RECOMENDACIONES MÍNIMAS DE SEGURIDAD AL CONTRATAR SERVICIOS DE INTERNET HOGAR

Nicolás Almanzar Espitia, Juan David Vanzina Solis, Alfonso Luque Romero

Resumen – Este artículo define las recomendaciones mínimas de seguridad que debería tener un usuario de internet hogar al contratar el servicio con algún proveedor. Esto con el fin de proteger la confidencialidad, disponibilidad e integridad de la información que circula en la red hogar contratada.

En el informe se realizan pruebas a tres proveedores del servicio de internet hogar en la ciudad de Bogotá, que permiten hacer un balance sobre las configuraciones realizadas por los proveedores y de esta forma se plantean recomendaciones para los usuarios de estas redes.

Índice de Términos - Ciberdelincuentes Confidencialidad, Disponibilidad, Integridad, Internet, proveedor, Recomendaciones, Seguridad informática, WiFi.

I. INTRODUCCIÓN

El uso de la red de internet ha presentado un crecimiento significativo en los últimos años y se ha incrementado el acceso desde diferentes dispositivos tecnológicos. En la actualidad estas redes pueden presentan vulnerabilidades en donde personas inescrupulosas aprovecharían para violar la confidencialidad, integridad y disponibilidad de los datos de los usuarios. Debido a esto, es de vital importancia tener redes de acceso a internet bajo esquemas que generen seguridad, sin embargo, para muchos usuarios y proveedores de internet esto no representa una prioridad en el momento de contratar o incluso configurar las redes alámbricas o inalámbricas de un hogar especialmente. Por lo que nos preguntamos ¿Qué consideraciones de seguridad debe tener un usuario que desea contratar un proveedor del servicio de internet para el hogar con el fin de obtener una adecuada protección de la información?
Esta investigación consiste en evaluar la seguridad de las redes de internet hogar de los tres proveedores con mayor cobertura de usuarios en la ciudad de Bogotá (Claro, Tigo/Une y Movistar), se realizará un análisis de los equipos que instalan en las viviendas y se verificara la configuración de las redes contratadas por los usuarios, con el fin de identificar vulnerabilidades o malas prácticas empleadas que pongan en riesgo la seguridad de la información.

Este estudio permitirá definir recomendaciones de seguridad de las redes hogar e identificar qué proveedor de internet proporciona mayor protección a la información.

II. PLANTEAMIENTO DEL PROBLEMA

A. Antecedentes del problema

La ampliación de cobertura de redes de internet, el incremento en número de usuarios y servicios de internet, la extensa oferta de servicios de internet para hogares y el crecimiento de tecnologías IoT ha aumentado el número de ciberataques al hogar. De acuerdo con la revista colombiana ENFOQUE los hogares también son vulnerables para la actuación de los ciberdelincuentes. La gran cantidad de dispositivos que hay en las casas, como: computadores, teléfonos móviles, televisores y otros electrodomésticos inteligentes, hacen de este espacio un blanco estratégico para los atacantes. (1)

Alejandro Agudelo, gerente del Centro de Seguridad y Vigilancia Digital (CSVD) de A3SEC, afirma que en los hogares se deben extremar los cuidados para tener seguridad y confiabilidad en la red, sobre todo cuando hay una época de alta transaccionalidad. Por ejemplo, el aprovechamiento de las múltiples ofertas en plataformas comerciales virtuales aumenta los riesgos de amenazas a los hogares a través de malware, virus que tienen como objetivo explotar vulnerabilidades en los equipos, tomando la información y usándola para cometer fraudes. (1)

La automatización del hogar a través de la tecnología Internet de las cosas (IoT) es una tendencia en crecimiento que está tocando las puertas de los hogares colombianos, ofreciendo eficiencia, comodidad y seguridad a solo un clic. Según estudios, para 2020 habrá entre 30.000 y 50.000 millones de aparatos conectados a Internet. (2)

La principal razón para automatizar un hogar es la seguridad, evitando que los dueños de lo ajeno entren a hurtar. Pero, como todo sistema conectado a Internet, no está exento de cualquier hackeo que pueda poner en peligro su casa y su información. (2)

Entre los ataques más comunes se encuentra la infección con

programas maliciosos que dañan los dispositivos, dejándolos completamente inútiles. La seguridad de la casa queda inhabilitada y los malintencionados pueden entrar fácilmente. En la actualidad, existe un ataque masivo de Malware llamado Silex, que borra información almacenada, configura cualquier firewall y modifica la configuración de la red obteniendo control sobre los dispositivos IoT. (2)

Una encuesta de la Comisión de Regulación de Comunicaciones de Colombia sobre el uso de plataformas para la prestación de servicios de telefonía, mensajería y televisión en Colombia, realizaron la pregunta ¿Cuáles de los siguientes servicios tiene usted disponible de forma permanente en su hogar?, el 96% de las personas encuestada respondieron que tienen internet en el hogar mientras que el 4% no tiene, como se muestra en la Figura 1. (3)

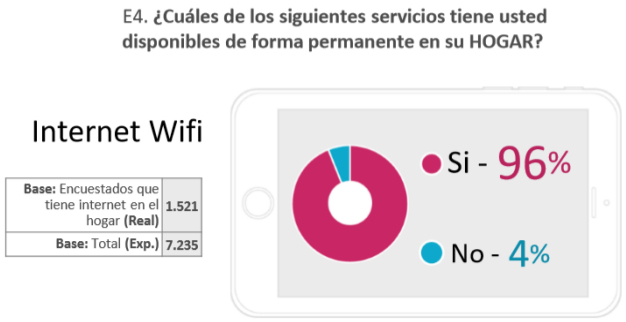

Fig. 1. Porcentaje de personas que tiene Wifi hogar. Fuente: Comisión de Regulación de Comunicaciones – CRC [Imagen], Estudio "El rol de los servicios OTT en el sector de comunicaciones" año 2018

A la pregunta ¿Cuál de los siguientes equipos/dispositivos tiene usted disponibilidad de forma permanente en su hogar?, en promedio el 1.8 de las personas encuestadas cuentan con TV en el hogar, el 1.4 tienen Smart TV mientras que el 1.5 tienen TV a color, como se muestra en la Figura 2.

