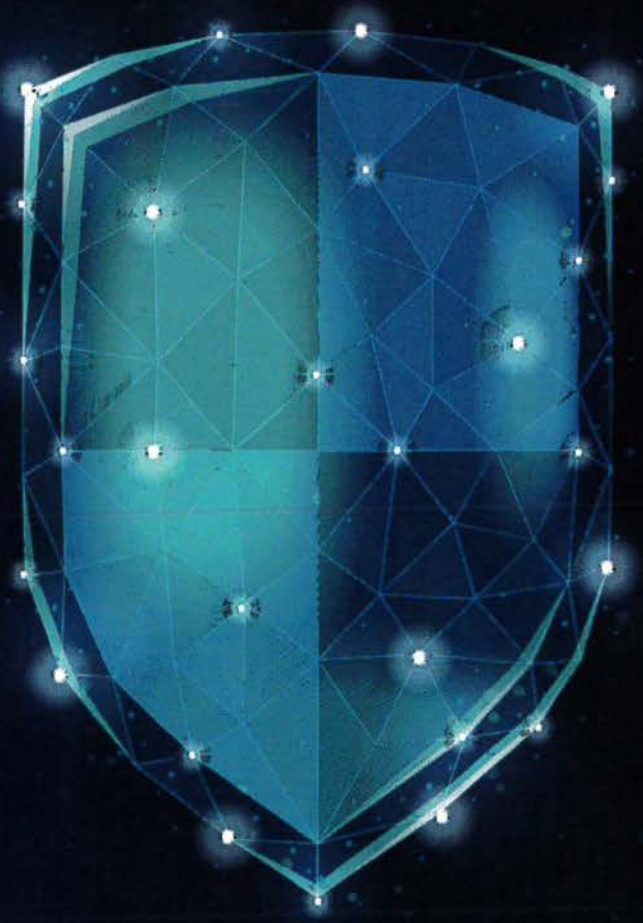
ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

INFORME ANUAL DE RESULTADOS

DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES QUE PERMITAN INHIBIR Y COMBATIR LA UTILIZACIÓN DE EQUIPOS DE TELECOMUNICACIONES PARA LA COMISIÓN DE DELITOS O ACTUALIZACIÓN DE RIESGOS O AMENAZAS A LA SEGURIDAD NACIONAL



JULIO 2022-JUNIO 2023

Antecedentes

En el marco de las obligaciones emanadas del Capítulo X de los *Lineamientos de colaboración en materia de seguridad y justica*, expedidas por el Pleno del Instituto Federal de Telecomunicaciones en el acuerdo publicado en el Diario Oficial de la Federación (DOF) el 2 de diciembre del 2015, se presenta el siguiente **Informe Anual de Resultados del Comité Especializado de Estudios e Investigaciones, para el período julio 2022 - junio 2023**.

Primero. De conformidad con lo establecido en los artículos 28, párrafo vigésimo, fracción IV de la Constitución Política de los Estados Unidos Mexicanos (la Constitución), así como en los diversos 1, 2, 3, 7, 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) y 1° del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, el Instituto Federal de Telecomunicaciones (IFT) en su carácter de órgano autónomo está facultado para promover el desarrollo eficiente y la prestación de los servicios públicos de radiodifusión y telecomunicaciones mediante la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico y de las redes públicas de telecomunicaciones y el acceso a la infraestructura activa, pasiva y otros insumos esenciales, a fin de garantizar lo establecido en los artículos 6° y 7° de la Constitución.

Asimismo, el IFT a través de su Órgano de Gobierno, resulta competente para emitir disposiciones administrativas de carácter general, planes técnicos fundamentales, lineamientos, modelos de costos, procedimientos de evaluación de la conformidad, procedimientos de homologación y certificación y ordenamientos técnicos en materia de telecomunicaciones y radiodifusión, así como disposiciones para el cumplimiento de su función regulatoria en los sectores de su competencia.

Segundo. El 2 de diciembre de 2015, se publicó en el DOF el "*Acuerdo mediante el cual el Pleno del IFT expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia*", que según lo dispuesto en su artículo Transitorio Primero, entraron en vigor el 1 de enero de 2016.

Tercero. El lineamiento Quincuagésimo de los *Lineamientos de Colaboración en Materia de Seguridad y Justica* dispone que los concesionarios, autorizados y las organizaciones a que se refiere el artículo 190, fracción XII de la LFTR realizarán bajo la coordinación del IFT, estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Para tales efectos, el IFT coordinará un Comité Especializado integrado por los referidos concesionarios, autorizados y organizaciones.

Cuarto. El auge de las telecomunicaciones ha potenciado la transformación de las tecnologías de la información y comunicación, siendo la telefonía móvil y el internet servicios que se constituyen como un elemento casi imprescindible para todas las actividades de la sociedad hoy en día. Sin embargo, el beneficio alcanzado por la sociedad de la información ha traído consigo algunos efectos colaterales negativos, ya que en los últimos años el uso para actividades ilegales de los equipos de comunicación, tanto móvil como fija, se ha convertido en un instrumento para realizar actos de delincuencia que afecta a la gran mayoría de los países y sus habitantes. Esto ha motivado que se emprendan acciones encaminadas a analizar y evaluar tales efectos, y de este modo posibilitar alternativas de solución.

Quinto. El lineamiento Quincuagésimo Cuarto del Capítulo X de los *Lineamientos de Colaboración en Materia de Seguridad y Justicia*, establece que el Comité Especializado de Estudios e Investigaciones contará con un Presidente, un Secretario Técnico y sus respectivos suplentes, cargos que serán ocupados por servidores públicos del IFT y serán designados por el Comisionado Presidente del mismo.

Sexto. El Acuerdo Único emitido el 13 de enero del 2016 mediante el cual, el Comisionado Presidente del IFT designa a los siguientes servidores públicos que son parte del mismo:

- Presidente del Comité: Titular del Centro de Estudios
  - Suplentes del Presidente del Comité: Titular de la Coordinación General de Vinculación Institucional, y el Titular de la Unidad de Política Regulatoria, en el orden indicado.

- Secretario Técnico del Comité: Director de Normatividad Técnica, adscrito a la Dirección General de Regulación Técnica de la Unidad de Política Regulatoria.
  - Suplentes del Secretario Técnico del Comité: Director de Análisis de la Capa Física en Telecomunicaciones y Radiodifusión, y el Subdirector de Criterios Normativos, ambos adscritos a la Dirección General de Regulación Técnica de la Unidad de Política Regulatoria, en el orden indicado.

Séptimo. Las funciones definidas para el Comité y su Presidente, incluyen las referentes a la coordinación de los trabajos y estudios del citado Comité, incluidas en las Disposiciones Generales de los Lineamientos de Colaboración, Capítulo X, en específico lo señalado en el lineamiento Quincuagésimo Quinto, inciso V), que establece como una de las funciones del Presidente del Comité, la coordinación de la elaboración del informe anual que contenga los resultados de los estudios e investigaciones, el cual será remitido al Congreso de la Unión y al Ejecutivo Federal.

A) Sesiones ordinarias.

Del mes de julio de 2022 a junio de 2023 se llevaron a cabo de manera remota y por medios electrónicos seis sesiones ordinarias del Comité. El detalle de los temas tratados, así como los acuerdos de cada sesión puede consultarse en las actas correspondientes en el Anexo I del presente documento.

En resumen, se tuvo quórum suficiente para declarar válidas las seis sesiones convocadas en el periodo señalado, y las fechas de dichas sesiones están indicadas en el Cuadro No.1.

Cuadro 1. Resumen de sesiones ordinarias del presente Informe

Reunión celebrada	Fecha de la reunión	Hora de inicio de la sesión de trabajo	Medio por el cual se llevó a cabo la reunión
Trigésima Sexta sesión ordinaria	18 de agosto de 2022	A partir de las 11:00 horas.	De manera remota por medios electrónicos
Trigésima Séptima sesión ordinaria	13 de octubre de 2022		
Trigésima Octava sesión ordinaria	15 de diciembre de 2022		
Trigésima Novena sesión ordinaria	16 de febrero de 2023		
Cuadragésima sesión ordinaria	13 de abril de 2023		
Cuadragésima Primera sesión ordinaria	15 de junio de 2023		

B) Estudios concluidos en el periodo

En el período reportado, los integrantes del Comité elaboraron y presentaron dos estudios, a saber:

1) **"ESTUDIO ESTADÍSTICO DEL NÚMERO DE TERMINALES MÓVILES, DE LLAMADAS DE MÓVILES Y DE CASETAS TELEFÓNICAS PÚBLICAS QUE OPERAN DENTRO DE UNA MUESTRA DE PENALES EN EL PAÍS SEXTA EDICIÓN".** El objeto de la investigación es actualizar las observaciones y análisis que se realiza año con año desde 2016 sobre el número de equipos terminales móviles que operan dentro de una muestra de recintos penitenciarios, y cuya actividad es monitoreada de manera simultánea por los concesionarios de redes móviles a lo largo de 3 semanas consecutivas. Dar continuidad a esta investigación permitió

a empresas y autoridades observar la dimensión del problema en materia de seguridad y su evolución. El estudio fue desarrollado por la Asociación Nacional de Telecomunicaciones (ANATEL), en representación de los Autorizados y Concesionarios que representa en el seno del Comité.

2) **"IDENTIFICACIÓN DE APLICACIONES Y RECURSOS TECNOLÓGICOS PARA MITIGAR LA COMISIÓN DE DELITOS"**. El objetivo del estudio es establecer recomendaciones para mitigación de amenazas mediante la identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos, que fue desarrollado por el grupo formado por AXTEL, S.A.B. de C.V; ALESTRA SERVICIOS MOVILES, S.A. de C.V; MEGACABLE COMUNICACIONES DE MÉXICO, S.A. de C.V; MARCATEL COM, S.A. de C.V; COORDINADORA DE CARRIER´S, S.A. de C.V; CABLEMÁS TELECOMUNICACIONES, S.A. de C.V; CABLEVISIÓN RED, S.A. de C.V; TV CABLE DE ORIENTE, S.A. de C.V; OPERBES, S.A. de C.V; MÉXICO RED DE TELECOMUNICACIONES, S.A. de C.V; CABLEVISIÓN, S.A. de C.V; TELEVISIÓN INTERNACIONAL, S.A. de C.V; CELMAX MOVIL S.A. de C.V. Y OPENIP COMUNICACIONES, S.A. de C.V.

El resultado de cada uno de los mencionados estudios, así como los comentarios y las conclusiones de los mismos son responsabilidad de los respectivos autores que los desarrollaron y presentaron durante el periodo, sin que necesariamente representen el punto de vista de los demás integrantes del Comité, ni del propio IFT. El texto íntegro de ambos estudios puede consultarse en el Anexo II del presente documento.

Con estos estudios los autores señalados dan cumplimiento al lineamiento Quincuagésimo de los *Lineamientos de Colaboración en Materia de Seguridad y Justica,* que dispone que los concesionarios, autorizados y las organizaciones a que se refiere el artículo 190, fracción XII de la LFTR realizarán bajo la coordinación del IFT, estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

ANEXO I

ACTAS DE LAS SESIONES

Periodo: julio 2022 a junio 2023

Fecha: 18 de agosto de 2022

ACTA RELATIVA A LA TRIGÉSIMA SEXTA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 07 minutos del día dieciocho de agosto del año dos mil veintidós, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Trigésima Sexta Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "***Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo***", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "***ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.***" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.

La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión.

En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quorum necesario para declarar válida la presente sesión.

La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

2. **Lectura del Orden del Día.**

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.
2. Lectura del Orden del Día.
3. Aprobación del Orden del Día.
4. Informe de los avances de los estudios en progreso.
    - Reporte del estudio: **"Identificación y comportamiento de llamadas desde líneas telefónicas denunciadas por ciudadanos"**. Responsable ANATEL
    - Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.
5. Integración del Informe Anual de Resultados del período julio 2021-junio 2022. Informe de comentarios recibidos.
6. Fecha de la próxima sesión.
7. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes de integrar o modificar cualquier otro punto a integrar a la Orden del Día.

El representante de Konecta México solicitó de manera respetuosa activar la cámara y silenciar los micrófonos hasta que sea necesaria la participación. Además, comentó sobre la situación actual que sufre Baja California y está relacionado con los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, por lo que solicitó un espacio para manifestar este caso en Asuntos Generales.

Los presentes no manifestaron ningún otro tema para incluir en al Orden del Día.

3. **Aprobación del Orden del Día.**

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día, posteriormente informó que no se recibieron objeciones al Orden del Día, por lo tanto, la Presidente del Comité señaló que el Orden del día se aprobó por unanimidad.

4. **Informe de los avances de los estudios en progreso:**

- Reporte del estudio: **"Identificación y comportamiento de llamadas desde líneas telefónicas denunciadas por ciudadanos"**. Responsable ANATEL

La Presidente del Comité dio seguimiento al Orden del Día consistente con el reporte del avance del estudio en proceso.

El representante de la ANATEL comentó que se han extendido las negociaciones con el Comité Ciudadano, y que decidieron aplazar los trabajos del informe en cuestión, sin embargo, señaló que a partir del lunes 22 de agosto presentará por escrito la propuesta de un nuevo estudio similar a los estudios que venían trabajando y actualizado en años anterior en este Comité.

Por lo cual, solicitó a la Presidente del Comité cambiar el estudio que habían propuesto **"Identificación y comportamiento de llamadas desde líneas telefónicas denunciadas por ciudadanos"** por el **"Estudio estadístico del número de terminales móviles de llamadas móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país"** aquel que venían trabajando anteriormente, año con año, debido a que rebaza la planeación que tenían prevista ya que le es útil a la autoridad correspondiente.

1. La Presidente del Comité preguntó a los miembros del Comité sobre este cambio solicitado. No hubo comentarios de los representantes por lo que se hizo válido este cambio de proyectos de estudio, considerando que: el cambio propuesto responde a un imprevisto, a una decisión ajena a los autores; se plantea una propuesta que ha generado información útil para dar seguimiento a un problema complejo que lastima a la sociedad y que se vincula con el mandato legal de este Comité.

Asimismo, se le solicitó a la ANATEL enviar por escrito el alcance, así como confirmar el título del estudio de investigación.

- Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

  La Presidente del Comité dio la palabra al representante de Axtel, Grupo Televisa (IZZI), Megacable Comunicaciones de México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones, para dar el reporte del avance del estudio en proceso.

  José Martín Figueroa consultor de Secnesys y representante de este grupo de trabajo recordó que se consideran dos alcances, en esta primera fase del periodo 2021-2022 estará enfocado en los sistemas operativos de equipos portátiles como laptops, y en el siguiente periodo estará enfocado en equipos móviles.

  Presentó el avance de dicho estudio, explicando que se encuentran en la cuarta sesión del avance de acuerdo con la metodología planteada. Comentó que se lleva un avance estimado del 81% del 93% planeado. Señaló que se encuentra en la Evaluación de las principales herramientas tecnológicas por lo que se llevaron a cabo las pruebas en los Sistemas Operativos Windows y están trabajando en las pruebas de Linux.

  Los miembros del Comité no manifestaron comentarios sobre el avance del estudio presentado.

  El secretario del Comité, el Ing. Ricardo Morán, propuso encontrar un mecanismo para evitar se interprete el resultado del estudio como un aval por parte del Comité a alguna tecnología en específico. El representante de Secnesys sugirió no incluir nombres de marcas. El Lic. José Luis Cruz sugirió mantener la información que sea necesaria para hacer de los estudios instrumentos útiles. A la luz de los resultados que se obtengan el Comité decidirá sobre esta opción.

  Dicha presentación formará parte de esta acta.

5. **Integración del Informe Anual de Resultados del período julio 2021-junio 2022. Informe de comentarios recibidos.**

   La Presidente cedió la palabra al Secretario Técnico del Comité para informar sobre el estado del Informe Anual de Resultados del Comité periodo julio 2021 a junio 2022.

Este Informe se inscribe en el marco de las obligaciones emanadas del Capítulo X de los Lineamientos de colaboración en materia de seguridad y justica.

El Secretario Técnico del Comité Informó que en atención al acuerdo QUINTO, de la Trigésima Quinta sesión ordinaria del Comité Especializado, llevada a cabo el pasado 16 de junio del presente, se envió a través del correo electrónico (srio-comiteespecializado@ift.org.mx) del Secretario Técnico, el borrador del Informe Anual de Resultados del Comité del periodo julio 2021 – junio 2022 para ponerlo a consideración de los miembros, para recibir, en su caso, sus comentarios u observaciones.

Para efecto de lo anterior, se estableció como fecha límite para la recepción de comentarios u observaciones el viernes 12 de agosto de 2022;

El Secretario Técnico del Comité adicionalmente indicó que no se recibieron comentarios u observaciones por parte de los representantes de concesionarios de telecomunicaciones y autorizados que impacten o modifiquen el borrador del Informe Anual de Resultados del Comité del periodo julio 2021 – junio 2022, salvo lo siguiente:

- Se recibió por parte de IZZI, un correo el 18 de julio con algunas preguntas relativas a el borrador de informe, se le dio respuesta ese correo contestándole sus dudas en invitándolo a hacer sugerencias al informe.

La Presidente comentó que los anexos del Informe contemplan: los estudios concluidos, así como copia de las actas, incluyendo las listas de asistencia.

Por lo que se señaló que no se recibieron otros comentarios u observaciones al borrador de dicho Informe.

La Presidente del Comité señaló que avanzarán con el siguiente paso, que es darle formato al Informe Anual y se procederá a circularlo a las autoridades correspondientes: Pleno del Instituto Federal de Telecomunicaciones, Secretaria de Gobernación, Cámara de Diputados y Senado de la Republica.

6. Fecha de la próxima sesión

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 13 de octubre de 2022, a las 11 horas.

7. **Asuntos Generales.**

El representante de Konecta México dio lectura a los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, y en relación con estos, comentó que se deben considerar al ciudadano y a la autoridad competente sobre los trabajos que se llevan en el Comité.

El representante de la ANATEL comentó de manera informativa que existen canales específicos para poder denunciar las actividades delictivas, así como también cuentan con el Consejo Ciudadano.

La Presidente del Comité, también expresó que sería importante fortalecer la cultura del uso de las herramientas tecnologías existentes, y la difusión de los informes emanados de este Comité.

