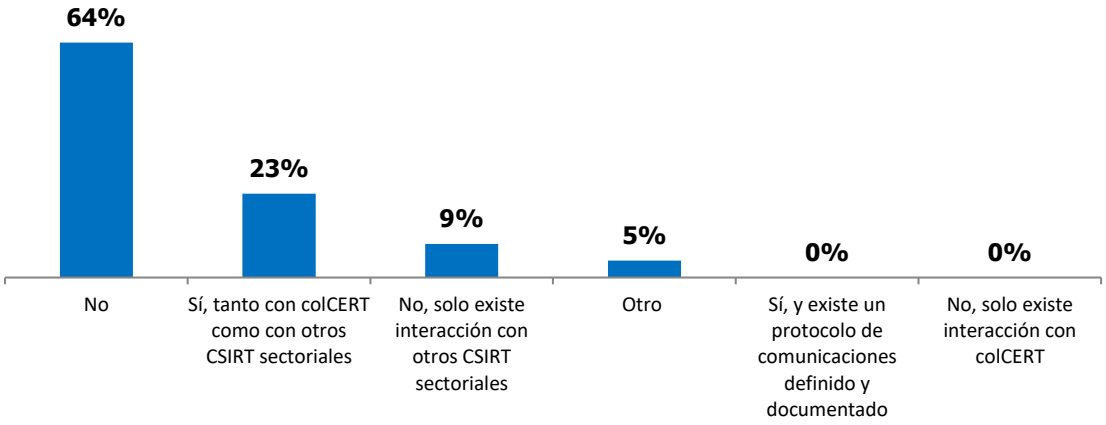
106 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60958.html

107 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60956.html

108 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60957.html

109 Para mayor información, ver: http://www.enticconfio.gov.co/

Gráfica 32 ¿El equipo responsable de la gestión de incidentes de seguridad informática se coordina con el colCERT y otros CSIRT del sector?



Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

Frente a estos resultados, existe una oportunidad para colCERT, como organismo coordinador a nivel nacional con otros organismos de ciberseguridad y ciberdefensa tales como el CCP y el CCOC, de convertirse en el punto focal nacional para la gestión de incidentes digitales en Colombia. Se recomienda, como parte de las acciones para alcanzar este objetivo, que el colCERT desarrolle protocolos específicos para el intercambio de información con los CSIRT y los equipos de seguridad del sector de las telecomunicaciones, de manera que pueda incrementarse de manera orgánica el nivel de cooperación actual.

De otra parte, teniendo en cuenta la propuesta de reporte de incidentes de seguridad al colCERT cuando estos sean ocasionados por actores maliciosos, se abre una oportunidad para que el colCERT genere informes sobre la incidencia e impacto de los incidentes de seguridad digital en el sector de las telecomunicaciones, así como recomendaciones específicas que puedan contribuir a gestionar los riesgos de seguridad digital por parte de los proveedores de servicios de comunicaciones.

La experiencia Internacional de Brasil y Estados Unidos, revela que desarrollar un sistema web con las medidas de cifrado adecuadas, puede mejorar la eficiencia en la recepción de reporte de incidentes. Se recomienda al colCERT estudiar la posibilidad de desarrollar un sistema como el NORS (Network Outage

Reporting System)[110] usado en EE. UU. donde se facilite el reporte de incidentes y se garantice la confidencialidad de la información.
Frente a la identificación de la infraestructura crítica en el sector de las telecomunicaciones, se recomienda al CCOC, una vez completado el inventario de infraestructuras críticas que se encuentra en etapa de desarrollo, y teniendo en cuenta las características particulares del sector de las telecomunicaciones, trabajar en conjunto con la CRC y el MinTIC en el desarrollo de una metodología de protección de infraestructuras críticas de telecomunicaciones, que pueda dar cuenta de la interdependencia de la infraestructura y analizar las amenazas específicas del sector con base en el análisis de riesgos específicos de los SGSI[111] que serán implementados por los PRSTs, de manera análoga a la experiencia documentada en el análisis internacional para el caso de Brasil.

7 PARTICIPACIÓN DEL SECTOR

Atendiendo el procedimiento establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, los documentos publicados son sometidos a consideración del Sector a partir de su publicación por el término de 10 días hábiles.

Los comentarios a la propuesta regulatoria serán recibidos a través del correo electrónico: seguridad.digital@crcom.gov.co, vía fax al (+57 1) 3198301, a través las redes sociales de la CRC en Twitter (@CRCCol) o en la página de Facebook "Comisión de Regulación de Comunicaciones", o en las oficinas de la CRC ubicadas en la Calle 59A Bis No. 5 – 53 Piso 9, Edificio Link Siete Sesenta, de la ciudad de Bogotá D.C.

No serán tenidos en cuenta los comentarios que se reciban respecto de disposiciones que no estén contenidas en la propuesta publicada.

110 https://www.fcc.gov/network-outage-reporting-system-nors
111 Sistemas de Gestión de Seguridad de la Información

Bibliografía

Centro Cibernético Policial. (2017). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Cisco. (2017). *Informe de ciberseguridad anual de Cisco 2017*. Recuperado de https://www.cisco.com/c/dam/m/digital/1226019/Cisco_2017_ACR_es-xl.pdf

Comisión de Regulación de Comunicaciones. (2017). *Resolución CRT 2258 de 2009*. Recuperado de https://normograma.info/crc/docs/resolucion_crc_2258_2009.htm?q=2258

Comisión de Regulación de Comunicaciones. (2017). *El Comercio Electrónico en Colombia, Análisis Integral y Perspectiva Regulatoria*. Recuperado de https://www.crcom.gov.co/recursos_user/2017/ComElecPtd_0.pdf

Comisión Europea. (2017). Telcoms Rules. Recuperado de https://ec.europa.eu/digital-single-market/telecoms-rules

Comisión Europea. (2017). *Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*. Recuperado de http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=ES

Conpes 3701. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. Recuperado de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Conpes 3854. (2016). *Política nacional de seguridad digital*. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

ENISA. (2012). *Shortlisting network and information security standards and good practices*. Recuperado de https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

ENISA. (2013). *Technical Guideline on Incident Reporting.* Recuperado de https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

ENISA. (2014). *Technical Guideline on Security measures for Article 4 and Article 13a.* Recuperado de https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article13a/TechnicalGuidelineonSecuritymeasuresforArticle4andArticle13a_version_1_0.pdf

ENISA. (2015). *Guideline for Threats and Assets*. Recuperado de https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

FCC. (2016). *Protecting and Promoting the Open Internet*. Recuperado de https://apps.fcc.gov/edocs_public/attachmatch/DA-16-271A1_Rcd.pdf

FCC. (2017). *White Paper: Cybersecurity Risk Reduction*. Recuperado de https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf

ICLG, China Telecoms. (2017). *Media & Internet Laws & Regulations.* Recuperado de http://www.kwm.com/~/media/library/Files/Knowledge/Insights/au/2016/10/12/iclg-telecoms-media-internet-2017-china.ashx?la=en

Imprenta Nacional de Colombia. (2017). *Diario Oficial N. 50376, 4 de octubre de 2017*. Recuperado de http://jacevedo.imprenta.gov.co/tempDownloads/50D3761508334567108.pdf

Information Technology and Innovation Foundation. (2015). *Cross-Border Data Flows Enable Growth in All Industries* Recuperado de http://www2.itif.org/2015-cross-border-data-flows.pdf

International Telecommunication Union, ITU. (2016). *Measuring the Information Society Report 2016*. Recuperado de https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf

JOIN. (2013). *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Recuperado de http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do

Kaspersky Lab. (2013). *Security Bulletins*. Recuperado de http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