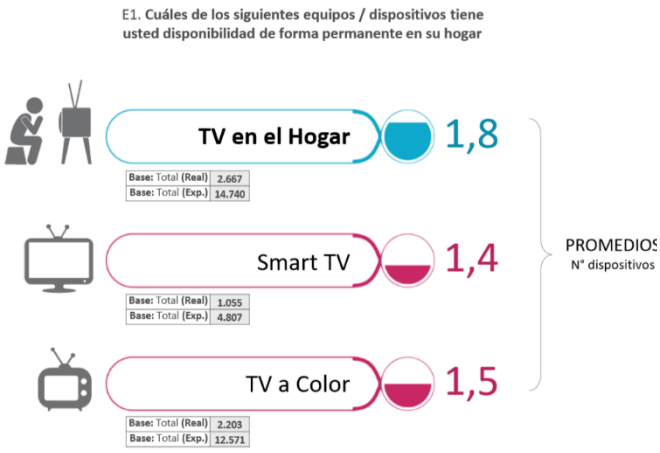

Fig. 2. Promedio de disponibilidad de dispositivos en el hogar. Fuente: Comisión de Regulación de Comunicaciones – CRC [Imagen], Estudio "El rol de los servicios OTT en el sector de comunicaciones" año 2018

De los resultados de las preguntas anteriores se deduce que la mayoría de hogares Colombianos tienen internet y además cuentan con dispositivos inteligentes que se conectan a esta red, es importante saber que los proveedores de servicios de internet garanticen la seguridad de la red del hogar con el fin de evitar posibles ataques cibernéticos, a través del establecimiento de claves, e instalación de dispositivos de última tecnología, sin embargo, la seguridad no está establecida al 100% en las redes del hogar debido a las malas prácticas de los usuarios así como el número de dispositivos con vulnerabilidades.

Según una tesis de la Universidad SAN BUENAVENTURA DE COLOMBIA (6) una red Wifi depende en gran parte de los usuarios finales que la usan; partiendo de la cultura de seguridad que tengan, así como de las buenas prácticas en la utilización de sus herramientas, software, dispositivos, y lo más relevante la información que manejan; esto es lo que permite que se fomente y se mantenga el nivel de seguridad adecuado. También aseguran que los entornos inalámbricos en general se hacen más seguros, en la medida que se implementen una serie de recomendaciones en seguridad para evitar o mitigar los riesgos que se puedan presentar.

De lo anterior se puede determinar la importancia que debe tener la red de internet hogar respecto a las dimensiones de integridad y confidencialidad, debido al alto riesgo que tiene los usuarios al realizar transacciones bancarias y el uso de información sensible cuando están conectados a la red de su casa.

B. Justificación

A partir de la estrategia del gobierno colombiano para convertir a Colombia en el primer país de la región en alcanzar cobertura 100% de internet de alta velocidad establecida en el plan vive digital Colombia 2014 – 2018, se ha ampliado la oferta de servicios de internet para el hogar y el número de usuarios conectados. Entre el año 2010 y el 2014 las estadísticas establecen que el 50% de los hogares se encontraban conectados a redes de fibra óptica, durante el año 2017 el acceso a internet en Colombia creció un 6.4% representado por un total de 30.3 millones de conexiones a internet en donde 16.32 millones de conexiones correspondían a conexiones a redes fijas y móviles. (4)

Según el informe del secretario de la OECD, Colombia se está preparando para la transformación digital a través del Pacto por la Transformación Digital de Colombia de 2018 y el plan El Futuro Digital es de Todos de 2019, los cuales estarían vinculados con el aumento de número de hogares y empresas colombianas con acceso de banda ancha. Sin embargo, es necesario resaltar que el país aún tiene desafíos estructurales importantes y deberá establecer estrategias que permitan una mayor penetración de banda ancha a nivel nacional. (5)

En función de lo anterior, según el diario LA REPÚBLICA, el presidente Iván Duque indicó que el objetivo a 2022 es que la cobertura de banda ancha en todo el territorio nacional sea del 70%. (6)

Por lo anterior los operadores de internet fijo han desarrollado planes para el hogar, económicamente más accesibles a la población colombiana, lo que ha permitido un índice de penetración más alto en el mercado por parte de los proveedores.