Sin otros asuntos generales que atender.

ACUERDOS GENERALES

PRIMERO. Se aprobó al representante de la ANATEL sustituir el estudio propuesto denominado "**Identificación y comportamiento de llamadas desde líneas telefónicas denunciadas por ciudadanos**" por el "**Estudio estadístico del número de terminales móviles de llamadas móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país**" aquel que venían trabajando anteriormente, año con año, debido a que rebasa la planeación que tenían prevista y que además le es útil a la autoridad correspondiente. Por lo que la ANATEL enviará por escrito el alcance, así como el título del estudio de investigación.

SEGUNDO. Se da por presentado el avance del estudio que elabora el Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi), Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* denominado "**Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos**". Este se encuentra en la cuarta sesión del avance de acuerdo con la metodología planteada. Y se encuentra en la Evaluación de las principales herramientas tecnológicas por lo que se llevaron a cabo las pruebas en los Sistemas Operativos Windows y están trabajando en las pruebas de Linux. Se lleva un avance estimado del 81% del 93% planeado.

Dicha presentación se enviará a través del correo del Secretario Técnico y formará parte de esta acta.

TERCERO. El Secretario Técnico del Comité informó que no se recibieron comentarios u observaciones por parte de los representantes de concesionarios de telecomunicaciones y autorizados que impacten o modifiquen el borrador del Informe Anual de Resultados del Comité del periodo julio 2021 – junio 2022, por lo que, el Informe Anual de Resultados del Comité periodo julio 2021 a junio 2022 será circulado a las autoridades correspondientes (Pleno del Instituto Federal de Telecomunicaciones, Secretaria de Gobernación, Cámara de Diputados y Senado de la Republica).

CUARTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 13 de octubre de 2022, a las 11 horas.

8. **Cierre de la sesión.**

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 13:16 horas del día 18 de agosto de 2022 se dio por terminada la **Trigésima Sexta** Reunión Ordinaria del Comité Especializado.

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidenta del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

Mtra. Rebeca Escobar Briones
Presidenta del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ing. Ricardo Morán González
Secretario Técnico del Comité

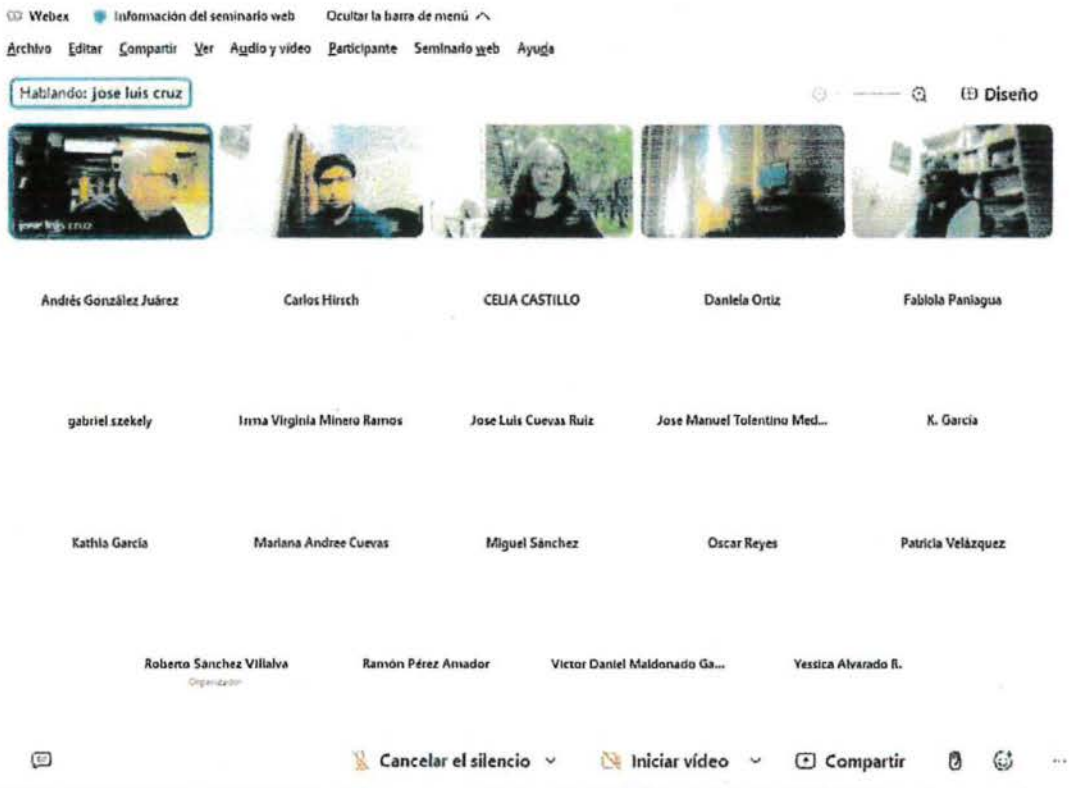
Fecha: 18 de agosto de 2022

La presente hoja forma parte del Acta de la Trigésima Sexta Reunión Ordinaria del Comité Especializado.

Nombre Completo	Correo Electrónico	Empresa
Gabriel Szekely	gszek@yahoo.com	ANATEL
Kathia García	kgarcia@anatel.org.mx	ANATEL
Jose Manuel Tolentino Medrano	jt789j@mx.att.com	AT&T
Carlos Hirsch	ch581s@att.com	AT&T
Oscar Reyes	oreyes@yobitelecom.com	CELMAX MOVIL
Daniela Ortiz	daniela.ortiz@inaece.com	CELMAX MÓVIL, BROMOVIL, MARKETING358, NEGOCIOS INTEGRALES DE MEXICO
Rafael	rafaelgm68@hotmail.com	GOGATEL
Yessica Alvarado R.	gogatel@gogatel.mx	GOGATEL, S.A. DE. C.V.
Victor Daniel Maldonado Garibay	victor.maldonado@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Rebeca Escobar Briones	rebeca.escobar@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Irma Virginia Minero Ramos	virginia.minero@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Jose Luis Cuevas Ruiz	jose.cuevas@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Ricardo Moran Gonzalez	ricardo.moran@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Sergio Vazquez Loyo	sergio.vazquez@ift.org.mx	INSTITUTO FEDERAL DE TELECOMUNICACIONES
Ramón Pérez Amador	rperezam@izzi.mx	IZZI
Jose Luis Cruz	mexmex2@konecta.mx	KONECTA DE MEXICO S DE RL DE CV
Susana Morales	smorales@vivaro.com	MARCATEL
Fabiola Paniagua	cfpaniagua@vivaro.com	MARCATEL/CCA
Jose Martin Figueroa	martin.figueroa@secnesys.com.mx	SECNESYS

Fecha: 18 de agosto de 2022

Patricia Velázquez	patricia.velazquez@secnesys.com	SECNESYS
Ever Molina	everardo.molina@secnesys.com	SECNESYS
Celia Castillo	ccastill@telmexomsasi.com	TELMEX
Miguel Sánchez	msbarqui@telmex.com	TELMEX
Mariana Andree Cuevas	mariana.andree@inaece.com	TELMOV, BENELEIT, COMERCIALIZADORA ROMEL, TENTIA, AFCAZA
Andrés González Juárez	andres.gonzalezj@totalsec.com.mx	TOTALPLAY



La presente hoja forma parte del Acta de la Trigésima Sexta Reunión Ordinaria del Comité Especializado.

Fecha: 13 de octubre de 2022

ACTA RELATIVA A LA TRIGÉSIMA SÉPTIMA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 10 minutos del día trece de octubre del año dos mil veintidós, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Trigésima Séptima Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "***Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo***", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "***ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.***" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. **Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.**

La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión.

En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quorum necesario para declarar válida la presente sesión.

La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

Fecha: 13 de octubre de 2022

2. Lectura del Orden del Día.

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.
2. Lectura del orden del día.
3. Aprobación del Orden del Día.
4. Informe de los avances de los estudios en progreso.
    - Reporte del estudio: "**Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país**". Responsable ANATEL
    - Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.
5. Información de la entrega del Informe Anual de Resultados del período julio 2021-junio 2022 a las autoridades correspondientes.
6. Fecha de la próxima sesión.
7. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes de integrar cualquier otro punto a el Orden del Día.

Los presentes no manifestaron ningún otro tema para incluir en el Orden del Día.

Fecha: 13 de octubre de 2022

3. **Aprobación del Orden del Día.**

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día, posteriormente informó que no se recibieron objeciones a la misma, por lo tanto, la Presidente del Comité señaló que el Orden del día se aprobó por unanimidad.

Informe de los avances de los estudios en progreso:
La Presidente del Comité dio seguimiento al Orden del Día consistente con el reporte del avance del estudio en proceso.

- Reporte del estudio: "**Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país**". Responsable ANATEL

El representante de la ANATEL informó que el estudio propuesto es similar a los estudios que venían trabajando y actualizado en años anterior en este Comité, el cual se está realizando la actualización 2022 asimismo comentó que se ha iniciado el estudio y los avances se presentarán en la sesión del mes de diciembre.

La ANATEL envió, al correo del Secretario Técnico del Comité, el alcance, objetivo, así como el título de la propuesta de estudio de investigación. Dicho estudio se titula *"Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición"*.
Por lo que se da por presentado el avance de la propuesta del estudio.

Klaus de Uranga representante de Clearcom Comunicaciones mencionó que la infraestructura dentro de los penales es precaria, por lo que cuestionó sobre las tecnologías utilizadas.

El representante de ANATEL comentó que la infraestructura la instala la autoridad correspondiente, sin embargo, señaló que esta es información sensible que solo la propia autoridad conoce y no comparte con los concesionarios y autorizados, por lo que señala que no es parte del alcance de la investigación del estudio propuesto.

Por otro lado, el representante de la ANATEL invitó a revisar la *"Disposición Técnica IFT-010-2016: especificaciones y requerimientos de los equipos de bloqueo de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen dentro de centros de readaptación social, establecimientos penitenciarios* o centros de internamiento para menores, federales o de las entidades federativas", en la cual se indica las especificaciones técnicas de los equipos inhibidores que deben instalarse en los centros penitenciarios.

Fecha: 13 de octubre de 2022

La Presidente del Comité invitó a los miembros a participar en un estudio relacionado con el tema de plataformas e inhibidores de señales en los centros penitenciarios y de readaptación social, en el marco del mandato que tiene este Comité. Un estudio de esta naturaleza podría complementar los estudios realizados y que realiza el Comité y podría generar una estrategia para el diálogo con las autoridades competentes.

La Presidente del Comité dio por presentado el avance de este estudio.

- Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsables: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

  La Presidente del Comité dio la palabra al representante de Axtel, Grupo Televisa (IZZI), Megacable Comunicaciones de México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones, para dar el reporte del avance del estudio en proceso.

  José Martín Figueroa consultor de Secnesys y representante de este grupo de trabajo informó que se consideran dos alcances, en esta primera fase del periodo 2021-2022 estará enfocado en los sistemas operativos de equipos portátiles como laptops, y en el siguiente periodo estará enfocado en equipos móviles (Android e iOS).

  Señaló que el objetivo de esta primera fase es de analizar la eficiencia del uso de herramientas tecnológicas que contribuyan a mitigar la comisión de fraudes y robo de identidad por medio de los equipos de usuarios final como por ejemplo laptops y/o desktops, así como de los operadores y concesionarios.

  Por lo que presentó el avance de dicho estudio, explicando que se encuentran en el último tramo del avance de acuerdo con la metodología planteada. Sin embargo, comentó que se tiene un desfase de la programación de un mes y medio.

  Señaló que se lleva un avance estimado del 91% planeado para presentar el reporte total para el mes de diciembre de este año. Señaló que los siguientes pasos serán I. Consolidación de información, II. Generación de reporte y III. Presentación de resultados ante el Comité.

  Los miembros del Comité no manifestaron comentarios sobre el avance del estudio presentado. La Presidente del Comité dio por presentado el avance de este estudio.

4. **Información de la entrega del Informe Anual de Resultados del período julio 2021-junio 2022 a las autoridades correspondientes.**

La Presidente en uso de la palabra informó lo siguiente:

Se comunica a los integrantes del Comité Especializado que el Informe anual de resultados del Comité Especializado julio 2021- junio 2022 ya fue enviado a las autoridades correspondientes. Específicamente, se remitió el Informe Anual de Resultados al Comisionado Presidente en Suplencia por Ausencia del IFT Javier Juárez Mojica; al Lic. Adán Augusto López Hernández, Secretario de Gobernación; Diputado Santiago Creel, Presidente de la Mesa Directiva de la Cámara de Diputados, y Lic. Alejandro Armenta Mier, Presidente de la Mesa Directiva del Senado de la República. Lo anterior en cumplimiento a lo previsto en el artículo 190, fracción XII, de la Ley Federal de Telecomunicaciones y Radiodifusión, y con lo señalado en la fracción V de las disposiciones Quincuagésima y Quincuagésima Cuarta de los Lineamientos de Colaboración en Materia de Justicia.

La Presidente comentó que los anexos del Informe contemplan: los estudios concluidos, así como copia de las actas, incluyendo las listas de asistencia.

No se recibieron comentarios u observaciones por parte de los integrantes del Comité.

5. **Fecha de la próxima sesión**

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de diciembre de 2022, a las 11 horas.

6. **Asuntos Generales.**

Sin asuntos generales por tratar.

Fecha: 13 de octubre de 2022

ACUERDOS GENERALES

PRIMERO. La ANATEL envió por escrito el alcance, objetivo, así como el título de la propuesta de estudio de investigación, por lo que se da por presentado el avance del "***Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición***". Se dio por presentado el avance de este estudio.

SEGUNDO. Se da por presentado el avance del 91% del estudio que elabora el Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi), Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* denominado "**Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos**". Este se encuentra en la fase final del avance de acuerdo con la metodología planteada. El reporte final de este estudio se tiene programado para el mes de diciembre de este año. La Presidente del Comité dio por presentado el avance de este estudio.

TERCERO. La Presidente informó a los integrantes del Comité Especializado que el **Informe anual de resultados del Comité Especializado julio 2021- junio 2022** fue enviado a las autoridades correspondientes. Específicamente, se remitió al Comisionado Presidente en Suplencia por Ausencia del IFT Javier Juárez Mojica; al Lic. Adán Augusto López Hernández, Secretario de Gobernación; Diputado Santiago Creel, Presidente de la Mesa Directiva de la Cámara de Diputados, y Lic. Alejandro Armenta Mier, Presidente de la Mesa Directiva del Senado de la República. Lo anterior en cumplimiento a lo previsto en el artículo 190, fracción XII, de la Ley Federal de Telecomunicaciones y Radiodifusión, y con lo señalado en la fracción V de las disposiciones Quincuagésima y Quincuagésima Cuarta de los Lineamientos de Colaboración en Materia de Justicia.

CUARTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de diciembre de 2022, a las 11 horas.

7. Cierre de la sesión.

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 12:28 horas del día 13 de octubre de 2022 se dio por terminada la **Trigésima Séptima** Reunión Ordinaria del Comité Especializado.

Fecha: 13 de octubre de 2022

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidenta del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

Mtra. Rebeca Escobar Briones
Presidenta del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ing. Ricardo Morán González
Secretario Técnico del Comité

Fecha: 13 de octubre de 2022

La presente hoja forma parte del Acta de la Trigésima Séptima Reunión Ordinaria del Comité Especializado.

NOMBRE	CONCESIONARIO O AUTORIZADO	CORREO ELECTRÓNICO
Alan Ochoa	MARCATEL (VIVARO)	alan.ochoa@secnesys.com
Andrés González Juárez	TOTALPLAY	andres.gonzalezj@totalsec.com.mx
Carlos Hirsch	AT&T	ch581s@att.com
Daniela Ortiz	WIMO TELECOM, GUGA TELECOM, CELMAX MÓVIL, MARKETING 358, PRO-COMUNICACIONES MÓVILES Y NEGOCIOS INTEGRALES DE MÉXICO	daniela.ortiz@inaece.com
Erika Antonia Lejsek	PEGASO SA DE CV (TELEFÓNICA)	erika.lejsek@telefonica.com
Esteban Morales	TELMEX	emgruner@telmex.com
Everardo Molina	SECNESYS / MARCATEL (VIVARO)	everardo.molina@secnesys.com
Fabiola Paniagua	COORDINADORA DE CARRIERS / MARCATEL COM (VIVARO)	cfpaniagua@vivaro.com
Fernando Butler Silva	IFT	fernando.butler@ift.org.mx
Francisco Clairin	CABLEVISIÓN	fclairin@izzi.mx
Gabriel Szekely	ANATEL	gszek@yahoo.com
Hugo Martínez	CANIETI	hugo.martinez@canieti.mx
Jaime Gudiño	GUGA TELECOM	jgudino@gugacom.com
José Luis Cuevas Ruiz	IFT	jose.cuevas@ift.org.mx
José Luis Ortega	SERVICIOS CASETEROS	joseluisortegapa@gmail.com
José Manuel Tolentino Medrano	AT&T	jt789j@mx.att.com
José Martín Figueroa	SECNESYS	martin.figueroa@secnesys.com.mx
Kathia García	ANATEL	kgarcia@anatel.org.mx
Klaus De Uranga	CLEARCOM	kul@clearcom.mx
Mariana Andree Cuevas	TELMOVIL, COMERCIALIZADORA ROMEL, AFCAZA, BENELEIT, EREGA Y TENTIA	mariana.andree@inaece.com
Miguel Sánchez	TELMEX	msbarqui@telmex.com
Oscar Cruz Zamora	IFT	oscar.cruz@ift.org.mx
Oscar Reyes	CELMAX MÓVIL	oreyes@yobitelecom.com
Patricia Velázquez	SECNESYS	patricia.velazquez@secnesys.com
Rafael Gómez	GOGATEL	rafaelgm68@hotmail.com
Ramón Pérez Amador	IZZI	rperezam@izzi.mx
Rebeca Escobar Briones	IFT	rebeca.escobar@ift.org.mx
Ricardo Moran González	IFT	ricardo.moran@ift.org.mx
Rodrigo Jiménez López	IFT	rodrigo.jimenez@ift.org.mx
Sergio Vázquez Loyo	IFT	sergio.vazquez@ift.org.mx
Yessica Alvarado	GOGATEL	yessica.alvarado@gogatel.mx

Fecha: 15 de diciembre de 2022

ACTA RELATIVA A LA TRIGÉSIMA OCTAVA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 8 minutos del día quince de diciembre del año dos mil veintidós, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Trigésima Octava Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "***Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo***", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "***ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.***" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. **Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.**

La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión. Asimismo, señaló que esta es la última sesión del año 2022.