Kaspersky Lab. (2014). *Security Bulletins*. Recuperado de https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf

Kaspersky Lab. (2015). *Security Bulletins*. Recuperado de https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Kaspersky Lab. (2016). *Security Bulletins*. Recuperado https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf

KPMG. (2017). *Overview of China's Cybersecurity Law*. Recuperado de https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

McKinsey Global Institute. (2016). *Digital Globalization: The New Era of Global Flows*. Recuperado de http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

MinTIC, OEA y BID. (2017). Recuperado de https://publications.iadb.org/bitstream/handle/11319/8552/Impacto_de_los_incidentes_de_seguridad_digital.pdf?sequence=1&isAllowed=y

MinTIC. (2016). *Seguridad y privacidad de la información.* Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity.* Recuperado de http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

Symantec Corporation. (2017). *Internet security threat report*. Recuperado de https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq

Zahid Ghadialy. (2004), UMTS Security: A Primer, disponible en: http://www.3g4g.co.uk/Tutorial/ZG/zg_security.html

ANEXO 1. ENCUESTA: DIAGNÓSTICO SEGURIDAD DIGITAL CRC

Con el propósito de conocer la adopción de buenas prácticas de gestión de riesgos de seguridad digital y evaluar el estado de implementación de modelos de seguridad en los operadores de redes en Colombia, la CRC realizó una encuesta al grupo objetivo con una muestra de 38 PRST, los cuales representan el 99% de la base de suscriptores del mercado, ahora bien, a la encuesta respondieron aproximadamente 24 PRST, siendo esta una muestra significativa con una participación del 95% de la base de suscriptores del mercado.

La encuesta se estructuró de la siguiente forma: una primera sección de preguntas estuvo enfocada en adelantar un **Diagnóstico**, con el objetivo de evaluar los modelos de seguridad implementados para cumplir con la normatividad vigente por parte de los PRST.

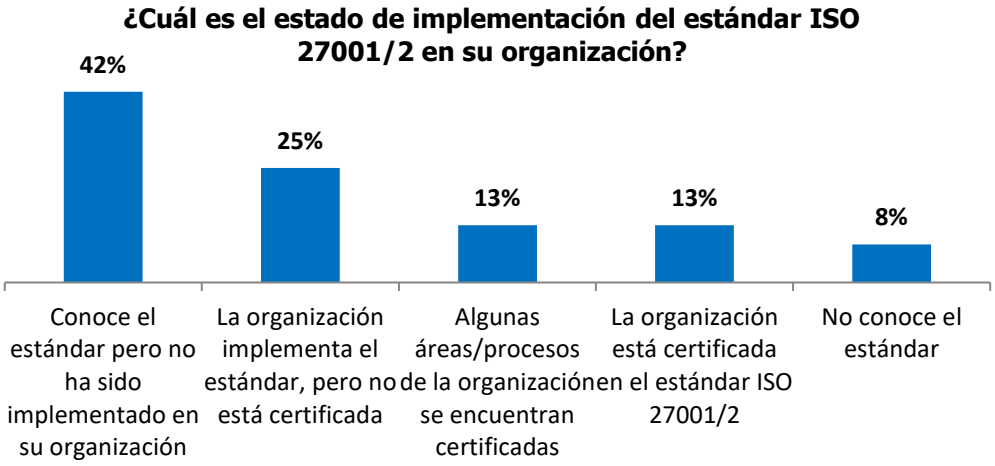
En un segundo aparte se indagó sobre la **Cooperación Institucional**, sección que tiene por objeto conocer los mecanismos de interacción entre la organización y la institucionalidad encargada de la gestión de incidentes de seguridad digital. Para esta sección se adoptó la definición de incidente del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), en el cual un incidente de seguridad informática o incidente de seguridad de la información es una violación o una amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas de seguridad estándar. Ejemplos de incidentes son:

- Un atacante ordena a una botnet enviar grandes volúmenes de peticiones de **conexión a un servidor web, causando que el mismo falle.**
- Los usuarios son engañados para que abran un "informe trimestral" enviado por correo electrónico **que es realmente malware; como consecuencia los equipos de los usuarios han sido infectados y han establecido conexiones con un host externo.**
- Un atacante obtiene datos confidenciales y amenaza con que los detalles se publiquen públicamente si la organización no paga una suma de dinero designada.
- Un usuario proporciona o expone información sensible a terceros a través de servicios de intercambio de archivos peer-to-peer.

En una tercera y cuarta sección se realizaron preguntas orientadas a visibilizar la preparación y el estado de despliegue del protocolo **IPV6** y **DNSSEC** dentro de las redes de los operadores en Colombia. En su orden, se indagó sobre las **Técnicas anti forjado de IP**, con el objetivo de conocer los controles implementados por los ISP para evitar el forjado de direcciones IP en sus redes.

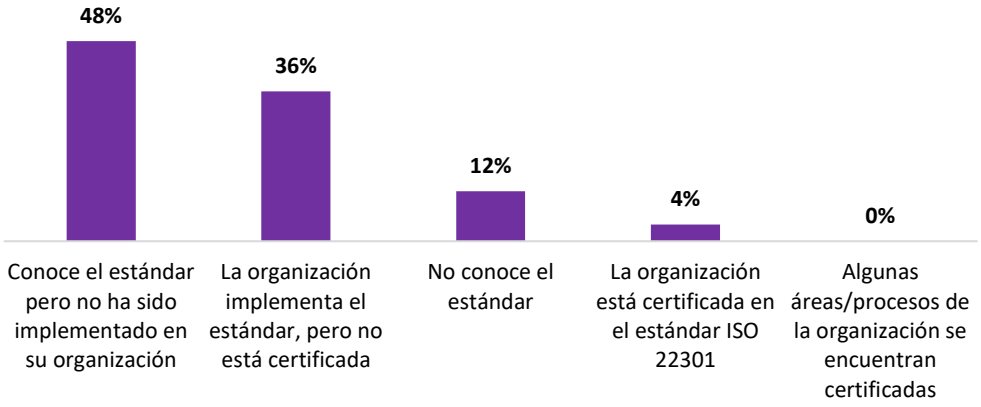
Finalmente, el punto 6 y 7 de la encuesta estuvieron orientados, por un lado, en conocer el estado del **Aseguramiento del BGP**, es decir sobre los controles implementados por los ISP para asegurar la integridad del protocolo de puerta de enlace de frontera, así como, conocer la incidencia del fenómeno de **Suplantación de tarjetas SIM card** en Colombia, respectivamente. A continuación, se describen los principales resultados de la encuesta:

I. Prácticas de seguridad implementadas por los PRST en línea con la normatividad vigente



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

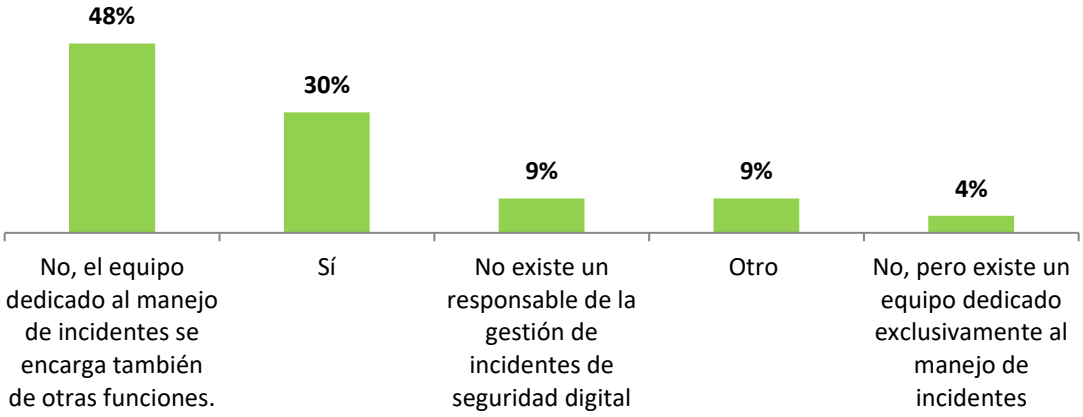
¿Cuál es el estado de implementación del estándar ISO 22301 en su organización?