"El número de accesos a Internet fijo al finalizar el primer trimestre de 2018 llegó a 6.444.813 y un índice de penetración del 12,9%, presentando un aumento de 0,6 puntos porcentuales con relación al índice del primer trimestre de 2017". (7)

En referencia a ello se evidencia en la Figura 4 el crecimiento por operador "Al cierre del primer trimestre de 2018, los cinco Proveedores de Redes y Servicios de Telecomunicaciones (PRST) que presentaron el mayor número de accesos a Internet fijo fueron: Telmex Colombia S.A. (2.384.831 accesos); UNE EPM Telecomunicaciones S.A. E.S.P. (1.311.196 accesos); Colombia Telecomunicaciones S.A. E.S.P. (986.358 accesos); Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. (654.486 accesos), y Edatel S.A. E.S.P (198.338 accesos). Por su parte, los demás PRST alcanzaron los 909.604 accesos"

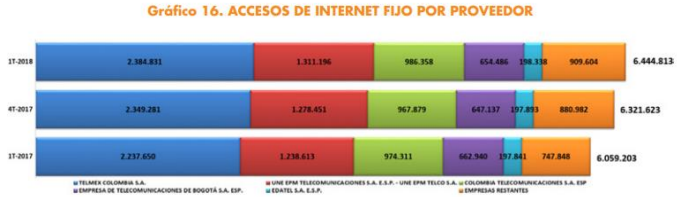

Fig. 3. Accesos de internet fijo por proveedor. Fuente: MinTic [Imagen], Accesos de internet fijo por proveedor [Consultado el 24 de octubre 2019]

La encuesta realizada por la Comisión de Regulación de Comunicaciones de Colombia sobre el uso de plataformas para la prestación de servicios de telefonía, mensajería y televisión en Colombia, realizaron la pregunta ¿Cuenta con el servicio de internet en su hogar?, en donde el 48% de los encuestados respondieron SI, mientras que el 52% NO tienen el servicio de internet hogar, como se muestra en la Figura 4. (3)

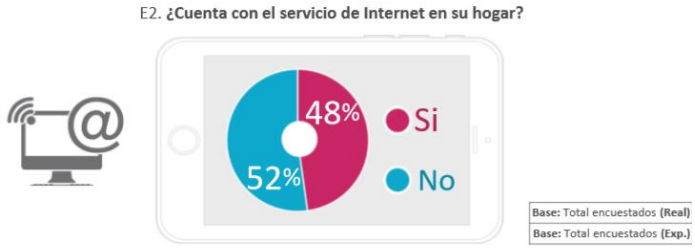

Fig. 4. Porcentaje de personas que tienen internet hogar. Fuente: Comisión de Regulación de Comunicaciones – CRC [Imagen], Estudio "El rol de los servicios OTT en el sector de comunicaciones" año 2018

A la pregunta ¿Con cuál operador? el 32% de los encuestados tienen operador Claro, el 25% tienen operador Tigo/Une, el 15% tienen operador Movistar, mientras que menos del 10 % tiene operador ETB, METROTEL O DIRECTTV, como se muestra en la Figura 5. (3)

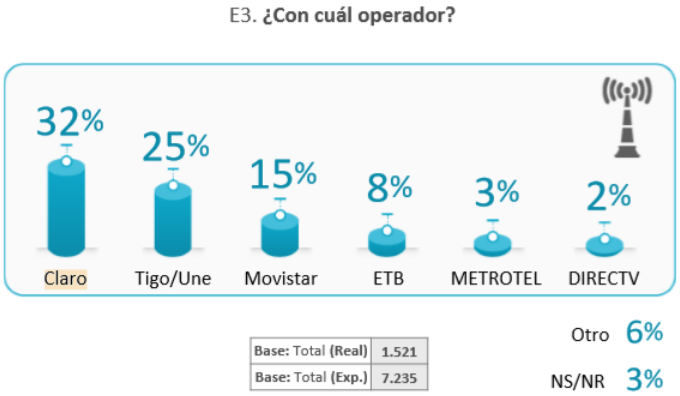

Fig. 5. Porcentaje de personas por uso de operador Fuente: Comisión de Regulación de Comunicaciones – CRC [Imagen], Estudio "El rol de los servicios OTT en el sector de comunicaciones" año 2018

Teniendo en cuenta lo anterior y el crecimiento en el número de hogares que tienen servicio de internet y del aumento de ciberataques, surge la necesidad de realizar un análisis del nivel de seguridad de las redes de internet hogar que ofrecen los 3 (Claro, Tigo/Une y Movistar) operadores con mayor cobertura.

III. METODOLOGÍA

La metodología propuesta contiene de 4 fases. La primera fase se desarrollarán actividades como la identificación de los dispositivos de red instalados por los tres principales proveedores (Claro, Tigo/Une y Movistar) de internet hogar de la ciudad de Bogotá. En la segunda fase se desarrollará un plan de pruebas, el cual permitirá identificar las prácticas de seguridad implementadas por los proveedores, posteriormente se ejecutarán las pruebas para el análisis de seguridad de la red, seguida por la tercera fase que se enfoca en realiza un análisis comparativo con el fin de evaluar los niveles de seguridad establecidos en la gestión de la red de los operadores y finalmente en la cuarta fase se documentará las recomendaciones de seguridad mínimas que los usuarios de internet hogar deben tener. Figura. 6 resume la metodología expuesta.