En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quorum necesario para declarar válida la presente sesión.

La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

Fecha: 15 de diciembre de 2022

2. Lectura del Orden del Día.

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.
2. Lectura del orden del día.
3. Aprobación del Orden del Día.
4. Informe de los avances de los estudios en progreso.
    - Reporte del estudio: "Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país". Responsable ANATEL.
    - Reporte del estudio: "Estudio de Identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos". Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Movil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.
5. Presentación de la propuesta del calendario de sesiones para el año 2023.
6. Recordatorio de la elaboración de nuevas propuestas de estudio para el Período 2023.
7. Fecha de la próxima sesión.
8. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes de integrar cualquier otro punto o modificación al Orden del Día.

Susana Morales aclaró que Coordinadora de Carrier´s, S.A. de C.V. no es parte de Grupo Televisa, por lo que solicita modificar el punto 4 del Orden del día.

Los demás presentes no manifestaron ningún otro tema para incluir en el Orden del Día.

Fecha: 15 de diciembre de 2022

3. **Aprobación del Orden del Día.**

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día con la modificación solicitada, posteriormente informó que no se recibieron objeciones a la misma, por lo tanto, la Presidente del Comité señaló que el Orden del día con el cambio señalado, se aprobó por unanimidad.

4. **Informe de los avances de los estudios en progreso:**
La Presidente del Comité dio seguimiento al Orden del Día consistente con el reporte del avance del estudio en proceso.

- Reporte del estudio: "**Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta Edición**". Responsable ANATEL

El representante de la ANATEL mencionó que van a integrar los resultados de las casetas dentro de los penales y la integrarían al avance de los resultados de los equipos móviles, para enviarlo al finalizar la sesión para ser presentado integralmente en la siguiente sesión ordinaria, Enfatizó que este estudio estadístico es la Sexta Edición.

El representante de ANATEL comentó de manera general algunos datos estadísticos obtenidos del estudio para el caso de los dispositivos y tráfico de llamadas móviles.

La Presidente del Comité puso a consideración de los asistentes, preguntas o comentarios al avance del estudio. No hubo comentarios de los asistentes.
Comentó que este estudio tiene relación con el cumplimiento de la "Disposición Técnica IFT-010-2016: especificaciones y requerimientos de los equipos de bloqueo de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen dentro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas"; agregó la relevancia de destacarlos hallazgos reportados por el representante de Anatel

Por lo que la Presidente del Comité dio por presentado el avance de este estudio y agradeció al representante de Anatel el envío en las próximas semanas del avance del reporte escrito para el archivo del Comité.

Fecha: 15 de diciembre de 2022

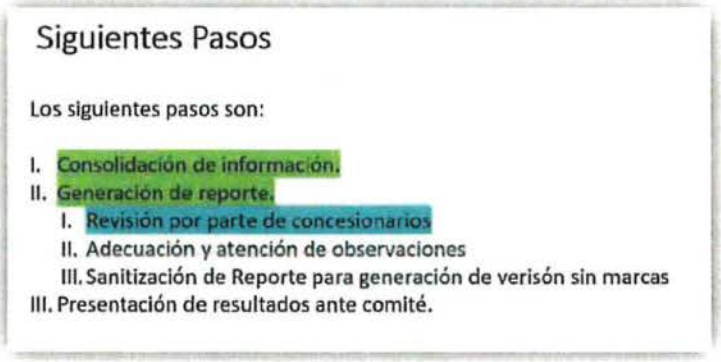
- Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsables: Axtel, S.A.B. de C.V., Grupo Televisa (Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

  La Presidente del Comité dio la palabra al representante de Axtel, Grupo Televisa (IZZI), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones de México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones, para dar el reporte del avance del estudio en proceso.

  Patricia Velázquez consultor de Secnesys y representante de este grupo de trabajo presentó el avance de su propuesta de estudio.

  Por lo que presentó información del avance de dicho estudio, explicando que se encuentran en el último tramo del avance de acuerdo con la metodología planteada.

  Señaló que se lleva un avance del 100% planeado por lo que se encuentra actualmente en revisión interna y el estudio integrado final se presentará para la siguiente sesión del Comité Especializado. Mostró como resumen lo siguiente:



Los miembros del Comité no manifestaron comentarios sobre el avance del estudio presentado. La Presidente del Comité dio por presentado el avance de este estudio.

Fecha: 15 de diciembre de 2022

5. Presentación de la propuesta del calendario de sesiones para el año 2023.

La Presidenta del Comité le dio el uso de la palabra al Secretario Técnico quien presentó la propuesta del calendario de sesiones para el año 2023.

El Secretario Tecnico del Comité señaló que, considerando la regla de operación del Comité Especializado de Estudios, en la que señala:

> *"El Comité Especializado se reunirá de manera ordinaria **el séptimo jueves de cada bimestre del año**, y en forma extraordinaria en cualquier momento previa convocatoria."*

Se presenta la siguiente propuesta de calendario de sesiones para el año 2023:

Reunión	Fecha propuesta	Inicio de sesión de trabajo
39°	16 de febrero de 2023	A partir de las 11:00 hrs
40°	13 de abril de 2023	
41°	15 de junio de 2023	
42°	17 de agosto de 2023	
43°	19 de octubre de 2023	
44°	14 de diciembre de 2023	

La Presidenta del Comité sometió a votación la aprobación de la propuesta del calendario de sesiones para el año 2023.

Sin comentarios para el calendario propuesto para las reuniones del Comité especializado para el 2023, se aprueba.

No se recibieron comentarios u observaciones por parte de los integrantes del Comité.

6. Recordatorio de la elaboración de nuevas propuestas de estudio para el Período 2023.

La Presidenta señaló que es conveniente recordar las obligaciones que establecen los Títulos de Concesión y el título 8° de la LFTyR, relativo a la colaboración con la justicia, que establece en el

artículo 190 fracción XII, que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

La Presidente reiteró la invitación a los miembros del Comité que aún no se han integrado a un grupo, así lo hagan, o planten temas en lo individual para la elaboración de nuevos estudios o bien, para que presenten nuevas propuestas de estudio para el siguiente período, con el objeto de dar cumplimiento a lo establecido en el Capítulo X, sección Quincuagésima de los Lineamientos de Colaboración en Materia de Seguridad y Justicia.

La Presidente indicó que, en la próxima sesión de febrero, presentará propuestas de temas de estudio.

Por otra parte, los miembros del Comité no manifestaron ningún otro comentario.

7. Fecha de la próxima sesión

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 16 de febrero de 2023, a las 11 horas.

8. Asuntos Generales.

El representante de Konecta de México señaló la relevancia de los avances presentados, que contribuyen a atender el problema de inseguridad nacional.

Sin asuntos generales por tratar.

ACUERDOS GENERALES

PRIMERO. La ANATEL enviará al correo del Secretario Técnico de manera integrada, los resultados de las casetas dentro de los penales así como los resultados de los equipos móviles del "***Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición***". La propuesta final de su Sexta edición de estudio se presentará en la siguiente sesión ordinaria del Comité. Se dio por presentado el avance de este estudio.

Fecha: 15 de diciembre de 2022

SEGUNDO. Se da cuenta de lo comentado por el Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi),* Coordinadora de Carrier´s, S.A. de C.V., *Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* denominado "**Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos**" quienes informaron que se tiene un avance del 100% planeado por lo que se encuentra actualmente en revisión interna y el estudio integrado final se presentará para la siguiente sesión del Comité Especializado. La Presidente del Comité dio por presentadla información de este estudio.

TERCERO. No se recibieron comentarios sobre la elaboración de nuevas propuestas de estudio para el Período 2023.

CUARTO. Se aprueba el calendario de sesiones del año 2023, quedando de la siguiente manera:

Reunión	Fecha propuesta	Inicio de sesión de trabajo
39°	16 de febrero de 2023	A partir de las 11:00 hrs
40°	13 de abril de 2023	
41°	15 de junio de 2023	
42°	17 de agosto de 2023	
43°	19 de octubre de 2023	
44°	14 de diciembre de 2023	

QUINTO. En la próxima sesión del Comité se presentarán propuestas de temas de estudio por parte de la Presidente.

SEXTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 16 de febrero de 2023, a las 11 horas.

Cierre de la sesión.

Fecha: 15 de diciembre de 2022

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 12:53 horas del día 15 de diciembre de 2022 se dio por terminada la **Trigésima Octava** Reunión Ordinaria del Comité Especializado.

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidenta del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

Mtra. Rebeca Escobar Briones
Presidenta del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ing. Ricardo Morán González
Secretario Técnico del Comité

Fecha: 15 de diciembre de 2022

La presente hoja forma parte del Acta de la Trigésima Octava Reunión Ordinaria del Comité Especializado.

NOMBRE	CORREO ELECTRÓNICO
Alfredo Emanuel Alarcon Deloya	alfredo.alarcon@directo.com
Andrés González Juárez	andres.gonzalezj@totalsec.com.mx
Carlos Hirsch	ch581s@att.com
Daniela Ortiz	daniela.ortiz@inaece.com
Dulce Maria Álvarez Núñez	dulce.alvarez@ift.org.mx
Erika Lejsek	erika.lejsek@telefonica.com
Esteban Morales	emgruner@telmex.com
Everardo Molina	everardo.molina@secnesys.com
Fernando Butler Silva	fernando.butler@ift.org.mx
Gabriel Székely	gszek@yahoo.com
Jorge Alberto Velázquez Olvera	jorge.velazquez@ift.org.mx
José Luis Cruz	mexmex2@konecta.mx
José Luis Cuevas Ruíz	jose.cuevas@ift.org.mx
Jose Martin Figueroa	martin.figueroa@secnesys.com.mx
Jose Tolentino	jt789j@mx.att.com
Kathia García	kgarcia@anatel.org.mx
Mariana Andree	mariana.andree@inaece.com
Miguel Sánchez	msbarqui@telmex.com
Oscar Cruz Zamora	oscar.cruz@ift.org.mx
Patricia Velázquez	patricia.velazquez@secnesys.com
Rafael Gómez	rafaelgm68@hotmail.com
Rebeca Escobar Briones	rebeca.escobar@ift.org.mx
Ricardo Morán González	ricardo.moran@ift.org.mx
Rodrigo Jiménez López	rodrigo.jimenez@ift.org.mx

Fecha: 15 de diciembre de 2022

Sergio Vázquez Loyo	sergio.vazquez@ift.org.mx
Susana Morales	smorales@vivaro.com
Victor Daniel Maldonado Garibay	victor.maldonado@ift.org.mx

La presente hoja forma parte del Acta de la Trigésima Octava Reunión Ordinaria del Comité Especializado.

Fecha: 16 de febrero de 2023

ACTA RELATIVA A LA TRIGÉSIMA NOVENA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 05 minutos del día dieciséis de febrero del año dos mil veintitrés, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Trigésima Novena Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "*Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo*", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "*ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.*" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. **Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.**

   La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión.

   En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quorum necesario para declarar válida la presente sesión.

   La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

Fecha: 16 de febrero de 2023

2. Lectura del Orden del Día.

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.
2. Lectura del orden del día.
3. Aprobación del Orden del Día.
4. Informe de actividades del Comité Especializado de Estudios e Investigaciones, correspondiente al año 2022.
5. Informe de los avances de los estudios en progreso:
   - Reporte del estudio: **"Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país"**. Responsable ANATEL.
   - Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Movil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.
6. Invitación a los miembros del Comité a presentar nuevas propuestas de estudios e investigaciones y presentación de temas de estudios que pudieran ser abordados por los miembros del Comité.
7. Fecha de la próxima sesión.
8. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes de integrar cualquier otro punto, comentario o modificación al Orden del Día.

Los asistentes no manifestaron ningún tema para incluir en el Orden del Día.

Fecha: 16 de febrero de 2023

3. **Aprobación del Orden del Día.**

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día, posteriormente informó que no se recibieron objeciones a la misma, por lo tanto, la Presidente del Comité señaló que el Orden del Día se dio por aprobado por unanimidad.

4. **Informe de actividades del Comité Especializado de Estudios e Investigaciones, correspondiente al año 2022.**

La Presidente del Comité Especializado mostró la presentación con el informe de actividades del Comité correspondiente al periodo del mes de enero a diciembre del año 2022.

Dicha presentación formará parte de la presente Acta del Comité.

5. **Informe de los avances de los estudios en progreso:**
La Presidente del Comité dio seguimiento al Orden del Día consistente con el reporte del avance del estudio en proceso.

- Reporte del estudio: "**Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta Edición**". Responsable ANATEL

  El representante de la ANATEL mencionó que continúan con la integración de los resultados de las casetas dentro de los penales y la integrarían al avance de los resultados de los equipos móviles, señaló que dicho avance integrado será enviado al correo electrónico del Secretario Técnico del Comité Especializado en un plazo de al menos dos semanas contadas a partir de esta sesión ordinaria.

La Presidente del Comité puso a consideración de los asistentes, preguntas o comentarios al avance del estudio. Los miembros del Comité no tuvieron comentarios o preguntas al reporte de avance del representante de ANATEL.

Por lo que la Presidente del Comité dio por presentado el avance de este estudio y agradeció a la representante de ANATEL el envío en las próximas semanas del avance del reporte el cual será reenviado a los representantes a este Comité para comentarios.

RM6.

Fecha: 16 de febrero de 2023

- Reporte del estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsables: Axtel, S.A.B. de C.V., Grupo Televisa (Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

La Presidente del Comité dio la palabra al representante del grupo para dar el reporte del avance del estudio en proceso.

José Eduardo Torres consultor de Secnesys y representante de este grupo de trabajo presentó el avance de su propuesta de estudio.

Después de la revisión interna señaló que dicho estudio se considera como el integrado final. Por lo que presentó información del avance del 100% con la metodología planteada.

Mostró los hitos del proyecto:

Los miembros del Comité no manifestaron comentarios sobre el avance del estudio presentado. La Presidente del Comité dio por presentado el avance de este estudio. Agregó que la versión integral del estudio fue recibida en días anteriores por la Secretaria del Comité; será enviado por correo a los representantes del Comité para comentarios y, en su caso, para someterlo a aprobación en la próxima sesión.

Fecha: 16 de febrero de 2023

6. **Invitación a los miembros del Comité a presentar nuevas propuestas de estudios e investigaciones y presentación de temas de estudios que pudieran ser abordados por los miembros del Comité.**

La Presidente señaló que es conveniente recordar las obligaciones que establecen los Títulos de Concesión y el título 8° de la LFTyR, relativo a la colaboración con la justicia, que establece en el artículo 190 fracción XII, que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

Señaló que en esta reunión se tiene como invitados a los investigadores del Centro de Estudios del IFT, el Dr. José Luis Cuevas y la Dra. Isabel Reza, quienes mostraron las siguientes propuestas de estudio:

- Mecanismos tecnológicos para coadyuvar en la reducción de estafas derivadas de portabilidad numérica (slamming).
- Mecanismos tecnológicos para coadyuvar en la reducción de estafas derivadas de intercambio de tarjeta SIM
- Descripción y uso de recursos tecnológicos utilizados por operadores a lo largo de la cadena de acceso a Internet para preservar la privacidad de los usuarios y la seguridad de la red.
- Analizar el panorama actual en México de los dispositivos móviles robados/falsificados, así como las tecnologías disponibles para combatir este delito.

Dichas propuestas de estudio serán compartidas con los miembros del Comité con el Acta de esta Sesión del Comité.

Por otra parte, el representante de Konecta de México, Lic. Jose Luis Cruz, detalló un par de comentarios, en lo que corresponde a los trabajos realizados en el senado sobre la ciberdelincuencia, acerca del convenio realizado en Budapest a principios de los años 2000, mencionó que el Senado hizo el análisis correspondiente y terminó aprobándola en su parte correspondiente y la envió al Ejecutivo, para que a su vez haga sus observaciones, y continue su curso. Finalmente, concluyó que es un tema interesante y complejo que se debe analizar en todos los puntos.

Por otra parte, los miembros del Comité no manifestaron ningún otro comentario.

Fecha: 16 de febrero de 2023

7. **Fecha de la próxima sesión**

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 13 de abril de 2023, a las 11 horas.

8. **Asuntos Generales.**

Sin asuntos generales por tratar.

ACUERDOS GENERALES

PRIMERO. Se dio por presentado el Informe de actividades del Comité Especializado de Estudios e Investigaciones, correspondiente al año 2022. Dicha presentación será compartida a los miembros del Comité a través del correo electrónico del Secretario Tecnico.

SEGUNDO. El representante de la ANATEL mencionó que continúan con la integración de los resultados de las casetas dentro de los penales y la integrarían al avance de los resultados de los equipos móviles, señaló que dicho avance integrado del "***Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición***" será enviado al correo electrónico del Secretario Técnico del Comité Especializado en un plazo de al menos dos semanas contadas a partir de esta sesión ordinaria y se enviará a los integrantes del Comité para comentarios.

TERCERO. El Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi),* Coordinadora de Carrier´s, S.A. de C.V., *Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* denominado "**Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos**" informaron que el estudio se considera como integrado final ya que se tiene un 100% de lo planeado. La Presidente del Comité dio por presentada la información de este estudio. El estudio integrado será compartido a los miembros del Comité a través del correo electrónico del Secretario Tecnico para recibir comentarios y en la siguiente sesión, en su caso, se dé por concluido y entregado.

RM6

Fecha: 16 de febrero de 2023

CUARTO. La Presidente del Comité Especializado presentó las nuevas propuestas de estudios a través de los investigadores del Centro de Estudios del IFT, el Dr. José Luis Cuevas y la Dra. Isabel Reza, quienes mostraron lo siguiente:

- Mecanismos tecnológicos para coadyuvar en la reducción de estafas derivadas de portabilidad numérica (slamming).
- Mecanismos tecnológicos para coadyuvar en la reducción de estafas derivadas de intercambio de tarjeta SIM.
- Descripción y uso de recursos tecnológicos utilizados por operadores a lo largo de la cadena de acceso a Internet para preservar la privacidad de los usuarios y la seguridad de la red.
- Analizar el panorama actual en México de los dispositivos móviles robados/falsificados, así como las tecnologías disponibles para combatir este delito.