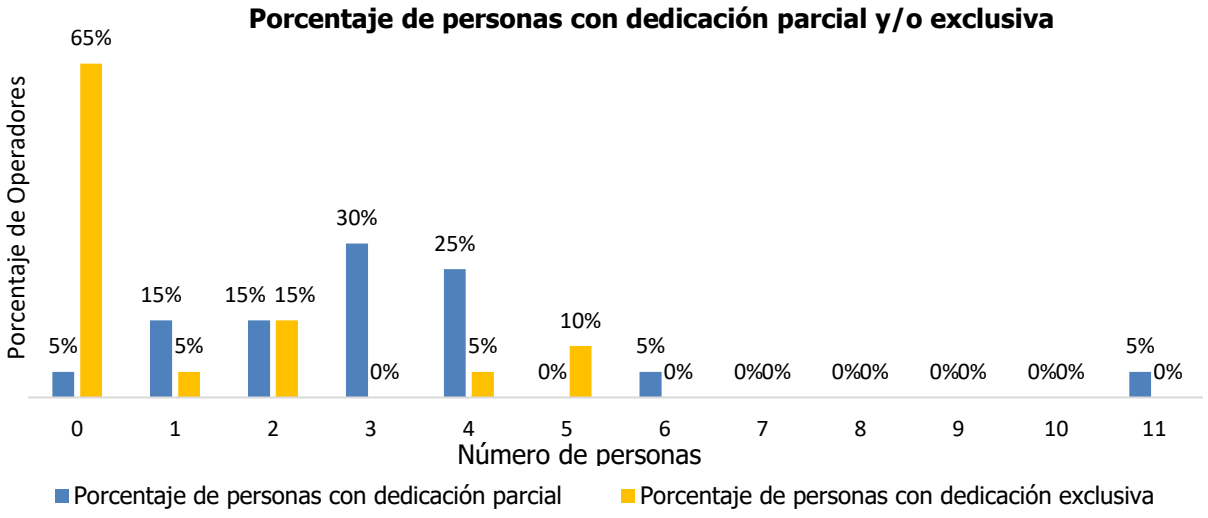
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

II. ¿Existe Cooperación Interinstitucional de los PRST con las entidades encargadas de los incidentes de seguridad?

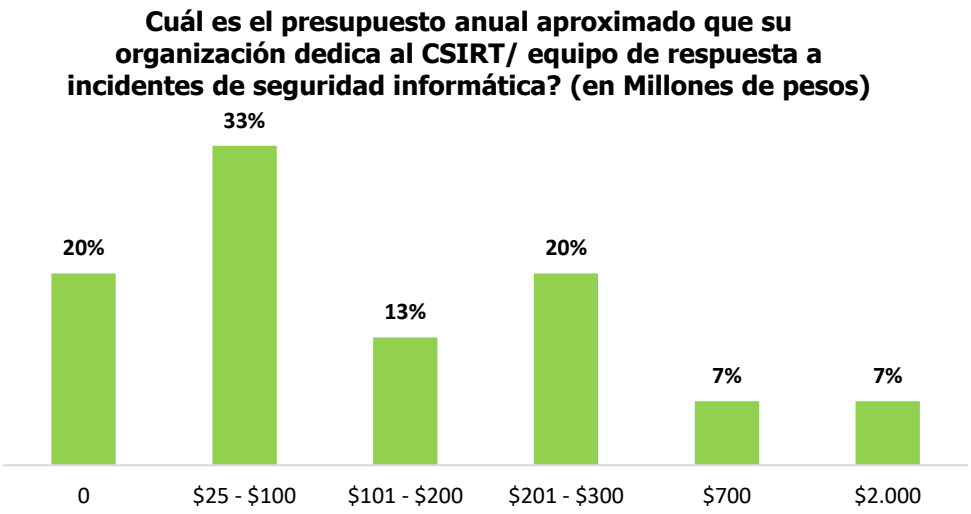
¿Cuenta su organización con un equipo de respuesta a incidentes de seguridad informática CSIRT?



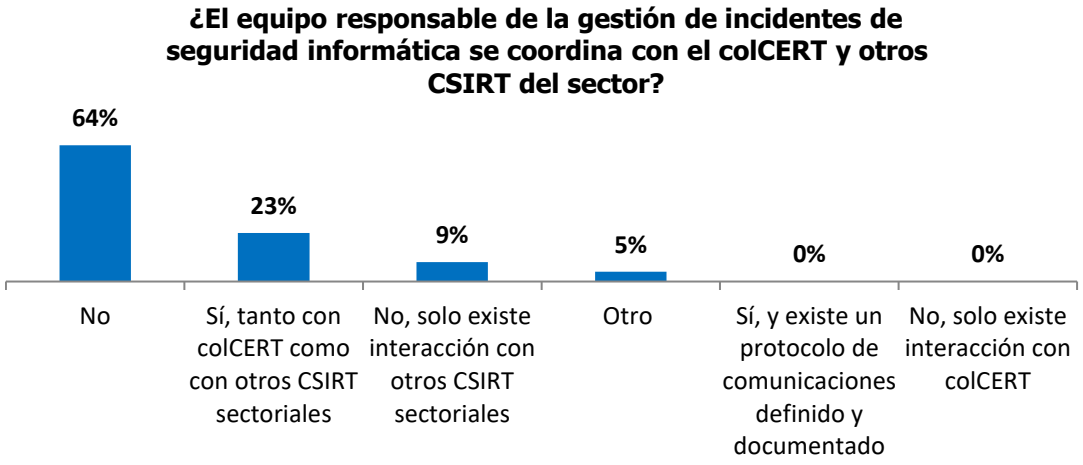
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC



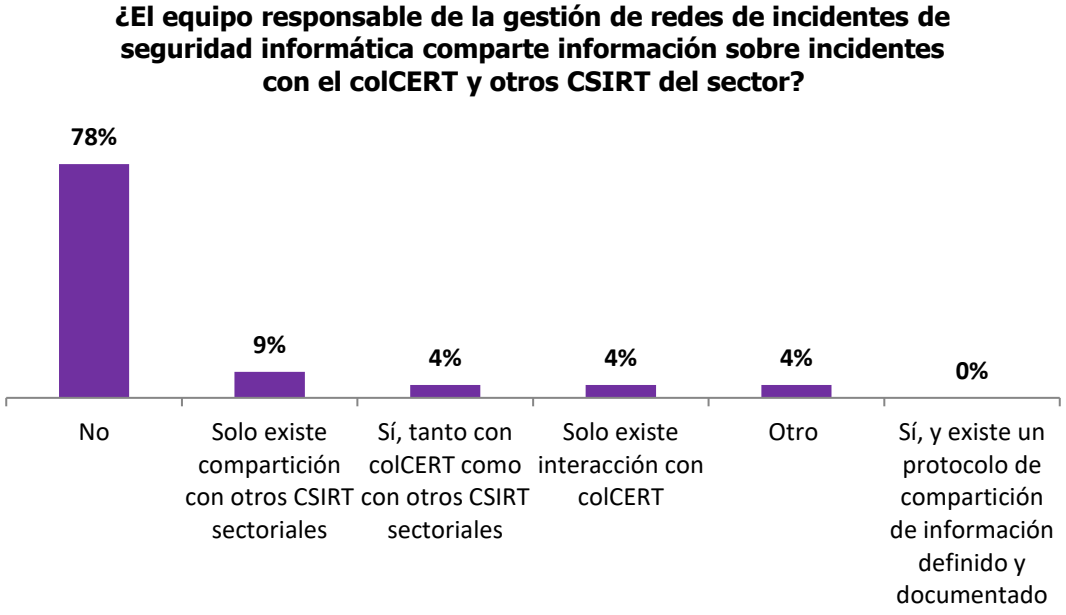
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC



Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

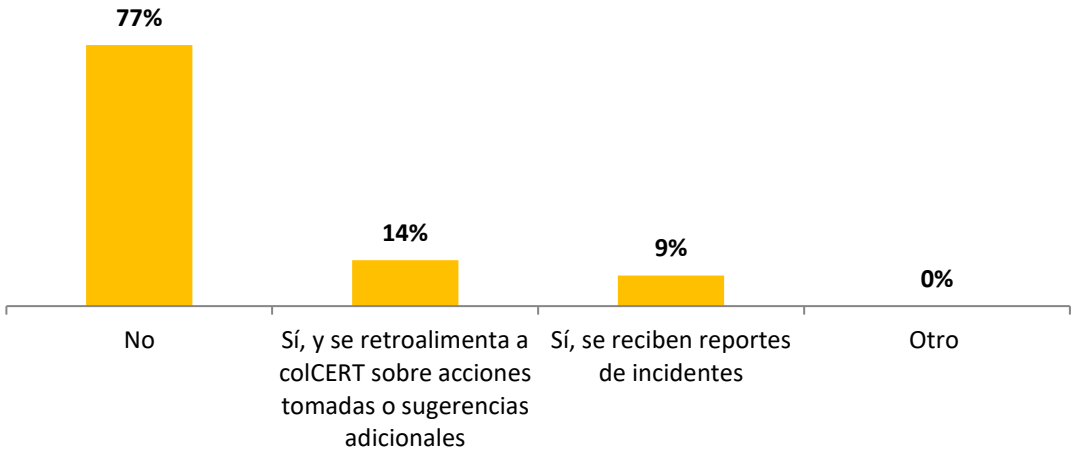


Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC



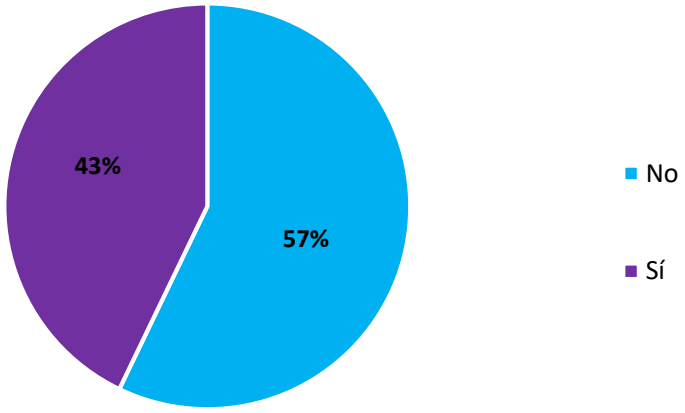
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Recibe su organización reportes de incidentes de seguridad informática emitidos por el colCERT?



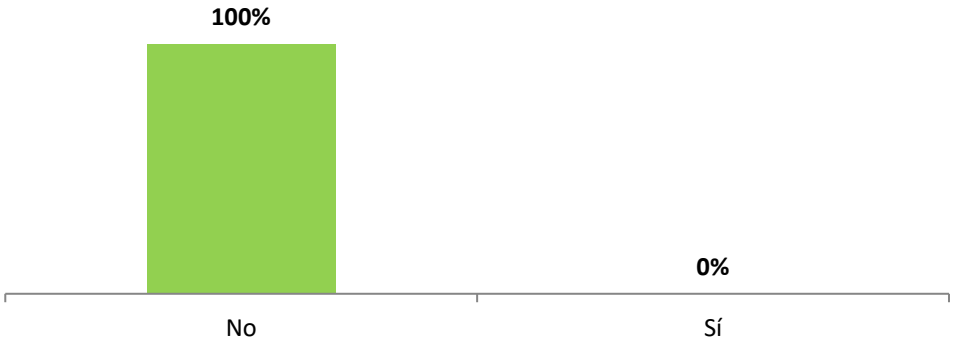
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Ha definido su organización algún protocolo y puntos de contacto para realizar reportes de incidentes a la SIC?



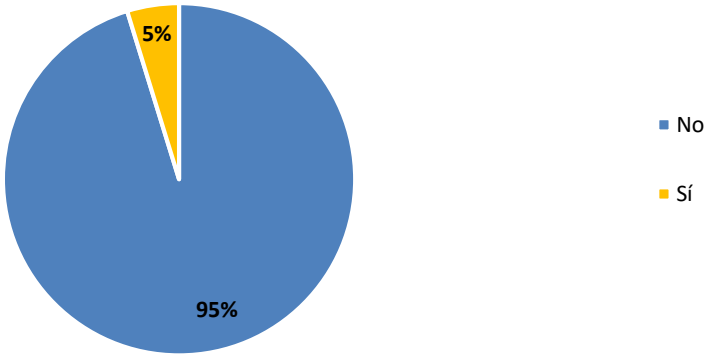
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Ha realizado su organización durante los últimos 3 años algún reporte a la delegatura para la protección de datos personales de la SIC por incidentes de vulneración?

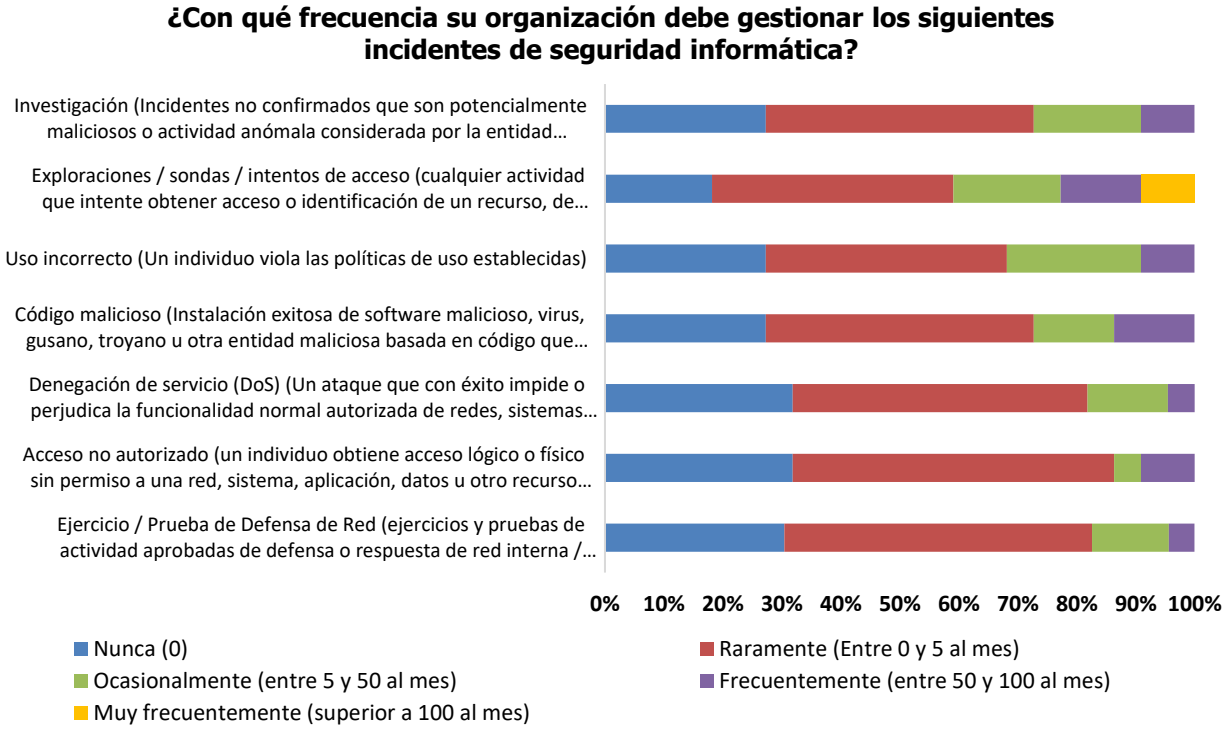


Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Ha realizado su organización durante los últimos 3 años algún reporte directamente a los usuarios por incidentes de vulneración a los sistemas donde se gestionan sus datos personales?