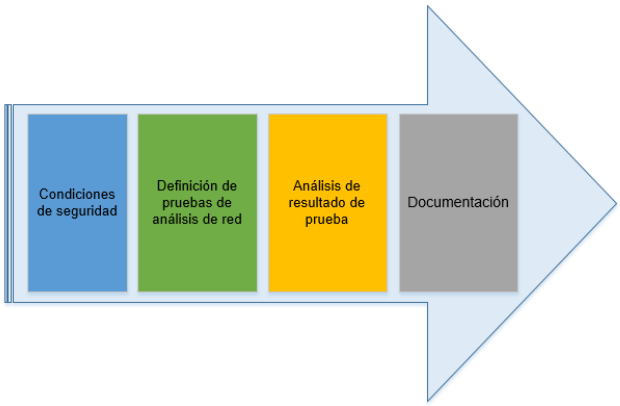

Fig. 6 Fases de trabajo de grado Estudio. Fuente: Autores

.

IV. IDENTIFICACIÓN DE LOS ROUTERS POR PROVEEDOR

Para realizar la identificación de los proveedores y las características de los routers que se van a analizar, se realiza un cuadro comparativo que permite observar las especificaciones de cada router por proveedor en cuanto a: megas de internet, marca del router, modelo del router, protocolo de cifrado, si la red wifi tiene clave, los puertos del router, si tiene protocolo WPS, los switch del router y los indicadores de LED, como se observa a continuación:

TABLA
FICHA TÉCNICA ROUTERS

Megas	Marca	Modelo	Protocolo de Cifrado	Clave	Puertos	WPS	Switch	Indicadores LED
10 MB	ARRIS	TG862A	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado)	Power, DS, US, Online, Ethernet, WiFi, Secure, Tel1 y Tel2
10 MB	UBEE	DVW32E	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado)	Power, DS,US, Ready, Tel1, Tel2, WLAN, WPS, LAN1, LAN2
40 MB	MITRA STAR	GPT274 1GNAC	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado), Botón WPS	Tel, Wifi 2.4Ghz, Wifi 5Ghz, Internet
50MB	Smart WIFI	RTF811 5VW	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado), Botón WPS	Tel, Wifi 2.4Ghz, Wifi 5Ghz, Internet
60 MB	ARRIS	TG2482	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado)	Power,DS,US, Online, 2.4GHZ, 5GHZ, Tel1, Tel2
10 MB	Technicolor	TC8305C	WPA2	SI	LAN, WAN	SI	Botón de encendido (encendido /apagado), Botón WPS	Power, Tel1, Tel2, WLAN, LAN1, WPS

V. EJECUCIÓN DE LAS PRUEBAS

A. Definición de las pruebas

Para realizar el análisis de seguridad de las redes Wifi hogar, se diseñaron un conjunto de pruebas que tienen como objetivo validar el nivel de seguridad del internet hogar de los proveedores seleccionados.

Las pruebas están identificadas por un código definido con la siguiente estructura:

PS#, donde la letra P significa prueba, la letra S significa seguridad y el símbolo # es el número de la prueba a realizar, además la prueba tiene el objetivo, la descripción de lo que se va a realizar en la prueba, y un campo de observación si se debe tener en cuenta algún característica especial o comentario al momento de realizar la prueba.

PS1: Realizar un escaneo de la red inalámbrica seleccionada, con el fin de verificar qué información sensible se puede obtener de la red.

PS2: Verificar que la contraseña de la consola del router no esté disponible en internet o sea una clave genérica.

PS3: Verificar que los dispositivos que están conectados a la red de internet hogar, sean conocidos por el titular de la red.

PS4: Verificar que la contraseña de la red de internet hogar haya sido cambiada por el usuario al momento de la instalación del servicio.

PS5: Identificar si el router cuenta con protocolo WPS para la conexión.

PS6: Identificar si el router dispone de opciones de prendido y apagado en ciertas horas del día o las opciones disponibles para evitar que todo el tiempo se encuentre disponible.

PS7: Comprobar el método de encriptación de la contraseña de Wifi.

PS8: Validar si el router dispone de creación de una red alterna para invitados.

PS9: Identificar si los protocolos de UPnP se encuentran habilitados para administración remota.

PS10: Visibilidad del SSID y filtrado de direcciones MAC.

B. Análisis de Resultados

El siguiente cuadro permite visualizar el resultado de las pruebas realizadas, indicando si cada red de internet hogar de los operadores Claro, Movistar y Tigo/UNE cumplió o no cumplió con la prueba, en donde SÍ significa cumple, NO incumple Y N/D no disponible.

TABLA 2
CUMPLIMIENTO DE LOS PROVEEDORES EN EL RESULTADO DE LAS PRUEBAS

Prueba	OPERADOR CLARO		Movistar		Tigo/UNE	
	ARRIS TG862A	UBEE DVW32E	ARRIS	MITRAS TAR	ARRIS TG2482	Technicolor TC8305C
PS1	SI	NO	SI	SI	NO	NO
PS2	NO	NO	SI	SI	NO	NO
PS3	SI	SI	SI	SI	SI	SI
PS4	SI	SI	NO	SI	SI	SI
PS5	SI	N/D	SI	SI	NO	NO
PS6	N/D	N/D	NO	SI	N/D	N/D
PS7	SI	SI	SI	SI	SI	SI
PS8	N/D	N/D	NO	SI	N/D	N/D
PS9	NO	N/D	SI	SI	NO	SI
PS10	SI	SI	SI	SI	NO	SI

Durante la ejecución de pruebas se evidenció que los proveedores configuran controles sobre los routers para ofrecer una mayor seguridad a los usuarios, sin embargo, ninguno cumple con todas las configuraciones esperadas y se evidencian mayores fortalezas en el operador movistar como se observa a continuación:

C. *Operador Claro*

A pesar de no tener disponibles algunas de las opciones de configuración en un 30%, el operador logró completar el 50% de configuraciones probadas de forma exitosa, tan solo el 20% no fue satisfactorio.