Dichas propuestas de estudio serán compartidas con los miembros del Comité a través del correo del Secretario Técnico para su consideración.

No se recibieron comentarios sobre la elaboración de nuevas propuestas de estudio para el Período 2023.

QUINTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 13 de abril de 2023, a las 11 horas.

Cierre de la sesión.

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 13:15 horas del día 16 de febrero de 2023 se dio por terminada la **Trigésima Novena** Reunión Ordinaria del Comité Especializado.

RMG

Fecha: 16 de febrero de 2023

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidente del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

Mtra. Rebeca Escobar Briones
Presidente del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ricardo Morán González

Ing. Ricardo Morán González
Secretario Técnico del Comité

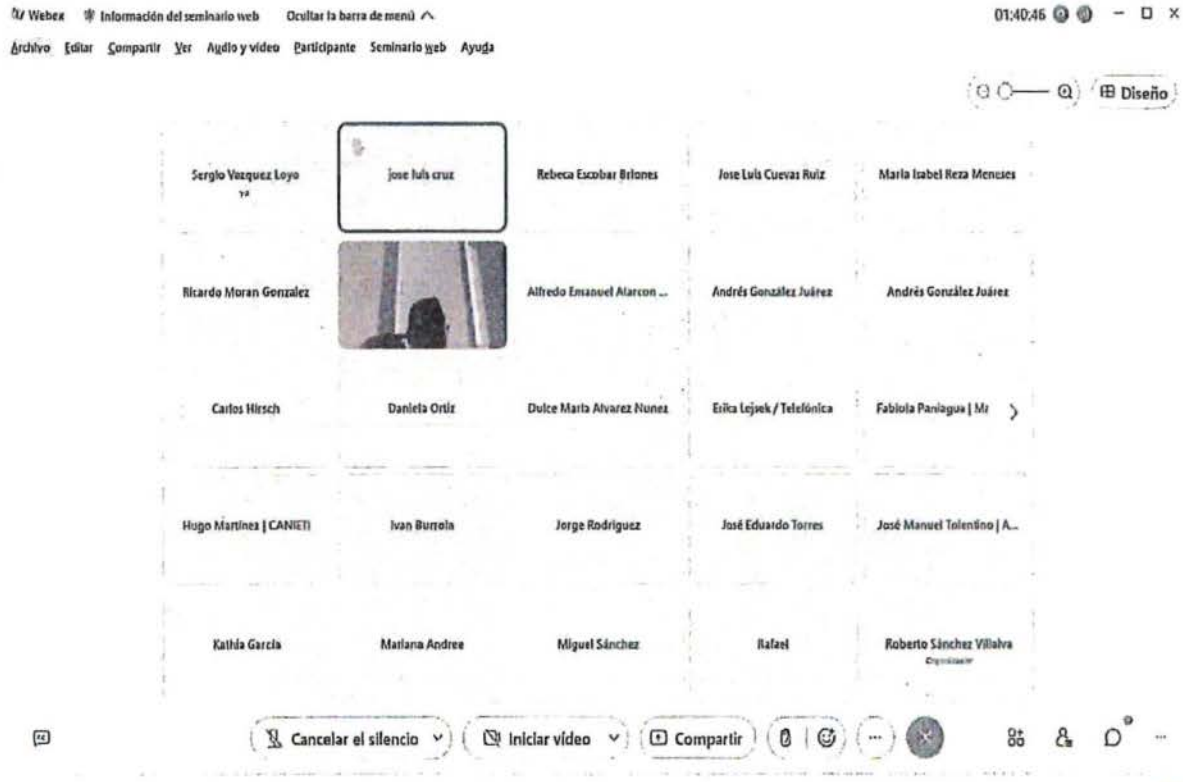
Fecha: 16 de febrero de 2023

La presente hoja forma parte del Acta de la Trigésima Novena Reunión Ordinaria del Comité Especializado.

Empresa	Nombre completo	Correo electrónico
ANATEL	Kathia García	kgarcia@anatel.org.mx
AT&T	Carlos Hirsch	ch581s@att.com
AT&T	José Manuel Tolentino Medrano	jt789j@mx.att.com
CANIETI	Hugo Martínez	hugo.martinez@canieti.mx
Celmax Movil, Brocomunicaciones Móviles, Marketing 358, Negocios Integrales de Mexico, Edilar, Wimotelecom, Guga telecom	Daniela Ortiz	daniela.ortiz@inaece.com
Comercializadora Frontera Mexicali S. de R.L. de C.V.	José Cruz Velázquez	mexmex2@konecta.mx
Directo Telecom	Alfredo Emanuel Alarcón Deloya	alfredo.alarcon@directo.com
Flo Networks	Iván Burrola	ibo@flo.net
Gogatel	Rafael Gómez Martínez	rafaelgm68@hotmail.com
IFT	Dulce María Álvarez Núñez	dulce.alvarez@ift.org.mx
IFT	José Luis Cuevas Ruíz	jose.cuevas@ift.org.mx
IFT	María Isabel Reza Meneses	maria.reza@ift.org.mx
IFT	Rebeca Escobar Briones	rebeca.escobar@ift.org.mx
IFT	Ricardo Morán Gonzalez	ricardo.moran@ift.org.mx
IFT	Rodrigo Jiménez López	rodrigo.jimenez@ift.org.mx
IFT	Sergio Vazquez Loyo	sergio.vazquez@ift.org.mx
Izzi	José Fernando Montes	jfmontes@izzi.mx
Marcatel Com	Claudia Fabiola Paniagua Esquivel	cfpaniagua@vivaro.com
Secnesys	Everardo Molina	everardo.molina@secnesys.com
Secnesys	Jorge Rodriguez	jorge.rodriguez@secnesys.com
Secnesys	José Eduardo Torres	jose.torres@secnesys.com
Telefónica	Erika Lejsek	erika.lejsek@telefonica.com
Telmex	Miguel Sánchez	msbarqui@telmex.com
Telmovil, Beneleit, Comercializadora Romel, Edilar, Tentia,Y Afcaza.	Mariana Andree Cuevas	mariana.andree@inaece.com
Totalplay	Andres Gonzalez	andres.gonzalezj@totalsec.com.mx
Vivaro | CCA	Susana Morales	smorales@vivaro.com

Fecha: 16 de febrero de 2023

La presente hoja forma parte del Acta de la Trigésima Novena Reunión Ordinaria del Comité Especializado.



RM6

INSTITUTO FEDERAL DE TELECOMUNICACIONES

INFORME ANUAL DE ACTIVIDADES DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES

Febrero 2023

RMG

Antecedente

- El lineamiento QUINCUAGÉSIMO de los **Lineamientos de Colaboración en Materia de Seguridad y Justicia** dispone que los Concesionarios, Autorizados y las Organizaciones a que se refiere el **artículo 190, fracción XII**, de la LFTyR realizarán, bajo la coordinación del IFT, estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.
- Para tales efectos, el Instituto coordinará un Comité Especializado integrado por los referidos Concesionarios, Autorizados y Organizaciones.

- Reglas de operación. Regla relativa a las Funciones del Comité Especializado.

  Inciso V.) Emitir un informe anual de actividades en el mes de enero de cada año

Cuadro No.1. Fechas de las Reuniones ordinarias efectuadas

Reunión		Fecha
1	33a.	17/02/2022
2	34a.	21/04/2022
3	35a.	16/06/2016
4	36a.	18/08/2022
5	37a.	13/10/2022
6	38a.	15/12/2022

Sesiones ordinarias.

De enero a diciembre de 2022 se llevaron a cabo seis Sesiones Ordinarias; las fechas de dichas Sesiones están indicadas en el Cuadro No.1.

RMG

Estudios realizados

En el período reportado, se terminaron dos estudios:

1. **Estudio estadístico del número de terminales móviles, de llamadas de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Quinta Edición**. Es una actualización del trabajo que se ha venido desarrollando, y que permite monitorear a través del tiempo la evolución de la problemática planteada. El estudio fue realizado por la Asociación Nacional de Telecomunicaciones (ANATEL), en representación de los Autorizados y Concesionarios que representa en el seno del Comité.

2. **Recomendaciones de medidas para la concientización de usuarios finales de servicios de telecomunicaciones en materia de seguridad de información,** desarrollado por el grupo formado por: AXTEL, S.A.B., DE C.V., MAXCOM TELECOMUNICACIONES, S.A.B. DE C.V., ALESTRA SERVICIOS MOVILES, S.A. DE C.V., MEGACABLE COMUNICACIONES DE MÉXICO, S.A. DE C.V., MARCATEL COM, S.A. DE C.V., COORDINADORA DE CARRIER´S, S.A. DE C.V., CABLE SISTEMA DE VICTORIA S.A. DE C.V., CABLEVISIÓN S.A. DE C.V., CABLEMÁS TELECOMUNICACIONES, S.A. DE C.V., TV CABLE DE ORIENTE S.A. DE C.V., CABLEVISIÓN RED S.A. DE C.V., DIRECTO TELECOM S.A. DE C.V., FTTH DE MÉXICO, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES S.A. DE C.V. TELEVISIÓN INTERNACIONAL, S.A. DE C.V., CELMAX MOVIL S.A. DE C.V.

RM6

Estudios en proceso

Actualmente se encuentran en desarrollo dos estudios titulados:

- **Estudio de Identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos.** Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V. Comunicaciones
- **Estudio estadístico del número de terminales móviles y de llamadas de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país.** Responsable: ANATEL.

Los estudios antes mencionados se han realizados a lo largo del año. Los resultados y conclusiones finales se incluirán en el informe de resultados del siguiente período.

Trabajos 2023

El Comité aprobó:

- Su calendario de trabajo para 2023

Reunión	Fecha propuesta	Inicio de sesión de trabajo
39°	16 de febrero de 2023	
40°	13 de abril de 2023	
41°	15 de junio de 2023	A partir de las 11:00 hrs
42°	17 de agosto de 2023	
43°	19 de octubre de 2023	
44°	14 de diciembre de 2023	

- Acordó la conclusión de los estudios en proceso, y su presentación en la sesión de febrero.
- Establecerá oportunamente nuevos temas de estudio.

RMG

Fecha: jueves, 13 de abril de 2023

ACTA RELATIVA A LA CUADRAGÉSIMA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 05 minutos del día trece de abril del año dos mil veintitrés, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Cuadragésima Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "***Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo***", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "***ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.***" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. **Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.**

   La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión.

   En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello informó que se contó con el quorum necesario para declarar válida la presente sesión.

   La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

Fecha: jueves, 13 de abril de 2023

2. Lectura del Orden del Día.

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de concesionarios de telecomunicaciones y autorizados.
2. Lectura del orden del día.
3. Aprobación del Orden del Día.
4. Informe de los comentarios recibidos de parte de los miembros del Comité Especializado de Estudios, en relación con los reportes de los siguientes estudios:
   - **"Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país".** Responsable ANATEL
   - **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsable: Axtel, S.A.B. de C.V., Grupo Televisa (Coordinadora de Carrier´s, S.A. de C.V., Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Megacable Comunicaciones México (MCM), Celmax Movil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.
5. Invitación a los miembros del Comité a presentar nuevas propuestas de estudios e investigaciones.
6. Fecha de la próxima sesión.
7. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes si deseaban integrar cualquier otro punto, comentario o modificación al Orden del Día.

Los asistentes no manifestaron ningún tema para incluir en el Orden del Día.

3. Aprobación del Orden del Día.

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día, posteriormente informó que no se recibieron objeciones a la misma, por lo tanto, la Presidente del Comité señaló que el Orden del Día se dio por aprobado por unanimidad en los términos en que fue presentado.

Fecha: jueves, 13 de abril de 2023

4. **Informe de los comentarios recibidos de parte de los miembros del Comité Especializado de Estudios, en relación con los reportes de los siguientes estudios:**

La Presidente del Comité dio seguimiento al Orden del Día consistente con el reporte de los comentarios recibidos.

- Reporte sobre el estudio: **"Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta Edición"**. Responsable ANATEL

  En atención al Acuerdo Segundo de la sesión 39 del Comité Especializado celebrada el día 16 de febrero del presente, por medio del correo electrónico del Secretario técnico del Comité, el día 23 de marzo se les envío a los miembros del Comité Especializado archivo electrónico que contenía el Estudio presentado por Anatel, en dicho correo se les solicito comentarios y que estos fueron entregados a más tardar el día 10 de abril del presente.

  El 30 de marzo se le hizo llegar a la representante de Anatel ante el comité observaciones de carácter general y los comentarios específicos al estudio, de parte de la Presidente del Comité.

  El representante de la ANATEL mencionó que continúan con la atención de los comentarios recibidos y, señaló que dicho estudio final será enviado al correo electrónico del Secretario Técnico del Comité Especializado en un plazo de al menos una semana contada a partir de esta sesión ordinaria.

  Por lo que la Presidente del Comité agradeció a la representante de ANATEL el envío en las próximas semanas del estudio integrado final con los comentarios atendidos, el cual será reenviado a los representantes a este Comité para su conocimiento.

- Reporte sobre el estudio: **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Responsables: Axtel, S.A.B. de C.V., Grupo Televisa (Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

  En atención al Acuerdo Tercero de la sesión 39 del Comité Especializado celebrada el día 16 de febrero del presente, por medio del correo electrónico del Secretario técnico del Comité, el día 16 de marzo se les envío a los miembros del Comité Especializado archivo electrónico que contenía el Estudio presentado por el grupo de operadores que conforman las empresas MCM, Axtel, Grupo Televisa, Marcatel, Celmax y Open Ip Comunicaciones, en dicho correo se les solicito comentarios y que estos fueron entregados a más tardar el día 31 de marzo del presente.

El 31 de marzo se le hizo llegar a la representante del grupo de operadores que conforman las empresas MCM, Axtel, Grupo Televisa, Marcatel, Celmax y Open IP Comunicaciones observaciones a dicho estudio, de parte de la Presidente del Comité.

Por otro lado, finalmente, el representante de Marcatel, Daniel Castañeda, solicitó presentar en esta misma reunión el estudio propuesto con los comentarios atendidos.

La Presidente del Comité dio la palabra al representante del grupo para dar detalle de los comentarios atendidos del estudio en proceso.

Por lo que Patricia Velazquez le solicitó a Eduardo Torres presentar a detalle dicha atención a los comentarios y mostrar la forma en la cual solventaron los comentarios. El representante de este grupo de trabajo presentó el detalle de los comentarios atendidos a su propuesta de estudio. Esta versión con la atención a los comentarios fue enviada a Daniel Castañeda, y será enviada al Secretario Técnico de este Comité.

Después de la revisión, la Presidente señaló al Secretario Técnico que dicho estudio sea enviado en carácter informativo a los miembros del Comité.

5. Invitación a los miembros del Comité a presentar nuevas propuestas de estudios e investigaciones.

La Presidenta reiteró la invitación para la presentación de nuevos estudios, recordando que es una obligación establecida en su Título de Concesión y en el Título 8° de la Ley Federal de Telecomunicaciones y Radiodifusión, relativo a la colaboración con la justicia, que establece en el artículo 190 fracción XII, que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

Recordó a los miembros del Comité que, en la reunión anterior los investigadores del Centro de Estudios del IFT, el Dr. José Luis Cuevas y la Dra. Isabel Reza mostraron algunas nuevas propuestas de estudio ante el Comité para ser consideradas.

Los representantes de ANATEL y de Marcatel comentaron que en la próxima reunión presentaran nuevas propuestas de estudio para el siguiente periodo.

Ningún concesionario o grupo de trabajo expuso algún otro tema.

La Presidenta reiteró la invitación a los miembros del Comité que aún no se han integrado a un grupo, así lo hagan, o planten temas en lo individual para la elaboración de nuevos estudios o bien,

RM6

para que presenten nuevas propuestas de estudio para el siguiente período, con el objeto de dar cumplimiento a lo establecido en la normativa antes señalada.

Por otra parte, los miembros del Comité no manifestaron ningún otro comentario.

6. **Fecha de la próxima sesión**

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de junio de 2023, a las 11 horas.

7. **Asuntos Generales.**

Sin asuntos generales por tratar.

ACUERDOS GENERALES

PRIMERO. El representante de la ANATEL mencionó que continúan con la atención de los comentarios recibidos sobre del "***Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición***". Señaló que dicho estudio final con los comentarios atendidos será enviado al correo electrónico del Secretario Técnico del Comité Especializado en un plazo de al menos una semana contada a partir de esta sesión ordinaria.

SEGUNDO. El Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi),* Coordinadora de Carrier´s, S.A. de C.V., *Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* presentó los comentarios atendidos sobre su propuesta "**Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos**". La Presidente del Comité dio por presentada la información de este estudio. Dicho estudio integrado con los comentarios atendidos será compartido a los miembros en carácter informativo.

TERCERO. La Presidente del Comité Especializado reiteró la invitación a los miembros del Comité para la presentación de nuevos estudios, recordando que es una obligación establecida en su Título de Concesión y en el Título 8° de la Ley Federal de Telecomunicaciones y Radiodifusión, relativo a la colaboración con la justicia

RM6

Fecha: jueves, 13 de abril de 2023

CUARTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de junio de 2023, a las 11 horas.

Cierre de la sesión.

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 12:32 horas del día 13 de abril de 2023 se dio por terminada la **Cuadragésima** Reunión Ordinaria del Comité Especializado.