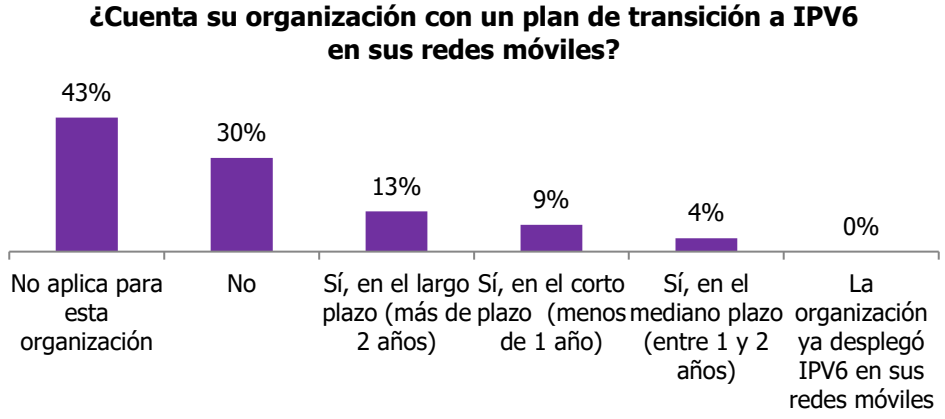


Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**



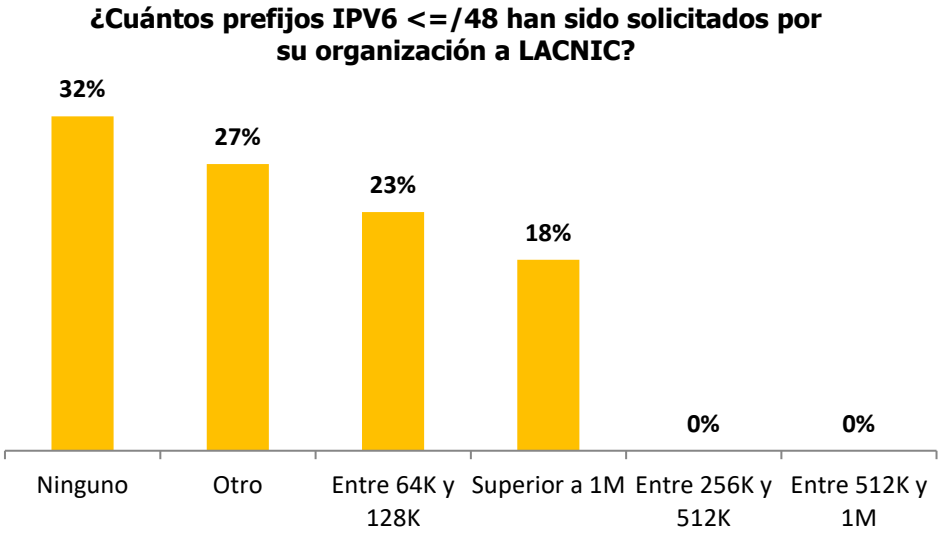
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

III. Estado de despliegue de IPv6



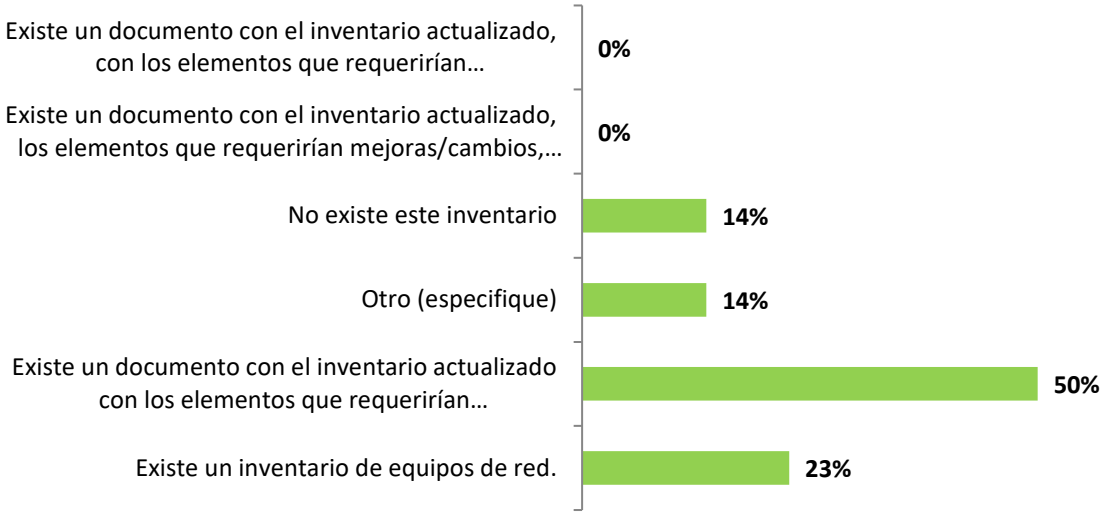
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**



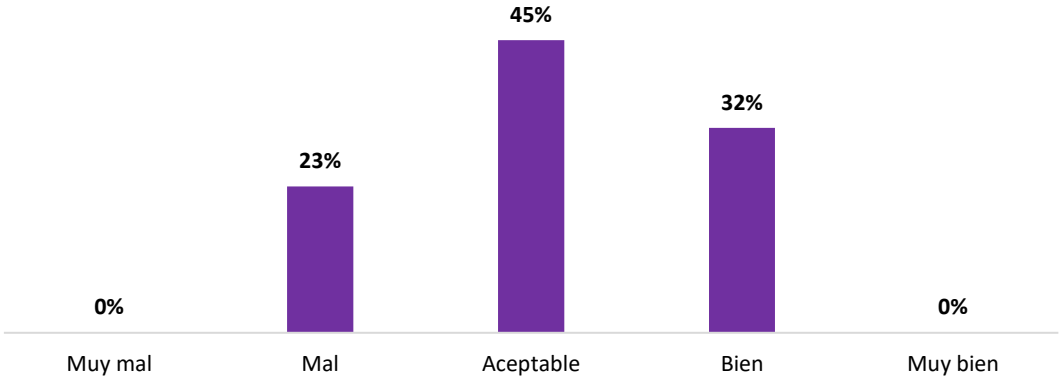
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Cuenta su organización con un inventario de equipos de red y cuáles de ellos requerirían mejoras/cambios para dar soporte IPV6?