Una oportunidad de mejora sería iniciar la implementación de routers que ofrezcan mayores y mejores configuraciones, además de capacitar a los usuarios en el uso de los canales de administración de la red desde el día en que toman la decisión de tomar sus servicios.

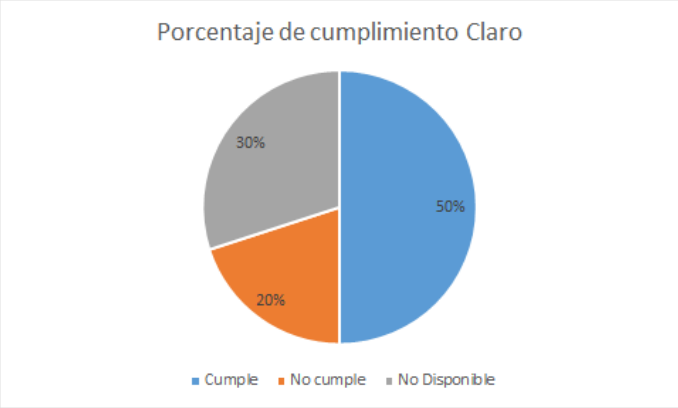

Fig. 7 Porcentaje de cumplimiento Claro. Fuente: Autores

D. *Operador Movistar*

Se identifica que el operador movistar ofrece todas las configuraciones ejecutadas durante las pruebas lo cual significa una fortaleza bastante notable, pues a pesar de no tenerlas habilitadas, si permite que los usuarios accedan al router y hagan sus configuraciones según la necesidad del cliente.

Además, dispone de un 75% de configuraciones probadas correctamente para brindar la mayor seguridad posible a los usuarios desde la instalación de los dispositivos de red. Tan solo el 25% de las pruebas no fueron exitosas.

Una oportunidad de mejora por parte del operador sería ofrecer capacitación a los usuarios sobre la configuración de su red, desde los diferentes canales y aplicaciones ya disponibles del operador.

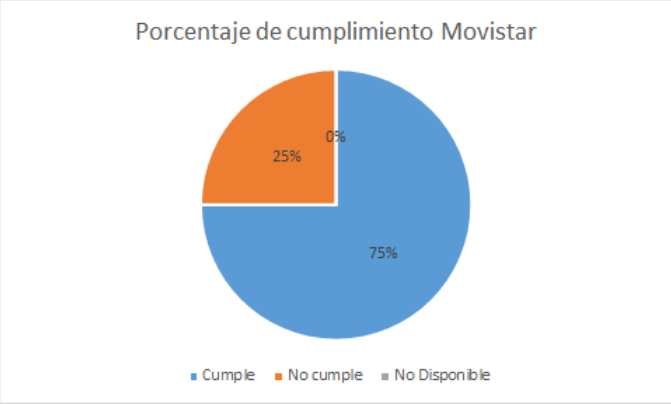

Fig. 7 Porcentaje de cumplimiento Movistar. Fuente: Autores

E. *Operador Tigo/Une*

El operador Tigo/Une tuvo el 40% de pruebas exitosas, el 40% de pruebas no exitosas y el 20% pruebas sin proceso de ejecución dado que no estaban disponibles en el router, lo que indica que existen fortalezas, pero se deben reforzar a partir de un número mayor controles para ofrecer a los usuarios una mayor seguridad de la información.

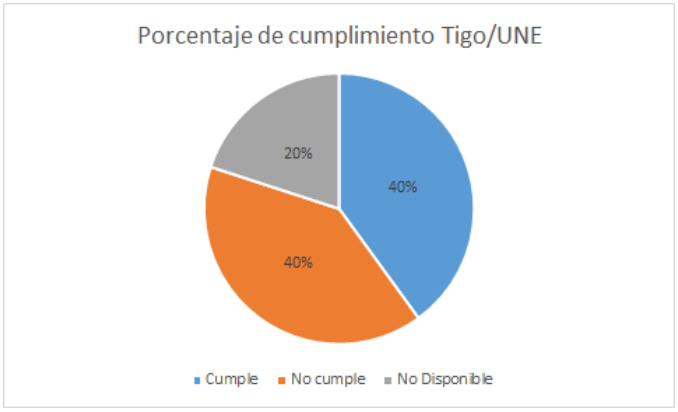

Fig. 8 Porcentaje de cumplimiento Tigo/UNE. Fuente: Autores

VI. RECOMENDACIONES

Dados los hallazgos evidenciados durante las pruebas, se procede a establecer las siguientes recomendaciones que permiten a los usuarios de internet hogar obtener una mayor seguridad de la información.

RC1: Al definir el nombre de la red Wifi hogar evitar establecer palabras o frases que puedan relacionarlo al usuario propietarios de la red o a las personas que la utilizan, esto con el fin de evitar ser identificado por delincuentes y de perder la confidencialidad de su información personal, también se puede ocultar el SSID (Nombre de la red), sin embargo, no suele ser muy práctico para algunas personas, se puede hacer uso de herramientas como Acrylic WiFi (4) Home que permiten realizar el escaneo de su red permitiendo verificar información como el SSID, el tipo de cifrado que tiene el router y si tiene activo el protocolo WPS.