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidente del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

Mtra. Rebeca Escobar Briones
Presidente del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ricardo Morán González

Ing. Ricardo Morán González
Secretario Técnico del Comité

Fecha: jueves, 13 de abril de 2023

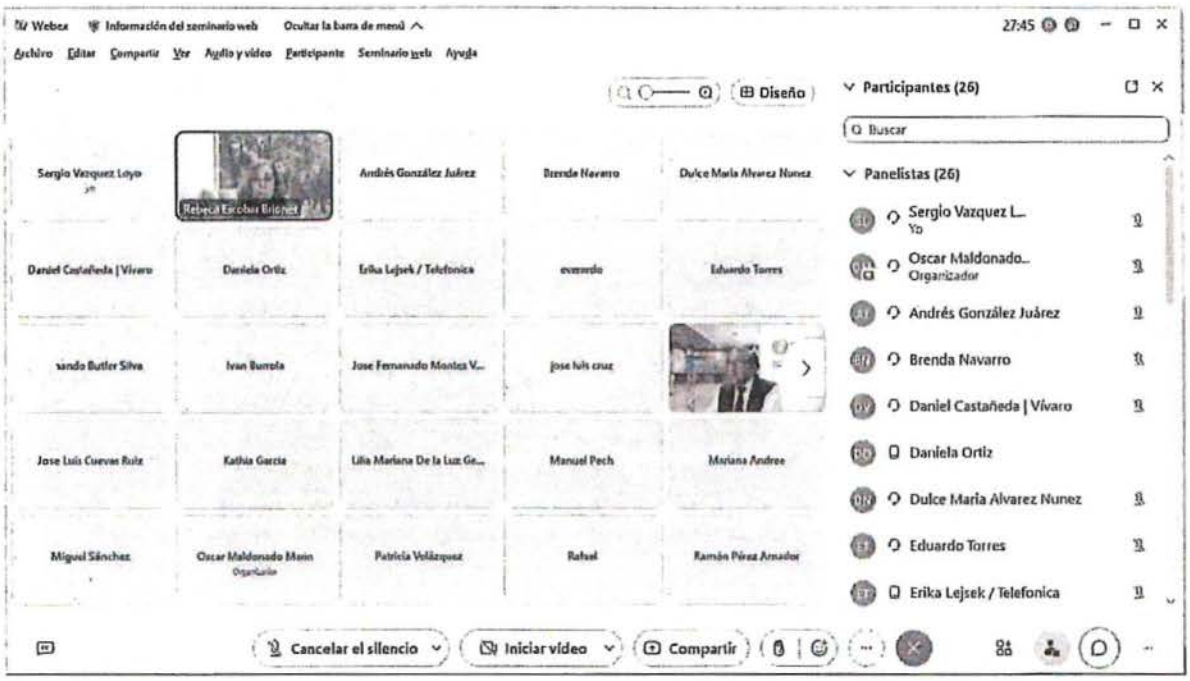
La presente hoja forma parte del Acta de la Cuadragésima Reunión Ordinaria del Comité Especializado.

Empresa	Nombre completo	Correo electrónico
ANATEL	Kathia García	kgarcia@anatel.org.mx
AXTEL	Michelle Ruíz	pruiz@axtel.com.mx
BENELEIT, COMERCIALIZADORA ROMEL, AFCAZA Y TENTIA	Lilia Mariana de la Luz Gerardo	liliamarianadelaluzgerardo@gmail.com
CELMAX, GUGA, WIMO, BROMOVIL	Daniela Ortiz	daniela.ortiz@inaece.com
FLO NETWORKS	Fernando Madrid	fme@flo.net
FLO NETWORKS	Iván Burrola	ibo@flo.net
FLO NETWORKS	Manuel Pech	jps@flo.net
GOGATEL S.A. DE C.V	Rafael Gómez Martínez	rafaelgm68@hotmail.com
IFT	Dulce María Álvarez Núñez	dulce.alvarez@ift.org.mx
IFT	Fernando Butler Silva	fernando.butler@ift.org.mx
IFT	José Luis Cuevas Ruiz	jose.cuevas@ift.org.mx
IFT	Rebeca Escobar Briones	rebeca.escobar@ift.org.mx
IFT	Ricardo Morán Gonzalez	ricardo.moran@ift.org.mx
IFT	Rodrigo Jiménez López	rodrigo.jimenez@ift.org.mx
IFT	Sergio Vázquez Loyo	sergio.vazquez@ift.org.mx
IZZI	José Fernando Montes Venancio	jfmontes@izzi.mx
IZZI	Ramón Pérez Amador	rperezam@izzi.mx
KONECTA DE MÉXICO S DE RL DE CV	José Luis Cruz	mexmex2@konecta.mx
MARCATEL	Valeria Hernández	vhernandez@marcatel.net
MARCATEL COM | CCA	Brenda Navarro	bnavarro@vivaro.com
MARCATEL COM | CCA	Daniel Castañeda	dcastaneda@vivaro.com
MARKETING 358, REDPHONE, EDILAR Y TELMOV	Mariana Andree Cuevas	mariana.andree@inaece.com
ROAD9 VASP, S. DE R.L. DE C.V.	Nancy Hernández	nancy.hernandez@banda-ancha.com.mx
SECNESYS	Eduardo Torres	jose.torres@secnesys.com
SECNESYS	Everardo Molina	everardo.molina@secnesys.com
SECNESYS	Patricia Velázquez	patricia.velazquez@secnesys.com
TELEFÓNICA	Erika Lejsek	erika.lejsek@telefonica.com
TELMEX	Miguel Sánchez	msbarqui@telmex.com
TOTALSEC	Andrés González Juárez	andres.gonzalezj@totalsec.com.mx

RM6

Fecha: jueves, 13 de abril de 2023

La presente hoja forma parte del Acta de la Cuadragésima Reunión Ordinaria del Comité Especializado.



RMG

Fecha: jueves, 15 de junio de 2023

ACTA RELATIVA A LA CUADRAGÉSIMA PRIMERA SESIÓN ORDINARIA DEL COMITÉ ESPECIALIZADO DE ESTUDIOS E INVESTIGACIONES EN TELECOMUNICACIONES A QUE SE REFIERE EL CAPÍTULO X DE LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA.

En la Ciudad de México, siendo las 11 horas 10 minutos del día quince de junio del año dos mil veintitrés, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Cuadragésima Primera Sesión Ordinaria del Comité Especializado**, de conformidad con lo establecido en el "*Acuerdo mediante el cual el Comisionado Presidente del Instituto Federal de Telecomunicaciones a que se refiere el Capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y designa a los servidores públicos que formaran parte del mismo*", publicado en el Diario Oficial de la Federación el veintidós de enero de dos mil dieciséis, adicionalmente, de conformidad con el "*ACUERDO que determina la conclusión de la vigencia del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones, por causa de fuerza mayor, determina los casos en que se suspenden los plazos y términos de ley, con fundamento en lo dispuesto en los artículos 28, párrafos segundo y tercero de la Ley Federal de Procedimiento Administrativo; 115, segundo párrafo y 121 de la Ley Federal de Competencia Económica, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19, así como sus excepciones, a fin de preservar las funciones esenciales a cargo del propio Instituto y garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión.*" publicado en el Diario Oficial de la Federación el 20 de agosto de 2021 y su modificación publicada el 01 octubre de 2021, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

1. **Verificación de quorum. Lista de asistencia y presentación de los representantes de Concesionarios de Telecomunicaciones y Autorizados.**

   La Presidente del Comité Especializado, dio la palabra al Secretario del Comité para verificar el quorum de la sesión.

   En uso de la palabra, el Secretario del Comité Especializado, pidió a los representantes presentarse e indicar a quién representaban, posterior a ello informó a la Presidente que se contó con el quorum necesario para declarar válida la presente sesión.

   La lista de asistencia que se generó en la presente reunión se anexa al Acta y forma parte integrante de la misma.

2. **Lectura del Orden del Día.**

La Presidente del Comité Especializado inició la sesión y cedió la palabra al Secretario Técnico del Comité, para dar lectura del orden del día.

El Secretario Técnico del Comité dio lectura al siguiente:

ORDEN DEL DÍA

1. Verificación de quorum. Lista de asistencia y presentación de los representantes de concesionarios de telecomunicaciones y autorizados.
2. Lectura del orden del día.
3. Aprobación del Orden del Día.
4. Informe de los comentarios recibidos de parte de los miembros del Comité Especializado de Estudios, en relación con los reportes de los siguientes estudios:
    - **"Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta Edición"**. Responsable ANATEL
5. Presentación de los operadores y autorizados de nuevas propuestas de estudios.
6. Invitación a los miembros del Comité a presentar nuevas propuestas de estudios.
7. Fecha de la próxima sesión.
8. Asuntos Generales.

La Presidente del Comité preguntó a los asistentes si deseaban integrar cualquier otro punto, comentario o modificación al Orden del Día.

Los asistentes no manifestaron ningún otro tema para incluir en el Orden del Día.

3. **Aprobación del Orden del Día.**

El Secretario Técnico del Comité Especializado puso a consideración de los representantes el Orden del Día, no hubo manifestaciones de objeción a la misma, por lo tanto, la Presidente del Comité señaló que el Orden del Día se dio por aprobado por unanimidad en los términos en que fue presentado.

4. **Informe de los comentarios recibidos de parte de los miembros del Comité Especializado de Estudios, en relación con los reportes de los siguientes estudios:**

La Presidente del Comité dio seguimiento al Orden del Día consistente con el informe de cierre de los estudios.

- Reporte sobre el estudio: **"Estudio estadístico del número de terminales móviles de llamadas móviles y casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta Edición"**. Responsable ANATEL

  La Presidente del Comité recordó el Acuerdo Primero de la sesión anterior, el cual señala lo siguiente:

  > "PRIMERO. El representante de la ANATEL mencionó que continúan con la atención de los comentarios recibidos sobre del "Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición". Señaló que dicho estudio final con los comentarios atendidos será enviado al correo electrónico del Secretario Técnico del Comité Especializado en un plazo de al menos una semana contada a partir de esta sesión ordinaria."

  Por lo que, el Secretario Técnico del Comité informó que el 21 de abril, ANATEL envió la versión final de su estudio al correo del secretario técnico, asimismo, el 25 de abril, dicho estudio se reenvió con carácter informativo, a los miembros del Comité.

  ANATEL no tuvo comentarios sobre lo señalado.

De igual manera, la Presidente del Comité pidió al Secretario Técnico el informe sobre el segundo estudio:

- **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"**. Presentado por: Axtel, S.A.B. de C.V., Grupo Televisa (Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V.

  Por lo que, el Secretario Técnico mencionó que el 08 de mayo envió el estudio en comento a los miembros del Comité con carácter informativo.

Por lo que la Presidente del Comité dio por concluido todos los puntos sobre los estudios.

5. **Presentación de los operadores y autorizados de nuevas propuestas de estudios.**

   En este Punto la Presidente, pidió a los representantes ante este Comité que presentaran sus nuevas propuestas de Estudio

   Ningún concesionario o grupo de trabajo se manifestó al respecto.

6. Invitación a los miembros del Comité a presentar nuevas propuestas de estudios

La Presidenta reiteró la invitación para la presentación de nuevos estudios, recordando que es una obligación establecida en su Título de Concesión y en el Título 8° de la Ley Federal de Telecomunicaciones y Radiodifusión, relativo a la colaboración con la justicia, que establece en el artículo 190 fracción XII, que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional.

La Presidente comentó a los miembros del Comité que aún no se han integrado a un grupo, así lo hagan, o planten temas en lo individual para la elaboración de nuevos estudios o bien, para que presenten nuevas propuestas de estudio para el siguiente período, con el objeto de dar cumplimiento a lo establecido en la normativa antes señalada.

El representante de Konecta de México reiteró acerca de los artículos 189 y 190 de la LFTR y propone ampliar los temas que se desarrollan en este Comité con respecto a la Seguridad Nacional. Señaló que hay más gente que utiliza las comunicaciones para delinquir, por lo que debemos ser más amplios, en los temas, no solo la parte técnica y estadística, ya que cada vez hay menos opiniones o motivaciones por participar.

La Presidente del Comité le propone al representante de Konecta que forme un grupo de trabajo con algún otro Concesionarios para que se analice la temática de los estudios que establece la ley.

Por otro lado, Daniel Castañeda, representante de Axtel, S.A.B. de C.V., Grupo Televisa (Cable Sistema de Victoria, S.A. de C.V., Cablevisión S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., TV Cable de Oriente, S.A. de C.V., Cablevisión Red, S.A. de C.V., FTTH de México, S.A. de C.V., Operbes, S.A. de C.V., México Red de Telecomunicaciones, S.A. de C.V., Televisión Internacional, S.A. de C.V.), Coordinadora de Carrier´s, S.A. de C.V., Megacable Comunicaciones México (MCM), Celmax Móvil S.A. de C.V., Marcatel Com, S.A. de C.V., Alestra Servicios Móviles, S.A. de C.V. y OpenIP Comunicaciones, S.A. de C.V. mencionó que desean darle una continuidad al estudio entregado recientemente, y asimismo hace la invitación para el resto de los miembros del Comité a integrarse a dicho estudio.

La Presidente del Comité solicitó al Secretario Técnico enviar el extracto del acta de una sesión previa en la cual se menciona el listado de temas de las propuestas de estudios que podrían desarrollarse en este Comité.

Por otra parte, los miembros del Comité no manifestaron ningún otro comentario.

RHG

7. **Fecha de la próxima sesión**

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de agosto de 2023, a las 11 horas.

8. **Asuntos Generales.**

Sin asuntos generales por tratar.

ACUERDOS GENERALES

PRIMERO. Se presentó el resumen histórico sobre el *"Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país. Sexta edición"* entregado por la ANATEL.

Asimismo, se presentó el resumen histórico sobre el **"Estudio de identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos"** entregado por el Grupo de Trabajo integrado por *Axtel, Grupo Televisa (Izzi),* Coordinadora de Carrier´s, S.A. de C.V., *Megacable Comunicaciones México (MCM), Celmax, Marcatel, Alestra Servicios Móviles y OpenIP Comunicaciones,* presentó los comentarios atendidos sobre su propuesta

Por lo que La Presidente del Comité recordó que ambos estudios fueron compartidos a los miembros de este Comité con carácter informativo.

SEGUNDO. La Presidente del Comité Especializado reiteró la invitación a los miembros del Comité para la presentación de nuevos estudios, recordando que es una obligación establecida en su Título de Concesión y en el Título 8° de la Ley Federal de Telecomunicaciones y Radiodifusión, relativo a la colaboración con la justicia

TERCERO. La Presidenta del Comité propone al representante de Konecta que forme un grupo de trabajo con algunos otros concesionarios para que se analice la temática de los estudios que establece la ley.

CUARTO. La Presidenta del Comité solicitó al Secretario Técnico enviar el extracto de un acta pasada en la cual se menciona el listado de temas de las propuestas de estudios que podrían desarrollarse en este Comité.

RMG

QUINTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de agosto de 2023, a las 11 horas.

Cierre de la sesión.

Atendido el Orden del Día, la Presidente del Comité Especializado agradeció la participación de los Concesionarios y Autorizados.

Siendo las 12:41 horas del día 15 de junio de 2023 se dio por terminada la **Cuadragésima Primera** Reunión Ordinaria del Comité Especializado.

Los acuerdos alcanzados en esta reunión del Comité Especializado, que se plasman en la presente acta, tendrán plena validez sin perjuicio de la carencia de firmas autógrafas de los Concesionarios y Autorizados que participaron en ésta, los cuales se listan a continuación, bastando la firma autógrafa de la Presidente del Comité y Secretario Técnico del mismo y su envío por medios electrónicos por parte del Instituto.

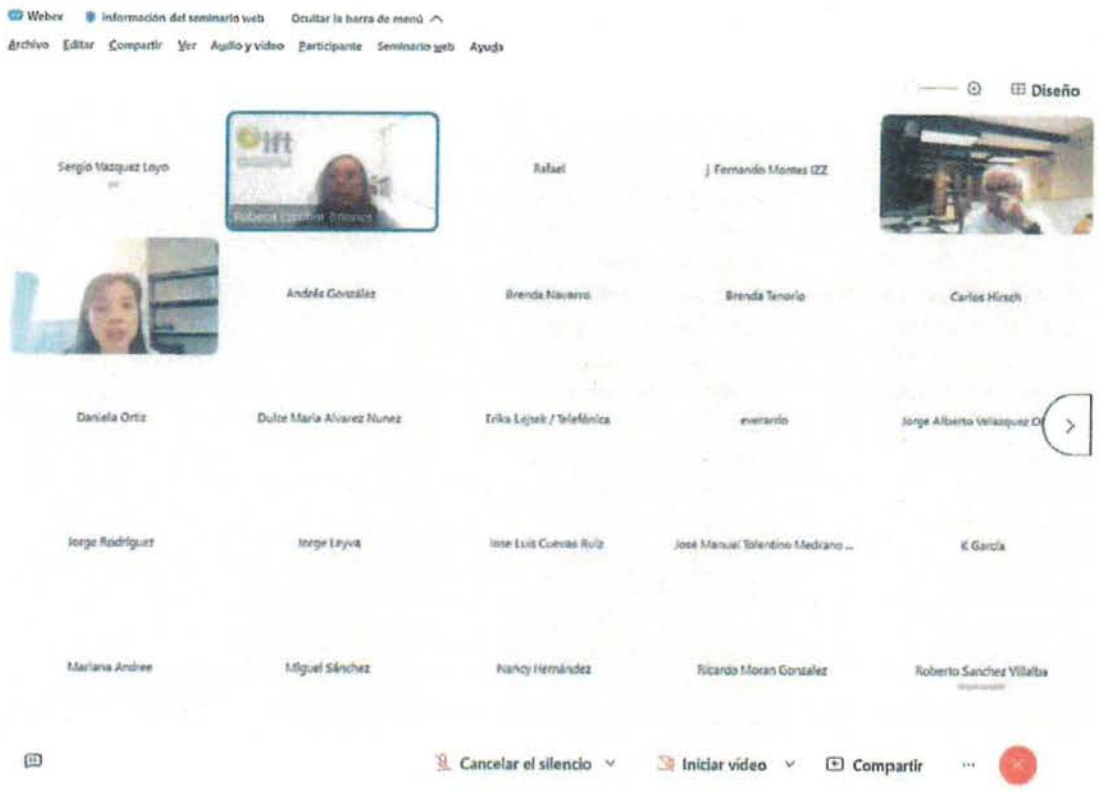
Mtra. Rebeca Escobar Briones
Presidente del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ricardo Morán González

Ing. Ricardo Morán González
Secretario Técnico del Comité

Fecha: jueves, 15 de junio de 2023

La presente hoja forma parte del Acta de la Cuadragésima Primera Reunión Ordinaria del Comité Especializado.



RMG

Fecha: jueves, 15 de junio de 2023

La presente hoja forma parte del Acta de la Cuadragésima Primera Reunión Ordinaria del Comité Especializado.