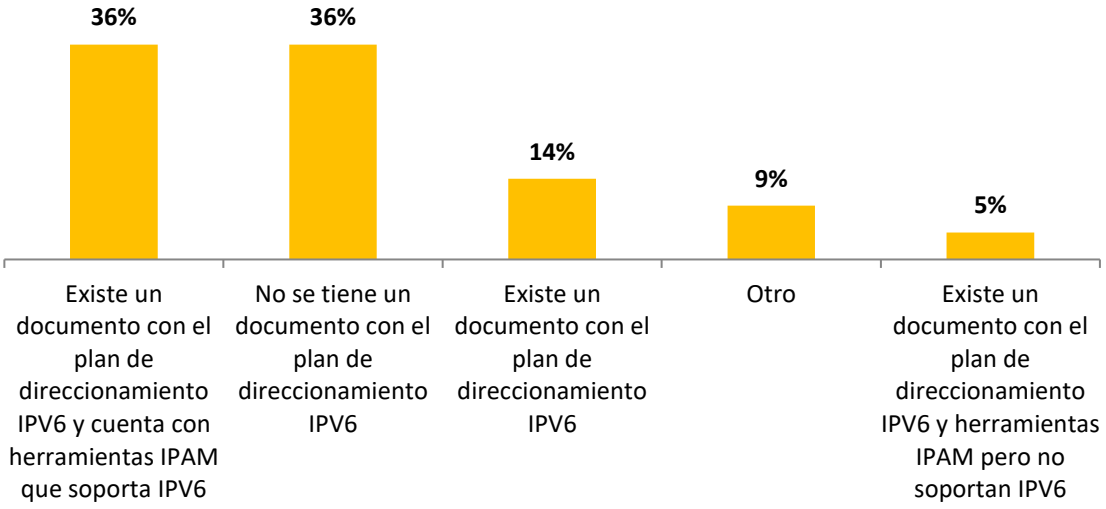
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿En la siguiente escala defina qué tan bien capacitado se encuentra el personal de su organización para desplegar IPV6?



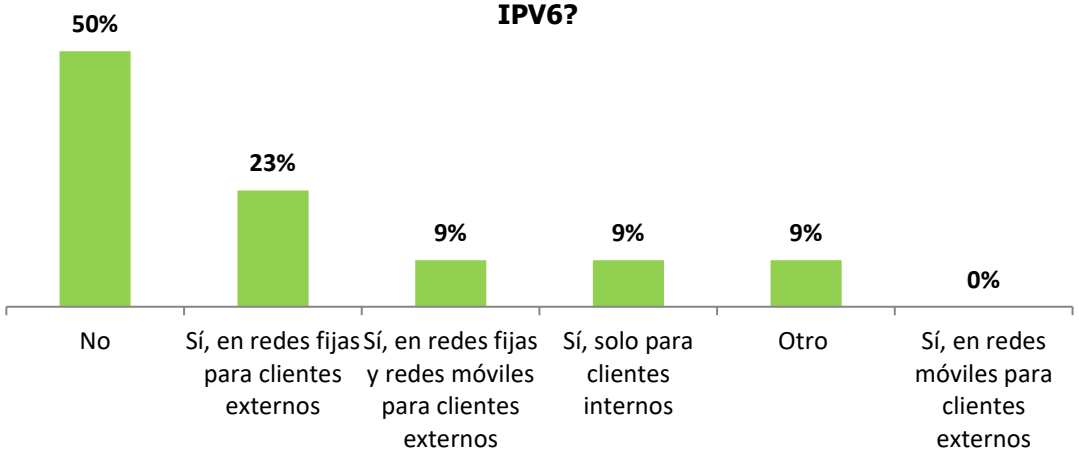
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Su organización cuenta con un plan de direccionamiento IPV6 y herramientas IPAM para la gestión del espacio de direcciones?



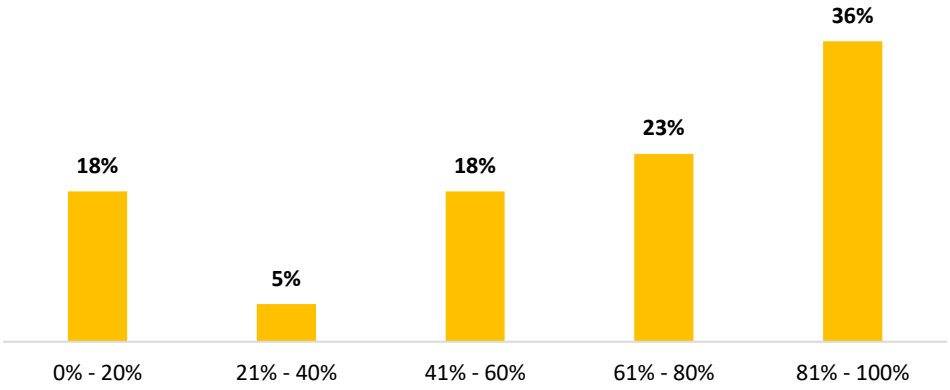
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Ha realizado su organización pruebas/ensayos de despliegue IPV6?



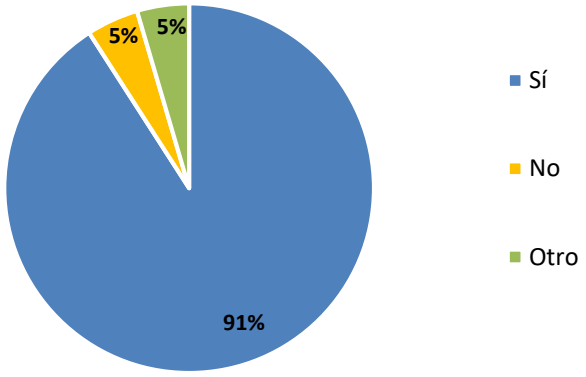
Fuente: **Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC**

¿Qué porcentaje de los dispositivos CPE (Ubicado en el domicilio del cliente) soportan dual stack (IPV4/IPV6)?



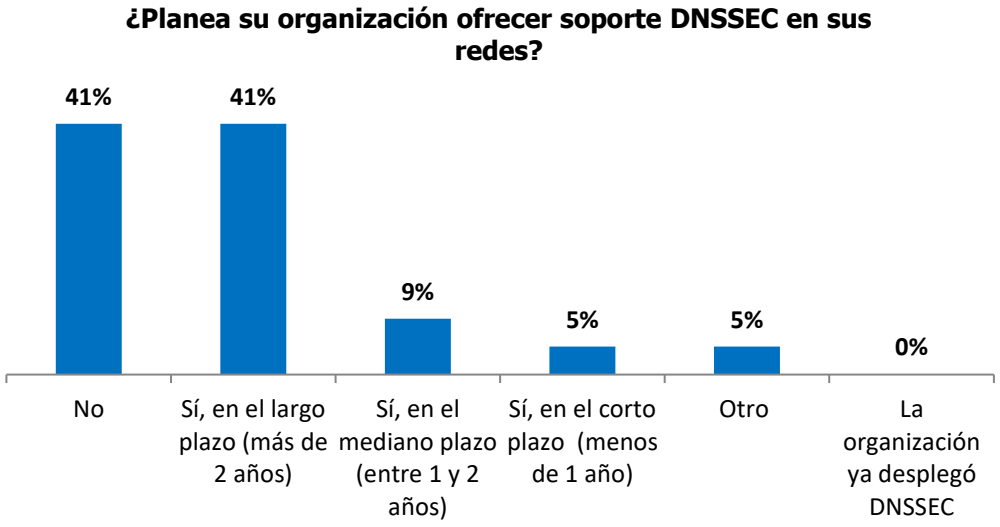
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

¿Los dispositivos CPE de su organización permiten gestión remota?