RC2: Se recomienda realizar el cambio de clave de la red wifi de internet hogar por lo menos 1 o 2 veces al año, los proveedores de Claro, Tigo/Une y Movistar cuentan con las aplicaciones móviles Mi Claro, Mi Tigo Colombia y App Mi Movistar Colombia respectivamente, las cuales permiten modificar la contraseña de la red desde su celular sin necesidad de ingresar al Router ni tener conocimientos técnicos.

RC3: Establecer una contraseña segura es una de las formas más efectivas para proteger la información de su red, por esta razón se recomienda establecer una contraseña de más de 8 caracteres usando números, letras mayúsculas, letras minúsculas y caracteres especiales. Pero especialmente se recomienda que no se utilicen números o palabras relacionados con usted o las

personas que utilizan la red constantemente. Recuerde utilizar los métodos de cifrado WPA3 o WPA2 con el fin de evitar perder la confidencialidad de la clave de autenticación de su red.

RC4: Realizar un escaneo a los dispositivos conectados a su red por medio de una aplicación como Escáner WiFi u otras disponibles que puede ser instalada en su celular, esta verificación permite detectar si hay un dispositivo intruso en su red, el cual puede ser de un ciber atacante tratando de obtener información sensible como credenciales bancarias, perdiendo así el principio de confidencialidad de su información. También podría ser el dispositivo de un tercero que está consumiendo ancho de banda de su internet afectando de esta forma la disponibilidad de su red.

RC5: Los Router instalados por los proveedores de internet ofrecen en muchas ocasiones el protocolo de conexión WPS (wifi protected setup), con el que el Router se empareja con otros dispositivos mediante un pin y de esta forma tener acceso a su red de internet hogar. En la actualidad existen métodos que permiten obtener el PIN WPS viéndose afectado el principio de confidencialidad de información, por este motivo lo mejor es mantenerlo deshabilitado revisándolo periódicamente.

RC6: Otro de los mecanismos de protección de la información está en la habilitación de las redes de invitados, pues el tráfico de datos que circula en estas redes está separado del tráfico de nuestra red habitual, lo que brinda mayor seguridad contra Sniffers (Capturadores de tráfico de datos en la red) evitando así la pérdida de confidencialidad de su información personal.

RC7: Un mecanismo de protección adicional es realizar el cambio de contraseña de nuestro Router, pues una vez los delincuentes puedan ingresar a la red pueden acceder al Router y desde allí hacer configuraciones para mantener el acceso remoto o ejecutar configuraciones que alteren la integridad, confidencialidad y/o disponibilidad de su información.

RC8: Para el internet de las cosas (Internet of things) tener en cuenta que al activar el protocolo UPnP (Universal Plug and Play) se pierden atributos de seguridad en el firewall por lo que se recomienda establecer contraseñas de acceso de alta complejidad a todos los dispositivos de la red, así como monitorear constantemente las peticiones de estos o inactivar el protocolo según necesidad.

RC9: Una opción recomendada es establecer horas de encendido y apagado de la red WiFi y programarlas en la configuración del Router, sin embargo, no siempre es práctico, pero puede prevenir ataques a su red en horas muertas en las que los usuarios no notan caídas de servicio o bajas de velocidad.

RC10: Se recomienda consultar con su proveedor de servicio de internet si tiene herramientas que le permitan la administración de la red de forma simple, pues en ocasiones son de bastante utilidad, pero desafortunadamente los usuarios desconocen su existencia y su uso.

RC11: Si desea una mayor protección de su información también puede adquirir dispositivos complementarios como Bitdefender BOX o FingBox que permiten proteger toda la red hogar de amenazas de forma automática ejecutando controles en tiempo real.

VII. PRIORIZACIÓN DE RECOMENDACIONES

Haciendo uso de una matriz de prioridad, se realizará la matriz ponderada para las recomendaciones de seguridad propuestas para la red hogar, ordenándose en términos de riesgo e impactos, con el fin de realizar una clasificación priorizada. Las recomendaciones se agruparán según al riesgo existente al no ejecutarse las recomendaciones sugeridas.

A continuación, se muestra las escalas de probabilidad e impacto utilizadas para la valoración de riesgo:

TABLA 3
ESCALA DE PROBABILIDAD

Probabilidad	
1	Baja
2	Media
3	Alta

TABLA 4
ESCALA DE VALORACIÓN DEL IMPACTO

Escala de Valoración de Impacto			
Valor	Confidencialidad	Disponibilidad	Integridad
1	bajo	bajo	bajo
2	medio	medio	medio
3	alto	alto	alto

A continuación, se realiza un análisis de la exposición al riesgo de las redes basadas en routers en los que no sea posible ejecutarse las once recomendaciones bajo los criterios de confidencialidad, disponibilidad e integridad a los cuales se les asignará un peso del 1 al 3 de acuerdo con la importancia en la seguridad de una red hogar, en donde la confidencialidad tiene un peso de 3, la disponibilidad tiene un peso de 1 y la integridad tiene un peso de 2, siendo 3 el peso más alto, 2 el medio y 1 el bajo.

A cada recomendación se le asignó el valor correspondiente de la probabilidad y el impacto, el resultado del producto de la probabilidad por el impacto por el peso del criterio da como resultado el nivel de riesgo de la no implementación de la recomendación de acuerdo con el criterio de evaluación. Con el fin de obtener la sumatoria final de las calificaciones de cada subproceso se realiza la suma de la

calificación obtenida en cada uno de los criterios de evaluación de riesgo.