Nombre	Correo electrónico	Empresa
Kathia García	kgarcia@anatel.org.mx	ANATEL
Carlos Hirsch	carlos.hirsch@att.com	ATT
José Manuel Tolentino Medrano	jt789j@mx.att.com	ATT
Yessica Toledo	yt191r@mx.att.com	ATT
Ana Herrera	aherrerac@axtel.com.mx	AXTEL
Hugo Martínez	hugo.martinez@canieti.mx	CANIETI
Rafael Gómez	rafaelgm68@hotmail.com	GOGATEL
Yessica Alvarado	yessica.alvarado@gogatel.mx	GOGATEL
Dulce María Álvarez Núñez	dulce.alvarez@ift.org.mx	IFT
Jorge Alberto Velázquez Olvera	jorge.velazquez@ift.org.mx	IFT
José Luis Cuevas Ruíz	jose.cuevas@ift.org.mx	IFT
Rebeca Escobar Briones	rebeca.escobar@ift.org.mx	IFT
Ricardo Morán Gonzalez	ricardo.moran@ift.org.mx	IFT
Rodrigo Jimenez López	rodrigo.jimenez@ift.org.mx	IFT
Sergio Vázquez Loyo	sergio.vazquez@ift.org.mx	IFT
Brenda Tenorio	brenda.tenorio@inaece.com	INAECE
Fernando Montes	jfmontes@izzi.mx	IZZI
José Luis Cruz	mexmex2@konecta.mx	KONECTA
Brenda Navarro	bnavarro@vivaro.com	Marcatel (Vivaro)
Daniel Castañeda	dcastaneda@vivaro.com	Marcatel (Vivaro)
Valeria Hernández	vhernandez@marcatel.net	Marcatel (Vivaro)
Erika Lejsek	erika.lejsek@telefonica.com	Pegaso SA de CV (Telefónica)
Nancy Hernández	nancy.hernandez@banda-ancha.com.mx	Road9 Vasp
Jorge Leyva	jorge.leyva@secnesys.com	Secnesys / Marcatel (Vivaro)
Jorge Rodríguez	jorge.rodriguez@secnesys.com	Secnesys / Marcatel (Vivaro)
Everardo Molina	everardo.molina@secnesys.com	Secnesys / Marcatel (Vivaro)
Miguel Sánchez	msbarqui@telmex.com	TELMEX
Mariana Andree	mariana.andree@inaece.com	Telmov móvil, Comercializadora Romel, Afcaza, Bene leit, Edilar y Tentia Consulting Group;
Andrés González	andres.gonzalezj@totalsec.com.mx	Totalplay
Daniela Ortiz	daniela.ortiz@inaece.com	Wirnotelecom, Guga Telecom, Celmax Móvil, Marketing 358, Brocomunicaciones móviles y Negocios integrales de México.

ANEXO II

ESTUDIOS CONCLUIDOS

Descargo de responsabilidad. El resultado de los presentes estudios, así como los comentarios y conclusiones de los mismos son responsabilidad del autor que los desarrolla y presenta, sin que necesariamente represente el punto de vista de los demás integrantes del Comité ni del propio IFT.

Nombre del estudio:

"ESTUDIO ESTADÍSTICO DEL NÚMERO DE TERMINALES MÓVILES, DE LLAMADAS DE MÓVILES Y DE CASETAS TELEFÓNICAS PÚBLICAS QUE OPERAN DENTRO DE UNA MUESTRA DE PENALES EN EL PAÍS. SEXTA EDICIÓN"

Estudio presentado por la
ANATEL

ESTUDIO ESTADÍSTICO DEL NÚMERO DE TERMINALES MÓVILES, DE LLAMADAS DE MÓVILES Y DE CASETAS TELEFÓNICAS PÚBLICAS QUE OPERAN DENTRO DE UNA MUESTRA DE PENALES EN EL PAÍS
SEXTA EDICIÓN

Presentado por un Grupo de Trabajo de concesionarios participantes en el Comité Especializado de Estudios e Investigaciones en Telecomunicaciones a que se refiere el capítulo X de los Lineamientos de Colaboración en Materia de Seguridad y Justicia.

Introducción

Resaltamos que los resultados presentados de estudios realizados desde 2016, podrían ser un insumo para que las autoridades correspondientes consideren decisiones de política pública orientadas a implementar medidas que combatan la introducción de equipos a los centros penitenciarios, la cual viola disposiciones legales vigentes; o enfocadas en garantizar que los inhibidores de señal instalados en estos sitios cumplan con la normatividad dispuesta por el propio IFT (DT-010). Esto es, no consideramos aconsejable ni deseable imponer barreras de acceso a las tecnologías y grandes costos financieros a las instituciones.

En esta edición del estudio participaron los concesionarios nacionales del servicio móvil. Como en años anteriores, se analizó el número de equipos celulares estimados, las tarjetas SIMs asociadas a éstos y las llamadas generadas desde una muestra de recintos penitenciaros ubicados en el territorio nacional. Es necesario aclarar que este documento sólo indica los resultados obtenidos en una muestra de establecimientos penitenciarios durante el tiempo de revisión, por lo que **el tamaño de dicha muestra no permite hacer una generalización de los resultados para los 315 centros que operaban al cierre de 2021**[1].

El objeto de la investigación es actualizar las observaciones realizadas desde 2016 sobre el número de equipos terminales móviles que operan dentro de una muestra de recintos penitenciarios, y cuya actividad es monitoreada de manera simultánea por los concesionarios de redes móviles a lo largo de 3 semanas consecutivas. Dar continuidad a esta investigación permitirá a empresas y autoridades observar la dimensión del problema en materia de seguridad y su evolución. Para las empresas, esto es particularmente relevante porque esta situación afecta de manera significativa a los usuarios legítimos que residen o transitan en zonas aledañas a dichos recintos, pues las interferencias generadas por bloqueadores de señal que no funcionan apropiadamente distorsionan la calidad de los servicios móviles.

Este seguimiento es relevante, pues en 2018 entró en vigor la Disposición Técnica IFT-010-2016, emitida por el Instituto Federal de Telecomunicaciones (IFT), cuyo objetivo es:

> *"... establecer las especificaciones técnicas y condiciones de operación para los equipos de bloqueo de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen en las bandas de frecuencia que se utilicen para la recepción en los equipos terminales de comunicación, así como los métodos de prueba para comprobar el cumplimiento de dichas especificaciones."*
>
> De acuerdo con lo establecido en el Transitorio Tercero de la mencionada Disposición:

[1] Censo Nacional de Sistema Penitenciario Federal y Estatales 2022, julio 2022.

"Los equipos de bloqueo de señales instalados en centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación, deberán adecuarse técnicamente a lo establecido en la presente Disposición Técnica, en un plazo no mayor de veinticuatro meses contados a partir de la entrada en vigor de la presente Disposición Técnica."

Los resultados de la investigación actual y los datos históricos nos permiten deducir que en los recintos incluidos en la muestra los bloqueadores de señal podrían estar cumpliendo con la normatividad; sin embargo, otros factores explican que continúe la utilización de los equipos sin que la señal se inhiba.

Metodología

Considerando los resultados del año anterior, para el estudio del año 2021 se sustituyeron los penales identificados como "B" y "C" con otro que ofrece la ventaja de contar con mayor población, haciendo que la muestra sea más representativa; es identificado como el recinto "3" a lo largo del documento; el resto de recintos se mantuvo sin cambios. En la presente edición todos los recintos son de administración estatal.

La metodología empleada es la que se ha seguido en los años anteriores. En la primera fase se analizó de manera simultánea la información proveniente de cada uno de los concesionarios, durante las tres semanas consecutivas. Los datos en los cuadros se presentan por semana para observar claramente cómo evoluciona cada variable. Las cifras son el resultado de la suma de llamadas, de equipos e IMSIs identificados como "sospechosos" por los operadores móviles en cada penal: Altán Redes, AT&T, Telcel y Telefónica Movistar.

En la segunda fase del análisis, se destinó también una elevada proporción del tiempo y recursos disponibles en el Grupo de Trabajo en el cruce de los datos con una importante cantidad de variables; en esta labor resalta la identificación del número de llamadas como un elemento muy importante en la investigación, no solo por los resultados totales identificados en sí, sino por las proporciones que guarda este indicador con respecto al número de equipos e IMSIs; a lo cual le hemos llamado **Índice promedio de intensidad en el uso de un equipo para realizar llamadas**.

Recabar la información, es un ejercicio que requiere de numerosas horas-hombre en distintas etapas y de inversiones adicionales que permitan distinguir con precisión los

equipos, IMSIs y el tráfico de los usuarios en una radio base aledaña al penal, que en muchos casos está rodeado de una amplia población civil, de las comunicaciones que tienen lugar desde un penal al exterior.

En la fase de recolección de datos, se identificaron sectores y radiobases; cada empresa requiere dedicar a esta labor un día de pruebas y, a lo largo de cada semana, el equivalente a dos personas durante 7 días hábiles con jornadas de 9 horas por penal. Para el análisis de la información se emplea a personal por el equivalente a 4 días hábiles por recinto, en la que intervienen dos analistas, un supervisor y un miembro del equipo de regulación.

Principales resultados del análisis en Telefonía Móvil

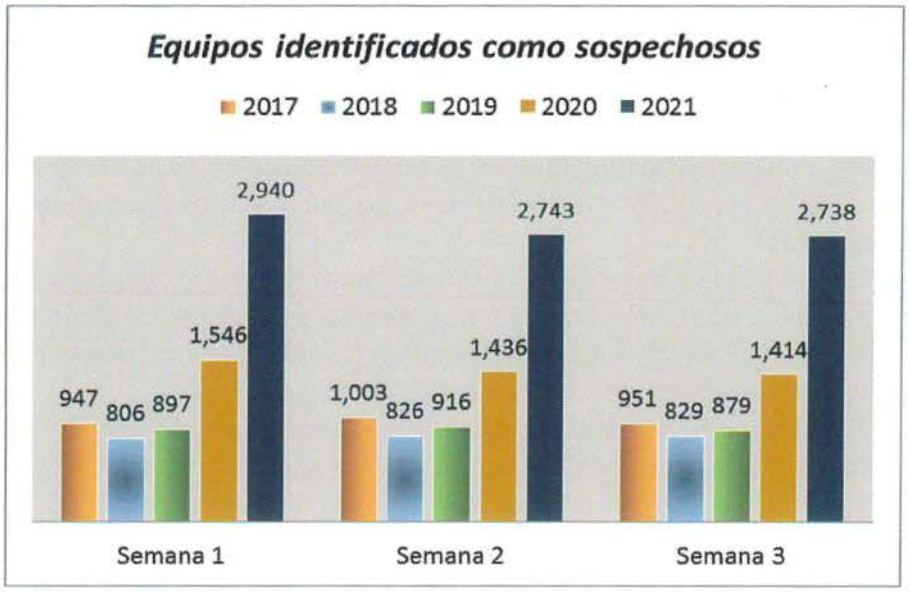
1. Los criterios para identificar a un equipo como "sospechoso" de ser utilizado para hacer llamadas desde un penal son: a) registrar un número atípico de llamadas salientes respecto del promedio registrado en esa radiobase; b) identificación de llamadas generadas desde varias tarjetas SIMs, que contienen un IMSI (Identidad Internacional de Abonado Móvil por sus siglas en inglés), y que estén funcionando con un solo IMEI (Identidad Internacional de Equipo Móvil por sus siglas en inglés) o viceversa; y, c) la modalidad de pago por servicios (solo participan los de prepago).
2. **Durante 2021 se observaron resultados contradictorios: para todas las semanas se observa un aumento del 91% de los equipos identificados como sospechosos; sin embargo, es notable que las llamadas cayeron 20% en promedio. Por primera vez se observa una disminución en las llamadas generadas.**
3. La investigación identificó **la cifra más alta de equipos sospechosos desde que inició el monitoreo en 2016**. Esta tendencia se repite en los IMSIs, con aumentos promedio de 85% para cada semana comparado al año anterior. En parte puede resultar de los cambios en los recintos bajo estudio y sus características, lo cual se debe por cierto a que las autoridades han cerrado algunos penales federales por temas de control e inseguridad.
   Se encontraron 2,940 equipos terminales "sospechosos" durante la primera semana de levantamiento de datos, relacionados con el uso de 3,573 IMSIs; durante la segunda semana se identificaron 2,743 equipos con 3,050 IMSIs asociadas; y, para la tercera semana, se hallaron 2,738 terminales utilizando 3,666 IMSIs. En promedio el 15% de los equipos "sospechosos" utilizó más de una IMSI.
4. Al comparar estas cifras con las semanas de estudio del año anterior, cuantificamos un incremento en el volumen de equipos del 90% y 77% para IMSIs en la primera. Durante la semana 2 los equipos operando se incrementan 91% y 61% los IMSIs. Para la tercera semana los equipos identificados aumentan 93% y 116% las IMSIs. Esta relación entre equipos e IMSIs se observa en las gráficas 1 y 2.

5. **La generación de llamadas desde los recintos presentó una tendencia a la baja por primera vez**, registrando caídas semanales de hasta 26% con respecto a los

valores de 2020. Se cuantificaron 266,663 llamadas durante la primera semana, 268,636 para la segunda, y 201,898 en la tercera.

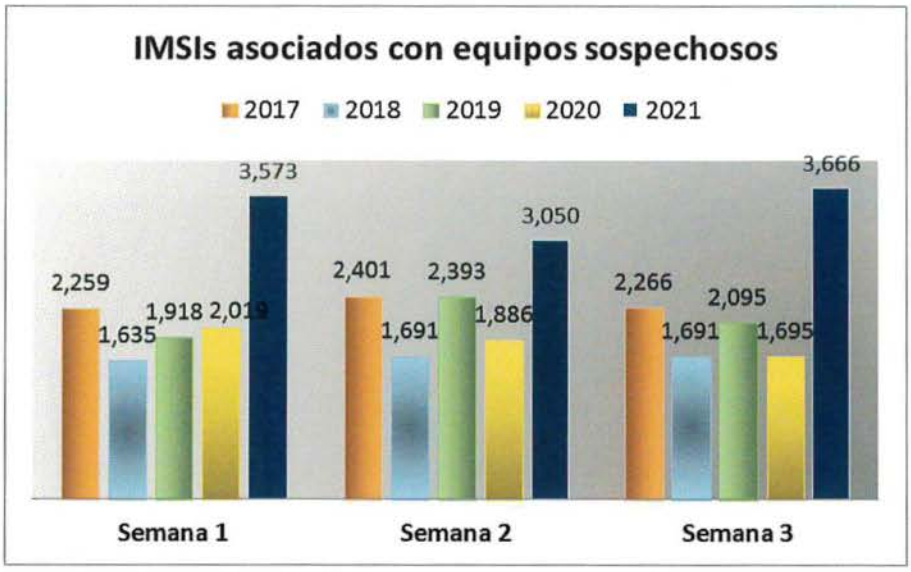
6. Cuando analizamos el **Índice promedio de intensidad en el uso de un equipo para realizar llamadas**, encontramos una disminución crítica que se explica por el alza en los equipos identificados y la caída en el volumen de llamadas; en 2021 dicho índice cayó en promedio 63% con respecto al periodo anterior; las gráficas 3 y 4 ilustran esta tendencia.

Gráfica 1



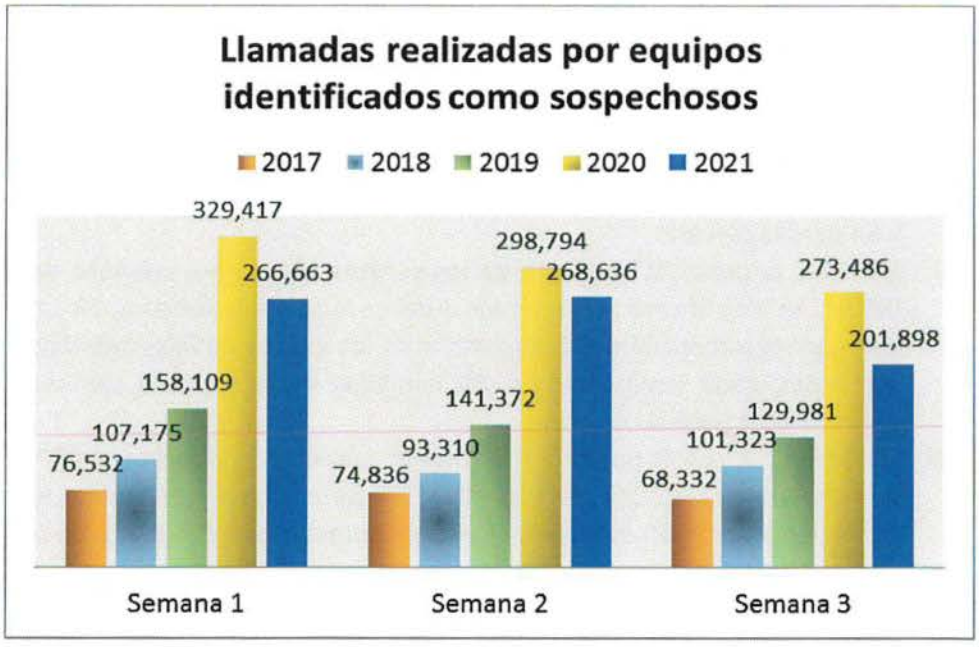
Fuente: Investigación ANATEL

Gráfica 2



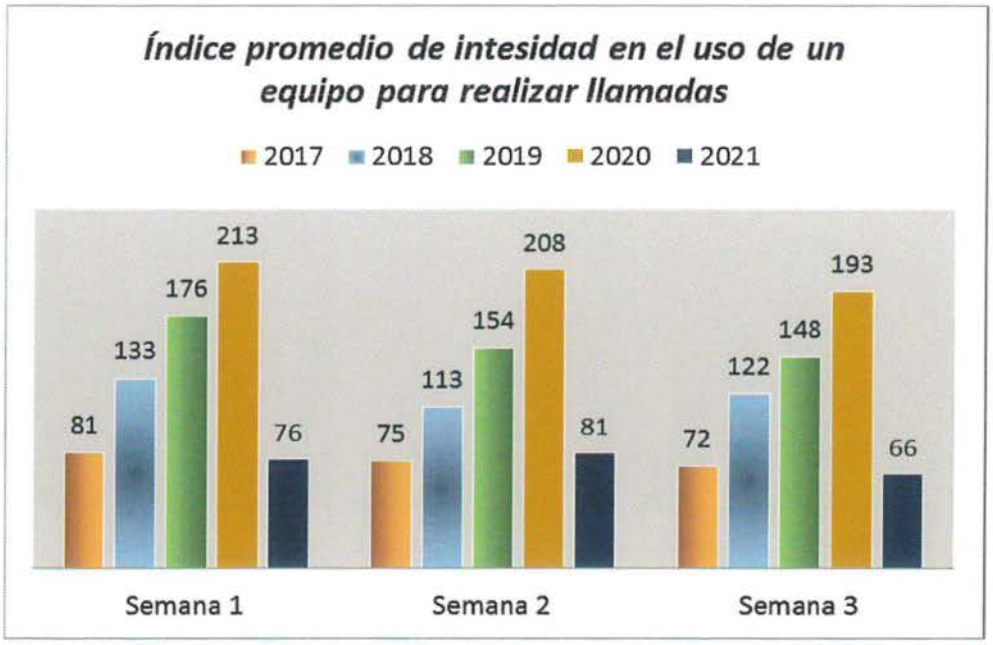
Fuente: Investigación ANATEL

Gráfica 3



Fuente: Investigación ANATEL

Gráfica 4



Fuente: Investigación ANATEL

7. A nivel individual, las tendencias descritas previamente en llamadas y equipos identificados como sospechosos se repite para todos los penales.
8. El recinto **"3", añadido a la muestra en sustitución de "B" y "C", encontramos un alto número de equipos y un bajo índice de intensidad de llamadas.** En promedio 742 aparatos por semana que realizaron 134,966 llamadas durante el periodo; el índice de intensidad fue de 57 en la primera semana, 61 en la segunda y 64 para la tercera.
9. En 2021, el penal **"1" fue uno de los centros con menor número de equipos e IMSIs[2].** Se identificaron 63 equipos durante la primera semana, 78 en la segunda y 64 para la tercera. Sin embargo, tiene de los **índices de intensidad más altos**. En promedio, cada equipo realizó 93 llamadas en la primera semana, 88 en la segunda y 77 para la tercera.
10. **El recinto "2" es el penal con el mayor número de equipos**, 1,097 durante la primera semana, 1,004 en la segunda y 987 para la tercera. El índice de intensidad de llamadas también es el **más alto de la muestra** con 121 llamadas por terminal durante la primera semana, 138 durante la segunda, y 85 en la tercera. El total de llamadas generadas desde este recinto fue 355,155. También se cuantifica un número elevado de IMSIs, 976 durante la primera semana, 952 en la segunda y 944 en la última.