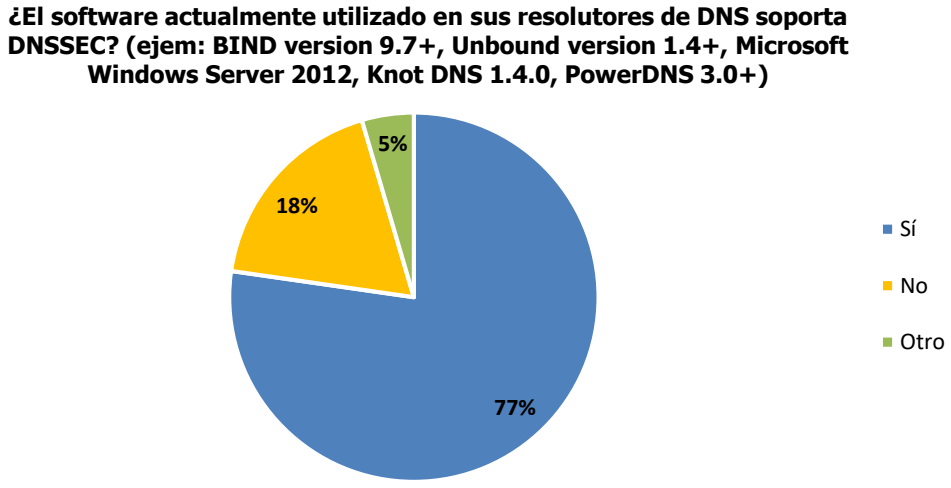


Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

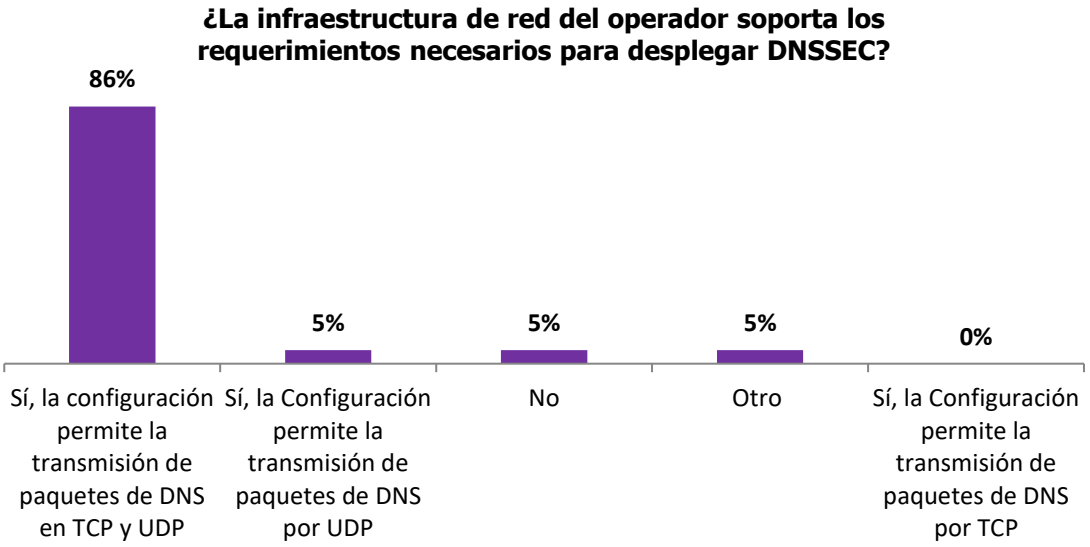
IV. Estado de despliegue de DNSSEC



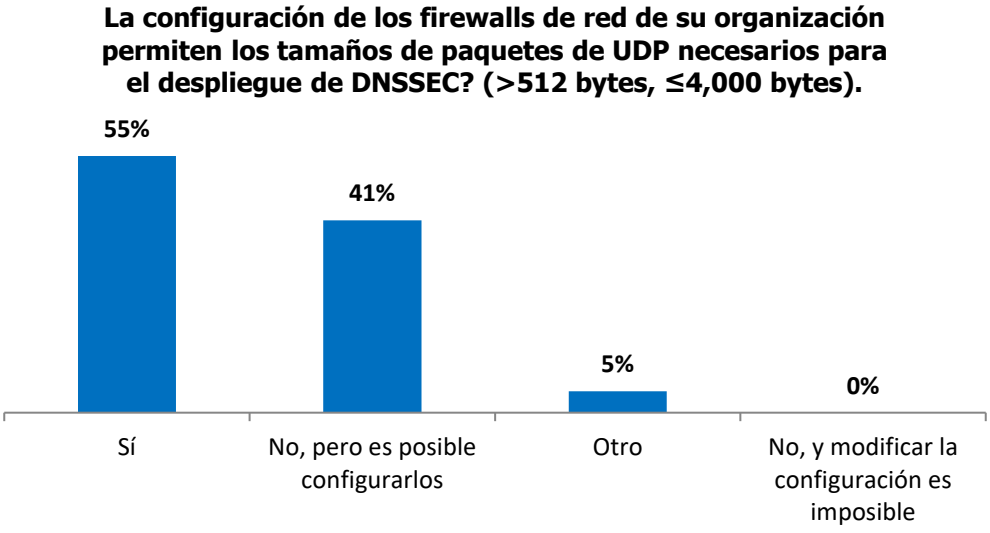
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