TABLA 5
NIVEL DE RIESGO SIN RECOMENDACIONES

Recomendaciones	Confidencialidad (Peso 3)	Disponibilidad (Peso 1)	Integridad (peso 2)	Sumatoria de Calificaciones
	Calificación	Calificación	Calificación	
RC1	18	1	6	26
RC2	18	2	6	26
RC3	27	4	4	35
RC4	9	3	4	16
RC5	9	2	2	13
RC6	18	2	12	32
RC7	27	6	12	45
RC8	9	2	6	17
RC9	6	3	2	11
RC10	18	1	2	21
RC11	3	1	2	6

Posteriormente, se obtiene la priorización de las recomendaciones para el internet hogar, en donde se evidencia que la recomendación RC7 se debe implementar con prioridad alta, las recomendaciones RC3, RC6, RC2 y RC1 tiene prioridad media mientras las recomendaciones RC10, RC8, RC4, RC5, RC9 y RC11 tienen prioridad baja.

TABLA 6
PRIORIZACIÓN DE LAS RECOMENDACIONES

Resultados de las recomendaciones Ordenadas		
Recomendaciones	Calificación de Riesgo	Prioridad
RC7	45	Alta
RC3	35	Media
RC6	32	Media
RC2	26	Media
RC1	25	Media
RC10	21	Baja
RC8	17	Baja
RC4	16	Baja
RC5	13	Baja
RC9	11	Baja
RC11	6	Baja

En la tabla anterior se evidencian los resultados de priorización de las recomendaciones agrupadas, de acuerdo con el nivel de prioridad. Por consiguiente, las recomendaciones con nivel de prioridad alto deben ser las primeras en implementarse, y en secuencia la prioridad medio y bajo.

VIII. CONCLUSIONES

Luego de culminar todo el proceso de pruebas para los proveedores, se concluye que:

- Se debe realizar una mejor apropiación de la seguridad de la información en los usuarios al momento de escoger el proveedor de servicio de internet para su hogar.

- Se realizaron recomendaciones a cada uno de los usuarios que permitieron ejecutar las pruebas de seguridad en su red de internet hogar, ayudándoles mejorar el nivel de seguridad de la información.

- El proveedor que presentó mayor deficiencia en el resultado de las pruebas de seguridad de la información de internet hogar fue Tigo/UNE, mientras que el proveedor Movistar fue el que presentó mayor fortaleza en el resultado de las pruebas en la seguridad en la red de internet hogar.

- Se definieron un conjunto de recomendaciones generales alineadas a la seguridad de la información en la red de internet hogar, presentadas en un infográfico, sirviendo como una herramienta para los usuarios al seleccionar el proveedor de servicio de internet.

- Se realizó el análisis de riesgo de las recomendaciones de seguridad de la información para el hogar de acuerdo con su probabilidad e impacto, bajo los criterios de disponibilidad, integridad y confidencialidad, obteniendo como resultado la priorización de las recomendaciones de acuerdo con su nivel de riesgo.

- Conforme a la priorización, la recomendación con nivel de prioridad más alta es la recomendación 7 (RC7), la cual indica que se debe realizar el cambio de contraseña del router, puesto que la clave siempre es genérica y el proveedor no la cambia al momento de la instalación, estas credenciales son fáciles de conseguir por internet y por ende la calificación del riesgo es mayor.

- Se identifican que las mejores herramientas y prácticas para la administración de la seguridad de la información de las redes hogar están implementadas en los routers del operador Movistar.

- Se evidencian falencias en la capacitación al usuario por parte de los proveedores al ofrecer la potestad de definir las reglas de seguridad en la red hogar.

REFERENCIAS

[1] Enfoque. ENFOQUE. [En línea] 17 de 01 de 2019. https://www.revistaenfoque.com.co/noticias/los-hogares-tambien-son-victimas-de-ciberataques.

[2] Sociedad. El nuevo siglo. [En línea] 24 de 08 de 2019. https://www.elnuevosiglo.com.co/articulos/08-2019-ciberataques-la-amenaza-de-los-hogares-inteligentes.