[2] Tal y como se reportó en la Quinta Edición del Estudio, en 2020 los penales 1 y 2 fueron incorporados a la muestra en sustitución de los centros penitenciarios que dejaron de operar.

Tres penales continúan siendo parte de la muestra desde el primer estudio en 2016, a continuación se presenta un análisis comparativo a través de los años para destacar hallazgos de interés en cada uno. Las cifras representan el promedio semanal de cada variable.

11. **En el recinto "D" cada año se han identificado incrementos constantes de equipos e IMSIs. Sin embargo, las llamadas generadas solo representaron el 35% del volumen de 2020.** Se cuantifican 149 equipos durante la primera semana, 148 en la segunda y 145 para la tercera; el índice de intensidad de llamadas por terminal durante la primera y segunda semana fue de 26 y en la tercera 25. En promedio operaron 139 IMSIs**, 18% más con respecto al volumen de 2020.**
12. **"E"** se ha caracterizado por ser **de los recintos con mayor número de equipos y llamadas en la muestra.** Para 2021 encontramos una disminución en el número de equipos e IMSIs, 5% y 25% respectivamente. Las llamadas generadas cayeron 56%. En promedio 717 aparatos por semana que realizaron 196,720 llamadas durante el periodo; el índice de intensidad fue de 97 en la primera semana, 98 en la segunda y 78 para la tercera.
13. Cuando analizamos **"F" no observamos una tendencia clara,** todas las variables un año aumentan y al siguiente disminuyen. En 2021 se cuantifican 123 equipos durante la primera semana, 91 en la segunda y 101 para la tercera. En promedio operaron 100 IMSIs**, 3.5 veces más con respecto al volumen de 2020.**

Datos de la investigación en recintos penitenciarios por semana, 2021

Semana 1

Penal	Equipos	SIMs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas /equipos
1	63	54	6	2	5,837	93
D	149	145	27	5	3,912	26
E	753	852	134	74	73,194	97
F	123	110	13	5	7,779	63
2	1,091	976	199	6	132,220	121
3	761	1,436	92	8	43,721	57
Total	**2,940**	**3,573**	**471**	**NA**	**266,663**	**NA**

Fuente: Investigación ANATEL

Semana 2

Penal	Equipos	IMSIs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas /equipos
1	78	71	7	2	6,856	88
D	148	137	23	5	3,846	26
E	698	827	120	82	68,631	98
F	91	98	15	4	6,598	73
2	1,004	952	169	6	138,616	138
3	724	965	83	9	44,089	61
Total	**2,743**	**3,050**	**417**	**NA**	**268,636**	**NA**

Fuente: Investigación ANATEL

Semana 3

Penal	Equipos	SIMs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas/equipos
1	64	58	2	2	4,958	77
D	145	136	22	5	3,658	25
E	700	797	104	75	54,895	78
F	101	91	9	3	6,912	68
2	987	944	167	5	84,319	85
3	741	1,640	87	8	47,156	64
Total	**2,738**	**3,666**	**391**	**NA**	**201,898**	**NA**

Fuente: Investigación ANATEL

Cifras históricas anuales

Recinto "D"

Año	Equipos	SIMs	Llamadas semanales	Llamadas /equipos
2017	18	38	909	51
2018	35	70	1,867	53
2019	52	77	1,771	34
2020	98	118	10,735	110
2021	147	139	3,805	26

Fuente: Investigación ANATEL

Recinto "E"

Año	Equipos	SIMs	Llamadas semanales	Llamadas /equipos
2017	505	1257	40,492	80
2018	464	1,024	57,196	123
2019	550	1386	107,523	195
2020	759	1,094	146,176	193
2021	717	825	65,573	91

Fuente: Investigación ANATEL

Recinto "F"

Año	Equipos	SIMs	Llamadas semanales	Llamadas /equipos
2017	74	141	3,317	45
2018	45	79	2,548	57
2019	106	183	5,468	52
2020	28	28	6,480	231
2021	105	100	7,096	68

Fuente: Investigación ANATEL

Implicaciones

Los esfuerzos de contención en el uso de equipos dentro de recintos penitenciarios realizados por las autoridades registran algunos avances, aunque se confirma que siguen operando equipos sospechosos en el conjunto de los penales de la muestra; mismos que realizan un menor número de llamadas que es el hallazgo más significativo en esta edición del estudio. Sin embargo, donde hay pocos teléfonos se observa que se realizan una gran cantidad de llamadas, afectando tanto a los usuarios como la calidad del servicio.

En años anteriores las autoridades al más alto nivel han dado pasos firmes al acordar una amplia colaboración con las empresas de telecomunicaciones que permite combatir este flagelo social con el principal propósito de reducir el número de llamadas que salen de penales, evitando posibles acciones de extorsión que afectan de manera económica y psicológica a la población. Posiblemente son estos trabajos los que explican la disminución en el número de llamadas generadas.

El Grupo de Trabajo de los Concesionarios en el Comité Especializado responsable de este estudio, en congruencia con los señalado en el artículo 15 fracción XLIV de la Ley Federal de Telecomunicaciones y Radiodifusión, sugiere a las autoridades penitenciarias la urgencia de diseñar nuevos programas que contribuyan a una mayor reducción de equipos terminales y de IMSIs introducidos en los recintos penitenciarios.

Principales resultados del análisis en Telefonía Fija

En atención al esfuerzo realizado por las empresas de telefonía móvil que participan en este Grupo y considerando el estudio 2017, 2018, 2019 y 2020, se llevó a cabo el mismo ejercicio complementario desde el ámbito de la telefonía fija durante el año 2021. Los principales resultados se presentan a continuación.

Se realizó un análisis de las llamadas originadas en las casetas telefónicas en los recintos durante ocho semanas (tomando la información de la primera semana completa de cada uno de los primeros ocho meses del año 2021). Se analizó el tráfico proveniente de 7 penales, de los cuales 5 de ellos cuentan con la opción habilitada de un mensaje de prevención que indica que la llamada se origina desde un centro penitenciario, a lo cual se le conoce como *Interactive Voice Response* (IVR). El resto de los centros penitenciarios sin IVR[3].

[3] Derivado de que a partir del año 2018 no se tienen bases de datos disponibles para realizar el análisis, se sustituyó el reclusorio "A" por el reclusorio "4"

Del análisis realizado se obtuvieron los siguientes resultados en el año 2021:

- En el total de la muestra se registraron 294,973 llamadas.
- De los cinco centros que cuentan con IVR habilitado el rechazo de llamadas alcanzó un 49.8% del total; en 2020 se observó un 20.1% de rechazo.
- Las llamadas rechazadas oscilan entre 9% y 58%, lo cual muestra un alto índice de variación por recinto penitenciario y sugiere la aversión al lugar de origen de las llamadas.
- El 8.2% del total de las llamadas aceptadas finalizó antes de los primeros 10 segundos.
- La duración promedio de cada llamada aceptada fue de 2.87 minutos, lo que sugiere que se estableció una conversación promedio en lo que refiere al uso residencial.
- Del total de llamadas, el 98% fueron realizadas entre las 7 y las 21 horas. Comparado con el año anterior, en términos de horarios, se observó este nivel dentro de dicho intervalo de horarios.
- Del total de las llamadas, el 54.3% se destinó a teléfonos móviles, el 45.6% a teléfonos fijos, el 0.04% a números especiales y/o de larga distancia internacional[4]. Comparado con el año 2020, las llamadas locales incrementaron en 6 puntos porcentuales y las llamadas a móviles disminuyeron en 2.7 puntos porcentuales.

[4] Se consideran las llamadas de larga distancia internacional, EUA y Canadá y resto del mundo.

Tabla 1. Resumen estadístico del tráfico analizado

Reclusorio	Tipo de Conexión	Porcentaje de Aceptación de Llamadas	Llamadas Procesadas	Duración Promedio (minutos)	Destinos (1)
D	Con IVR	91%	24	2.3	29% Móvil 70% Local
E	Con IVR	50%	262,518	2.9	55% Móvil 45% Local
F	Con IVR	63%	439	3.7	52% Móvil 48% Local
1	Con IVR	42%	2,646	1.5	65% Móvil 35% Local
2	Con IVR	89%	487	3.6	40% Móvil 53% Local
3	Sin IVR	---	1,068	2.6	71% Móvil 26% Local
4	Sin IVR	---	27,791	2.1	47% Móvil 53% Local

Nota: (1) La diferencia porcentual que completa el 100% corresponde al rubro denominado "otros".

Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior de los centros penitenciarios analizados.

Metodología

Se diseñó una muestra que permitió analizar las llamadas provenientes de las casetas telefónicas en 7 centros penitenciarios del país, algunos se mantuvieron en la muestra y fueron analizados durante los estudios de 2017, 2018[5], 2019, 2020 y 2021.

Los centros identificados con letras corresponden a los mismos reclusorios presentados en el estudio de móviles.

[5] Para el año 2018 se sustituyó el recinto "A" por el recinto "4".

Las llamadas analizadas se toman de la primera semana de cada uno de los primeros 8 meses (enero-agosto) del año 2021:

Mes	Inicio	Fin
Enero	Lunes 4	Domingo 10
Febrero	Lunes 1	Domingo 7
Marzo	Lunes 1	Domingo 7
Abril	Lunes 5	Domingo 11
Mayo	Lunes 3	Domingo 9
Junio	Lunes 7	Domingo 13
Julio	Lunes 5	Domingo 11
Agosto	Lunes 2	Domingo 8

Las variables utilizadas fueron:
- Número de llamadas realizadas;
- El reclusorio cuenta o no con IVR;
- Llamadas aceptadas o rechazadas;
- Día de generación de la llamada;
- Hora de generación de la llamada;
- Destino de la llamada (local, celular y otros, que incluye: larga distancia nacional e internacional o números especiales), y;
- Duración de la llamada.

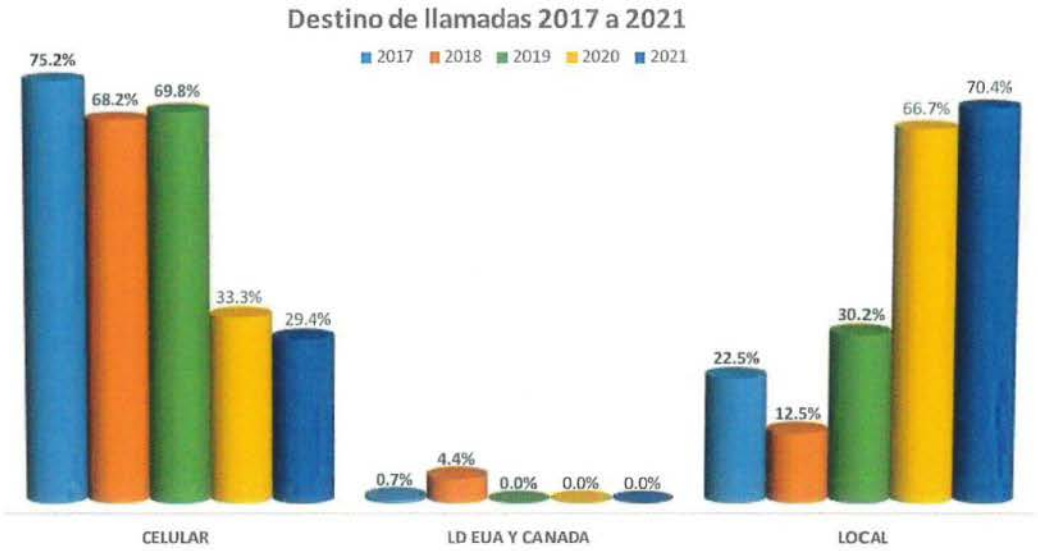
Análisis de Llamadas de Telefonía Fija por Reclusorio

Penal D

Este centro penitenciario registró muy poco tráfico en las casetas telefónicas analizadas. No se observaron llamadas al extranjero o números especiales de las casetas telefónicas, solo se registraron llamadas a teléfonos fijos, así como a móviles; de las escasas llamadas que pasaron por el sistema de IVR, se registró un índice de rechazo del 9% (porcentaje más bajo de rechazo en la muestra).

De las llamadas aceptadas, cuya duración promedio fue de 2.3 minutos, el total de las llamadas se realizaron entre las 7:00 y las 21:00 horas. Asimismo, el 6.1% de las llamadas aceptadas tuvieron una duración menor a los 10 segundos. El 14.2% de las llamadas tuvieron una duración entre 10 y 60 segundos.

De las llamadas generadas, el 29.4% se dirigió a teléfonos móviles, las llamadas cursadas a números locales alcanzaron un 70.4%, es decir, manteniendo la estructura de ambos tipos de llamadas respecto al año anterior. Finalmente, no se registraron llamadas dirigidas a EUA y Canadá o al resto del mundo.



Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal D analizado.

Penal E

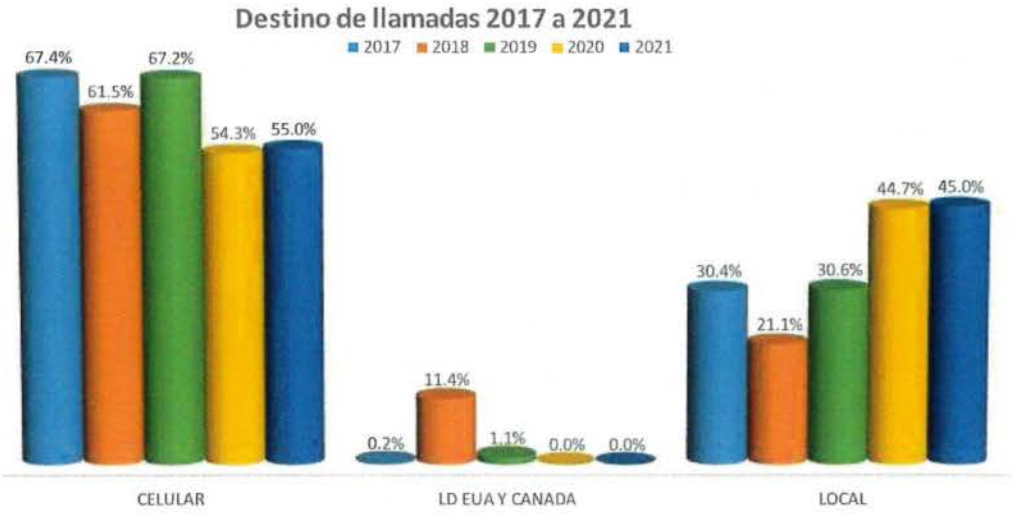
Del total de las llamadas analizadas en este penal, se rechazó el 49.1% de ellas, lo cual representó un aumento de 26% respecto al 2020. Esto sugiere un mejor resultado del IVR implementado.

En relación con el horario de las 131,628 llamadas aceptadas, cuya duración promedio fue de 2.9 minutos, el total de las llamadas se realizaron entre las 7:00 y las 21:00 horas.

El 6.9% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa una reducción de 2% respecto a 2020. Asimismo, el 35.7% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un decremento comparado con el año anterior de 76.6%.

De las llamadas generadas, el 55% se dirigió a teléfonos móviles. En términos generales, lo anterior representa un decremento de 0.7 puntos porcentuales comparado con 2020 (54.3%). Las llamadas cursadas a números locales alcanzaron un 45%, es decir, una

reducción ligera de 0.3% respecto al 2020. Finalmente, no se realizaron llamadas de larga distancia internacional, al resto del mundo ni a números especiales.



Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal E analizado.