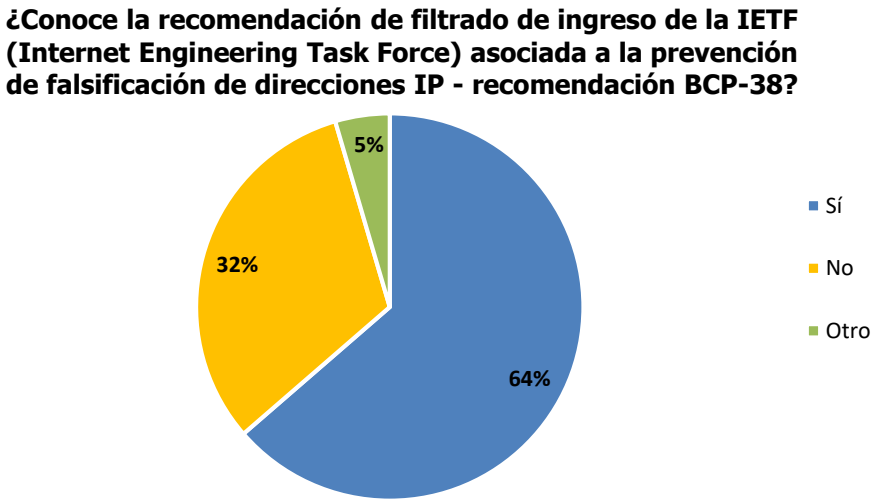


Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

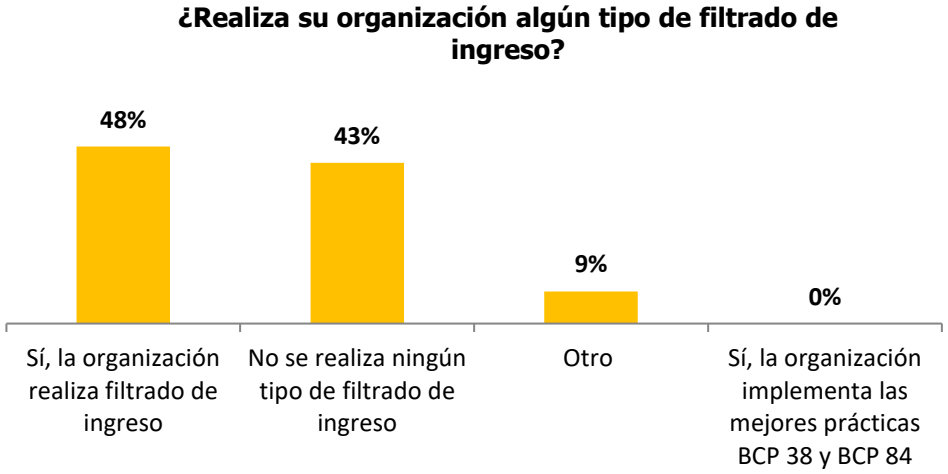


Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

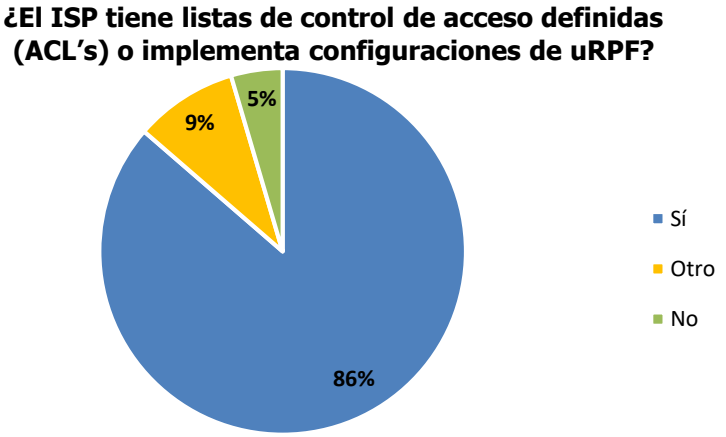
v. ¿Cómo se evita el forjado de direcciones IP en las redes?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

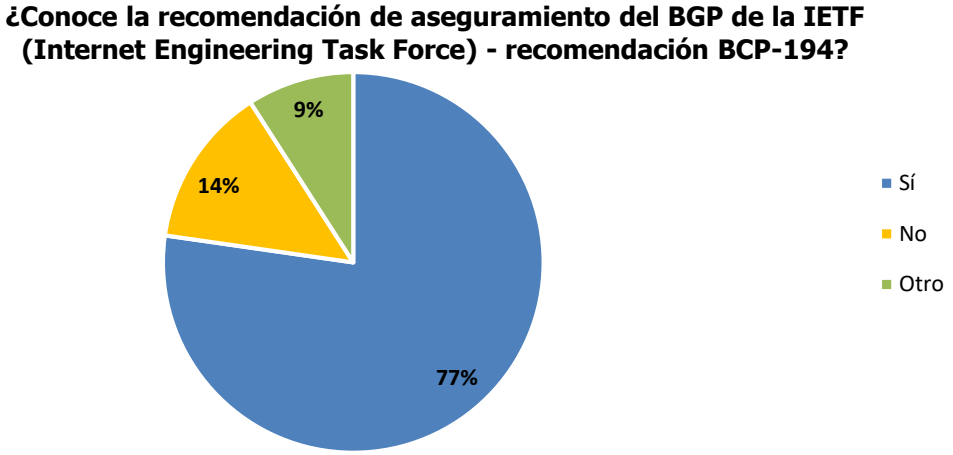


Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC



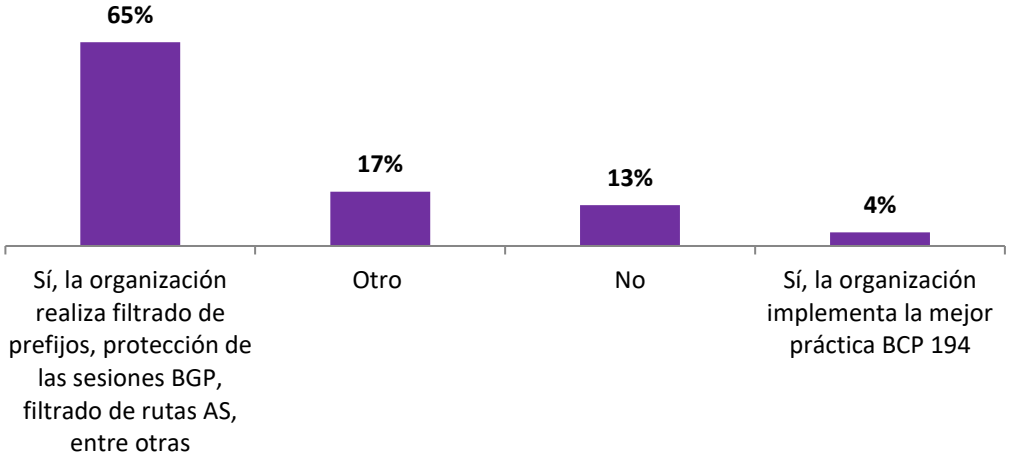
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

VI. ¿Cómo aseguran los ISP la integridad del protocolo de puerta de enlace de frontera?



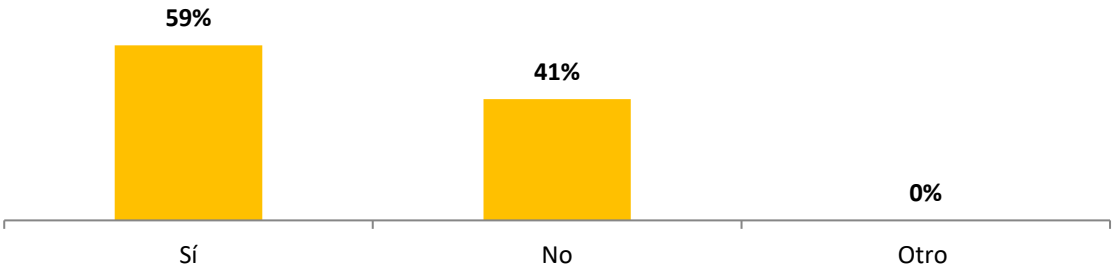
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

¿Las redes provistas por su organización implementan medidas de aseguramiento del BGP?



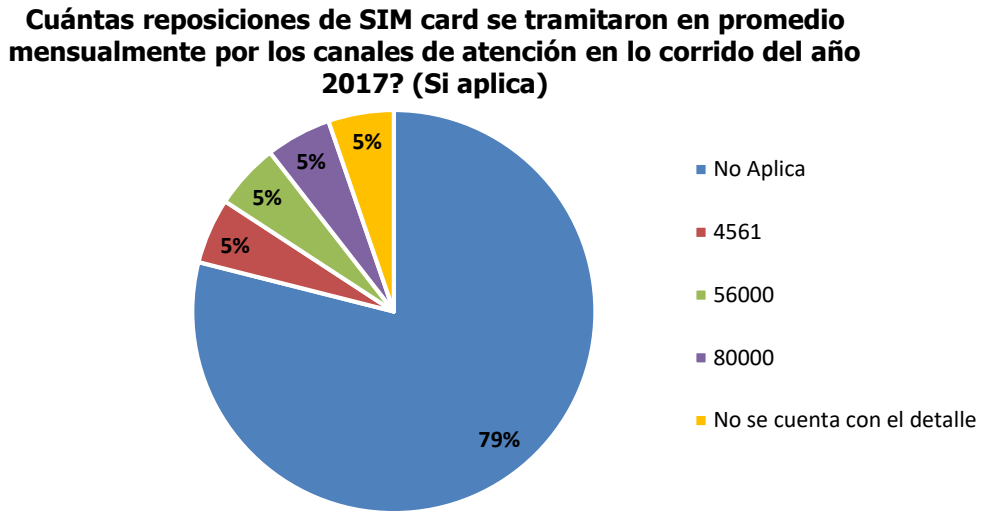
Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

Las redes provistas por su organización implementan medidas de filtrado de direcciones IP falsas o paquetes con direcciones IP de espacios de direcciones IP reservadas, pero aún no asignadas o delegadas por (IANA)?



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC

VII. Incidencia del fenómeno de suplantación de tarjetas SIM card en Colombia



Fuente: Encuesta "Diagnóstico Seguridad Digital CRC". Elaboración: CRC