[3] Comisión de Regulación de Comunicaciones - CRC. Informe Final de Campo – Estudio “EL ROL DE LOS SERVICIOS OTT EN EL SECTOR DE COMUNICACIONES”. 2019.
[4] MinTIC. Plan Vive Digital Colombia. [En línea] 2018. https://www.mintic.gov.co/portal/604/articles-5193_recurso_2.pdf.
[5] Gurría, Angel. OECD. [En línea] 25 de 10 de 2019. https://www.oecd.org/about/secretary-general/launch-of-going-digital-in-colombia-review-bogota-october-2019.htm.
[6] González, José. La República. [En línea] 28 de 06 de 2019. https://www.larepublica.co/economia/cobertura-de-internet-banda-ancha-en-el-pais-sera-de-70-en-2022-presidente-duque-2879281.
[7] MinTIC. BOLETÍN TRIMESTRAL DE LAS TIC. 2018.
[8] 27000, ISO. ISO 27000. [En línea] http://www.iso27000.es/download/doc_iso27000_all.pdf.
[9] La gestión en la seguridad informática. [En línea] https://s3.amazonaws.com/academia.edu.documents/47441491/57-53-1-PB.pdf?response-content-disposition=inline%3B%20filename%3DLa_gestion_en_la_seguridad_de_la_informa.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191017%2Fus.
[10] LEY 19 DE 1958. [En línea] 18 de 11 de 1958. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=8271.
[11] Conpes 3701. [En línea] 14 de 07 de 2011. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.
[12] Conpes 3854. [En línea] 11 de 04 de 2016. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.
[13] LEY 1273 DE 2009 . [En línea] 5 de 01 de 2009. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.
[14] MinTIC. Ley 1341 de 2009. Ley 1341 de 2009. [En línea] https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf.
[15] LEY ESTATUTARIA 1581 DE 2012. [En línea] 18 de 10 de 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.
[16] MinTIC. Seguridad y privacidad de la información. [En línea] 15 de 12 de 2010. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.
[17] WeAreSocial. [En línea] 2019. https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.
[18] Mundial, Grupo Banco. Banco Mundial. [En línea] 2019. https://datos.bancomundial.org/indicator/IT.NET.BBND.P2?end=2018&start=1998&view=chart.
[19] Martínez, Jose Luis. [En línea] 15 de 08 de 2018. https://bogota.gov.co/mi-ciudad/gestion-publica/wifi-publico-en-bogota-para-conectarse-internet.
[20] Torres. Smartekh. [En línea] 28 de 04 de 2017. https://blog.smartekh.com/isp-seguridadweb.
[21] Medina, María Alejandra. Proveedores de internet, más transparentes. 17 de 12 de 2018, págs. https://www.elespectador.com/economia/proveedores-de-internet-mas-transparentes-articulo-829735.
[22] ESET. Riesgos asociados a las redes Wi-Fi públicas: cuáles son y cómo prevenirlos. [En línea] 5 de 02 de 2019. https://www.welivesecurity.com/la-es/2019/02/05/riesgos-asociados-redes-wi-fi-publicas/.
[23] Lab, VU. ProUP. [En línea] 19 de 04 de 2019. https://www.iproup.com/innovacion/4118-tecnologia-inventos-tecnologicos-seguridad-El-50-de-las-empresas-en-Latinoamerica-sufrio-un-ciberataque.
[24] Izquierdo, Luis Alberto Herrera. Las Redes WiFi en Sitios de Mayor Concurrencia de Usuarios. [En línea] 11 de 2015. https://repositorio.pucese.edu.ec/bitstream/123456789/553/1/HERRERA%20IZQUIERDO%20LUIS%20ALBERTO.pdf.
[25] DANIEL ERNESTO VERBEL SALGADO, HERMAN ALVAREZ CANO. ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS. [En línea] 2016. http://45.5.172.45/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf.
[26] Armenta, Mauricio Hernandez. Forbes Mexico. [En línea] 17 de 07 de 2019. https://www.forbes.com.mx/los-riesgos-de-conectarse-a-una-red-wifi-abierta-o-gratuita/.
[27] Publimetro. [En línea] 20 de 06 de 2018. https://www.publimetro.co/co/bogota/2018/06/20/zonas-que-tendran-internet-gratis-en-bogota.html.
[28] Heidy Monterrosa. La republica. [En línea] 17 de 03 de 2018. https://www.larepublica.co/internet-economy/las-zonas-de-wifi-gratis-para-la-gente-llegaron-a-1080-puntos-en-el-pais-2611906.
[29] universidadviu. Universidad Internacional de Valencia. [En línea] 21 de 03 de 2018. https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/.
[30] Excellence, ISOTools. [En línea] 1 de 02 de 2018. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.
[31] Ibersystems. [En línea] http://www.redeswifi.info/.
[32] Avast. [En línea] https://www.avast.com/es-es/c-hacker.
[33] Gorgona, Luis. [En línea] https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf.
[34] Vieites, Álvaro Gómez. Enciclopedia de la seguridad informática. s.l. : RA-MA, 2017.
[35] Ley 1341 de 2009. [En línea] 30 de 07 de 2009. https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009.
[36] Loon. [En línea] 2019. https://loon.com/.
[37] Google Station. [En línea] 2019. https://station.google.com.
[38] MinTIC. [En línea] 16 de 04 de 2016. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15066:Presidente-Santos-lanzo-proyecto-de-1-000-zonas-WiFi-gratis-en-Colombia.
[39] Zonas WiFi - MinTIC. [En línea] (https://colombiatic.mintic.gov.co/679/w3-propertyvalue-36408.html.
[40] Wifi para todos TM. [En línea] 12 de 03 de 2014. https://www.transmilenio.gov.co/publicaciones/147930/wifi_bogota_en_transmilenio/.
[41] Kasperky Latam. [En línea] 2019. https://latam.kaspersky.com/resource-center/preemptive-safety/public-wifi.
[42] WeLiveSecurity. [En línea] 5 de 2 de 2019. https://www.welivesecurity.com/la-es/2019/02/05/riesgos-asociados-redes-wi-fi-publicas/.
[43] Carlos Martínez, Leonardo Vidal. Seguridad en un Proveedor de Servicios de Internet (ISP). Seguridad en un Proveedor de Servicios de Internet (ISP). [En línea] https://iie.fing.edu.uy/eventos/telcom2006/conferencias/Seguridad_en_un_ISP.pdf.
[44] Comisión de regulación de Comunicaciones. CRC. [En línea] Revisión del marco regulatorio para la gestión de.
[45] questionpro. [En línea] 2020. https://www.questionpro.com/blog/es/muestreo-por-conveniencia/.
[46] acrylicwifi. [En línea] 2020. https://www.acrylicwifi.com/descargas-versiones-gratuitas-programas-software-herramientas-wifi/