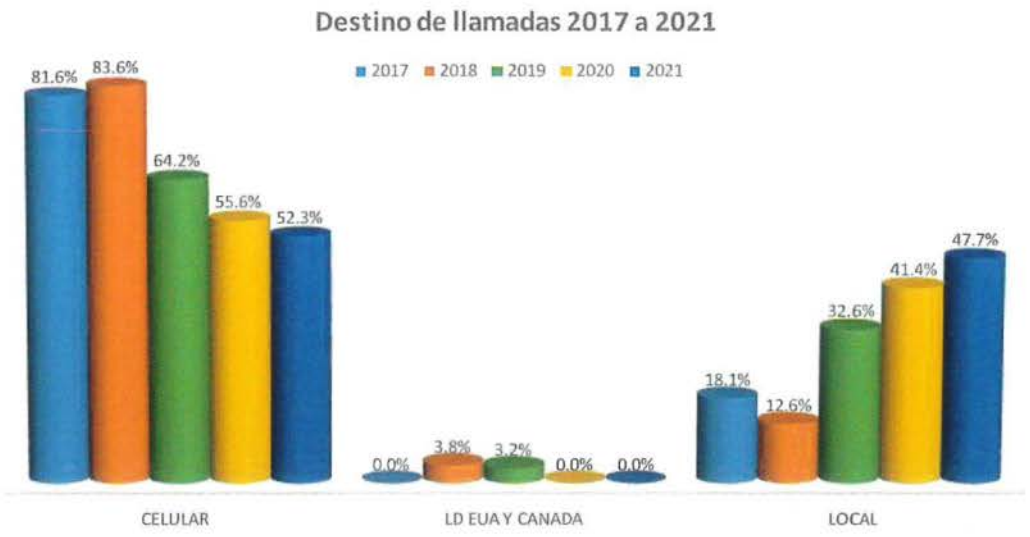
Penal F

Se analizaron 439 llamadas, de las cuales 160 llamadas fueron rechazadas, es decir un 36.4%. Estas llamadas se redujeron un 17.8% respecto al año anterior.

De las llamadas aceptadas, cuya duración promedio fue de 3.7 minutos, el 52.5% de las llamadas se realizaron después de las 7:00 y antes de las 21:00 horas. El 59.6% de las llamadas se rechazaron.

Se observó que el 2.5% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa una variación a la baja de 4.6 puntos porcentuales respecto a 2020. Asimismo, el 20.4% de las llamadas aceptadas tuvieron una duración entre 10 y 60 segundos.

De las llamadas generadas, el 52.3% se dirigió a teléfonos móviles, lo anterior representa una disminución de 3.3 puntos porcentuales comparado con 2020. Las llamadas cursadas a números locales alcanzaron un 47.7%, es decir, un aumento de 6.3% respecto al 2020.



Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal F analizado.

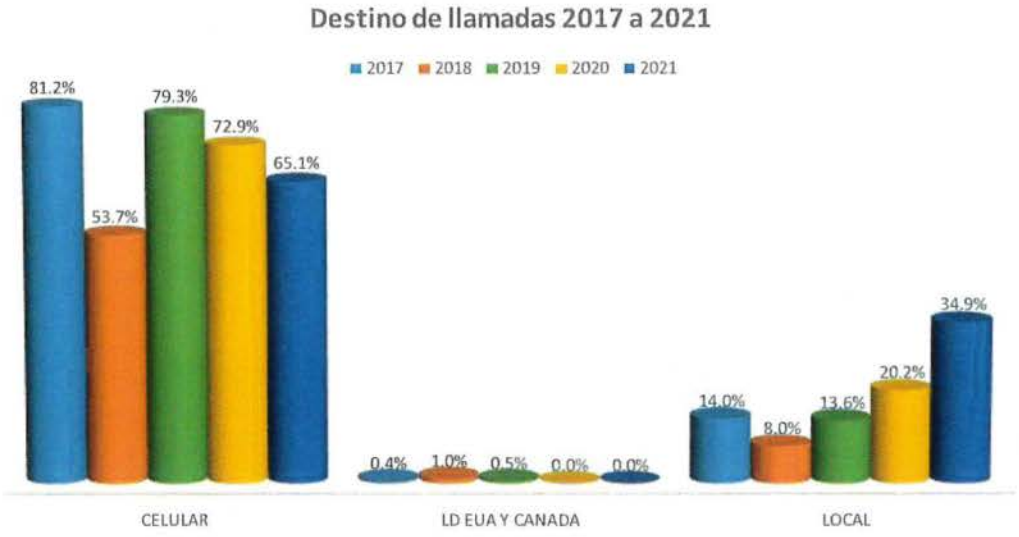
Penal 1

Solamente 84 llamadas pasaron de forma directa sin pasar por IVR; el resto de las llamadas, es decir, 2,562 llamadas pasaron por el sistema de IVR.

De las 1,694 llamadas aceptadas, cuya duración promedio fue de 1.5 minuto (similar que el año pasado), todas las llamadas se realizaron a partir de las 7:00 horas. Las llamadas rechazadas siguen un patrón similar a 2020. Se rechazaron el 82.6% de llamadas.

El 6.6% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, y tan solo un 14% tuvo una duración entre 10 y 30 segundos. El 79.4% de las llamadas aceptadas duraron más de 30 segundos.

De las llamadas generadas, el 65.1% se dirigió a teléfonos móviles, lo anterior representa una caída de 7.8 puntos porcentuales comparado contra el 2020. Las llamadas cursadas a números locales alcanzaron un 34.9%, es decir, un aumento de 14.7 puntos porcentuales respecto al 2020. Finalmente, no se realizaron llamadas de larga distancia internacional ni hubo llamadas a números especiales.



Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 1 analizado.

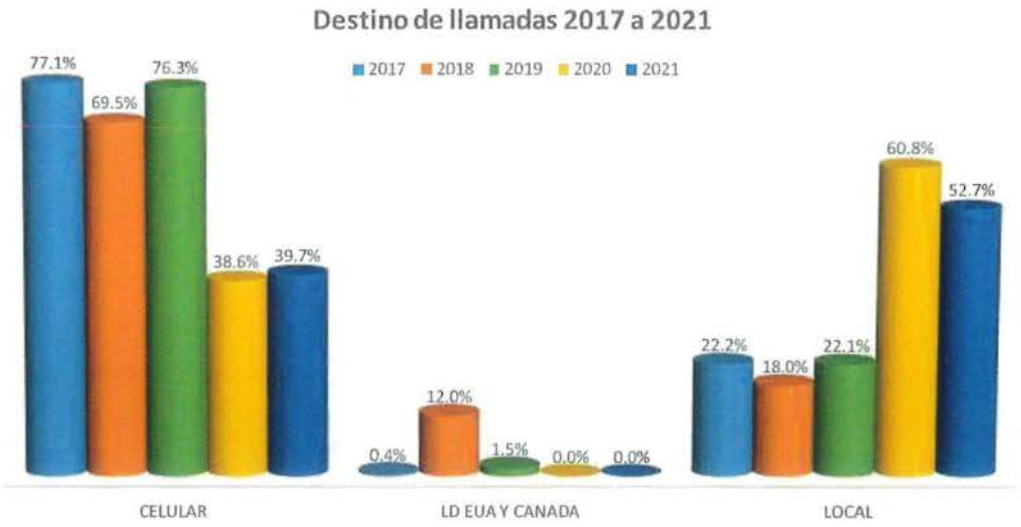
Penal 2

El 7.7% de las llamadas efectuadas pasaron de forma directa, el resto pasó por el sistema de IVR, de las cuales se registró un índice de rechazo del 11% (el segundo porcentaje más bajo de rechazo en la muestra).

De las llamadas aceptadas, cuya duración promedio fue de 3.6 minutos, el total de las llamadas se realizó entre las 7:00 y las 21:00 horas. El 98.2% de las llamadas se rechazaron.

El 5.3% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, similar respecto a 2020. Asimismo, el 12.6% de las llamadas aceptadas tuvieron una duración entre 10 y 60 segundos, lo que representa una disminución de 1.5% comparado con el año anterior.

De las llamadas generadas, el 39.7% se dirigió a teléfonos móviles, en términos generales, lo anterior representa un aumento de 1.4 puntos porcentuales comparado contra el año 2020. En cambio, las llamadas cursadas a números locales alcanzaron un 52.7%, es decir, una caída de 7.8 puntos porcentuales respecto al 2020.



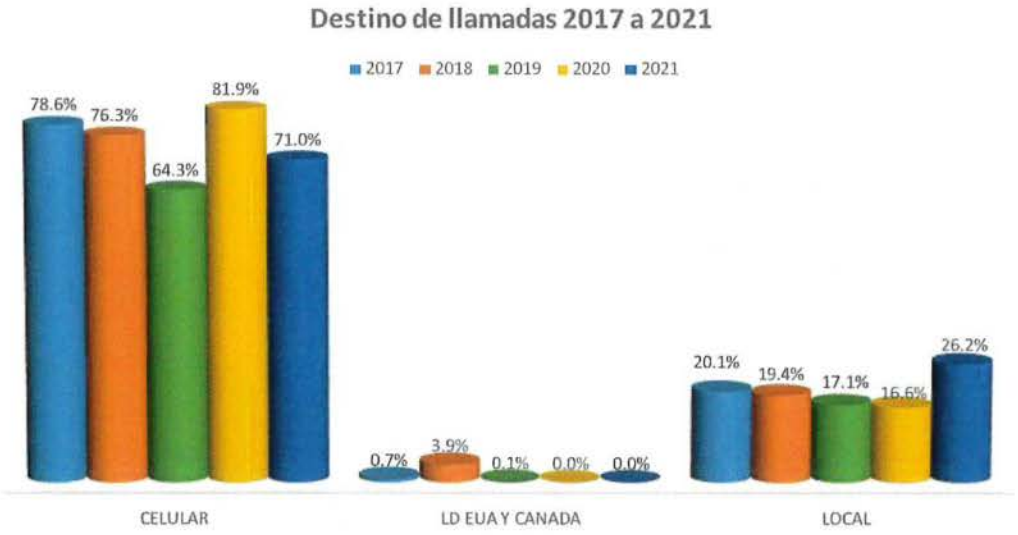
Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 2.

Penal 3

Se analizaron 1,068 llamadas; debido a que este penal no cuenta con IVR todas las llamadas son enlazadas de forma directa y no hay estadísticas de rechazo. De las llamadas realizadas, cuya duración promedio fue de 2.6 minutos (1.1 mayor que el año pasado), el total de las llamadas tuvieron lugar entre las 7:00 y las 21:00 horas.

El 53.8% de las llamadas tuvieron una duración menor a 10 segundos, cifra ligeramente menor (54.4%) que la del 2020. Asimismo, el 6.3% de las llamadas tuvieron una duración entre 10 y 60 segundos.

De las llamadas generadas, el 71% se dirigió a teléfonos móviles, lo que representa un decremento de 10.9 puntos porcentuales comparado contra el año 2020. Las llamadas cursadas a números locales alcanzaron un 26.2%, es decir, un incremento de 9.6 puntos porcentuales respecto al 2020. Finalmente, no se realizaron llamadas de larga distancia internacional y solo el 2.8% fueron a otros destinos.



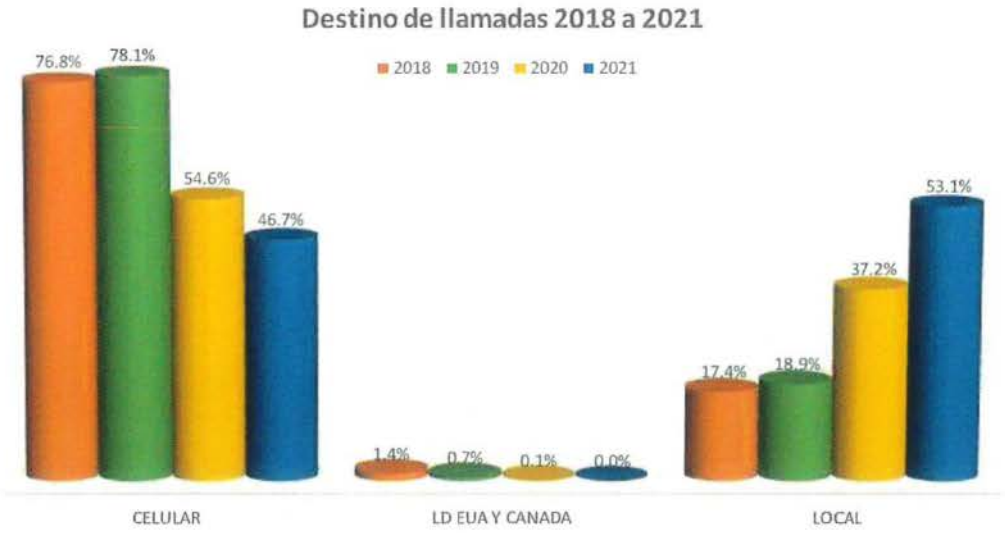
Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 3 analizado.

Penal 4

Se estudiaron 27,791 llamadas, debido a que este penal no cuenta con IVR todas las llamadas son enlazadas de forma directa y no hay estadísticas de rechazo. De las llamadas realizadas, cuya duración promedio fue de 2.1 minutos (muy similar que el año pasado), el 98% tuvieron lugar entre las 7:00 y las 21:00 horas.

El 46.5% de las llamadas tuvieron una duración menor a 10 segundos, mientras que solamente el 2.1% de las llamadas tuvieron una duración entre 10 y 30 segundos. Por lo que, el 51.5% de las llamadas realizadas duraron más de 30 segundos.

De las llamadas generadas, el 46.7% se dirigió a teléfonos móviles, lo que representa una disminución de 7.9 puntos porcentuales respecto al año 2020. Las llamadas cursadas a números locales alcanzaron un 53.1%, es decir, un incremento de 15.9 puntos porcentuales respecto al 2020, lo cual podría explicarse por el efecto de la pandemia durante 2021.



Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 4 analizado.

Implicaciones

El 49.8% de las llamadas en los recintos penitenciarios analizados que cuentan con un mensaje de prevención sobre el lugar de origen (IVR) fueron rechazadas, ello pudiera indicar que este mecanismo es un disuasivo importante; lo anterior, se refuerza al observar que dicho porcentaje aumentó 27.5 puntos porcentuales comparado respecto al año anterior.

El 8.2% de las llamadas aceptadas concluyeron en los primeros 10 segundos, lo que sugiere que la gente colgó como reacción inmediata a lo que escuchó, cabe mencionar que esta métrica aumentó 1.1 puntos porcentuales comparado con 2020.

Otro elemento de interés es que, en los 7 recintos analizados, 1 de cada 2 llamadas tuvieron como destino un equipo móvil.

También se observó que existen centros penitenciarios con un horario restringido para llamadas, a saber, entre las 7:00 y las 21:00 horas, si se consideran los centros que no cuentan con esta restricción, existe un 0.3 % de llamadas que tienen lugar fuera de dicho horario y que se podría suponer que, al llevarse a cabo fuera de la vista de todos, buscarían objetivos delictivos; cabe mencionar que dicha cifra se redujo en 6.3 puntos porcentuales respecto a 2020.

En resumen, la información que se desprende de este esfuerzo preliminar al que pudieran sumarse todas las empresas de telefonía fija, sugiere que las autoridades contarán con información complementaria a la generada por los operadores móviles que podría ser útil para sus investigaciones de combate al delito.

Nombre del estudio:

"IDENTIFICACIÓN DE APLICACIONES Y RECURSOS TECNOLÓGICOS PARA MITIGAR LA COMISIÓN DE DELITOS"

Estudio presentado por el grupo integrado por:

AXTEL, S.A.B. de C.V,
ALESTRA SERVICIOS MOVILES, S.A. de C.V,
MEGACABLE COMUNICACIONES DE MÉXICO, S.A. de C.V,
MARCATEL COM, S.A. de C.V,
COORDINADORA DE CARRIER´S, S.A. de C.V,
CABLEMÁS TELECOMUNICACIONES, S.A. de C.V,
CABLEVISIÓN RED, S.A. de C.V,
TV CABLE DE ORIENTE, S.A. de C.V,
OPERBES, S.A. de C.V,
MÉXICO RED DE TELECOMUNICACIONES, S.A. de C.V,
CABLEVISIÓN, S.A. de C.V,
TELEVISIÓN INTERNACIONAL, S.A. de C.V,
CELMAX MOVIL S.A. de C.V., y
OPENIP COMUNICACIONES, S.A. de C.V.

ESTUDIO INTITULADO "IDENTIFICACIÓN DE APLICACIONES Y RECURSOS TECNOLÓGICOS PARA MITIGAR LA COMISIÓN DE DELITOS" QUE PRESENTAN LAS EMPRESAS AXTEL, S.A.B. DE C.V., ALESTRA SERVICIOS MOVILES, S.A. DE C.V., MEGACABLE COMUNICACIONES DE MÉXICO, S.A. DE C.V., MARCATEL COM, S.A. DE C.V., COORDINADORA DE CARRIER´S, S.A. DE C.V., CABLEMÁS TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN RED, S.A. DE C.V., TV CABLE DE ORIENTE, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN, S.A. DE C.V., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., CELMAX MOVIL S.A. DE C.V. Y OPENIP COMUNICACIONES, S.A. DE C.V.

Contenido

Tablas

Ilustración

1. Introducción.

En el mundo digital en el que vivimos hoy existen múltiples elementos, los cuales se encuentran en constante cambio y evolución, nos referimos a los procesos, la tecnología y las personas. Las organizaciones en el curso diario de operación deben de ser capaces de identificar la constante necesidad de cambio al estar interactuando con estos elementos y ser capaces de identificar nuevas oportunidades de mejora y también, en términos del riesgo, que el cambio representa, tanto positiva como negativamente.

Es evidente como la pandemia aceleró la adopción de la tecnología durante los últimos 3 años y como las tendencias que emergieron a raíz de esta impulsaron la adaptación de las tácticas de ataque de los cibercriminales.

Con la consolidación del teletrabajo, las personas han pasado a ser un punto débil para la seguridad de las empresas, sin embargo, muchas de ellas ni siquiera son conscientes del riesgo que acarrean algunas prácticas rutinarias de estos. Las personas intervienen en todos los ciclos de vida de la información, desde la recopilación, el tratamiento y el almacenamiento de la misma, por lo que es importante estar concienciados de la importancia de la ciberseguridad.

2. Antecedentes.

Conforme al artículo 190 fracciones XII de la Ley Federal de Telecomunicaciones y Radiodifusión, los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

> *"XII. Realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal."*

Los concesionarios AXTEL, S.A.B. DE C.V., ALESTRA SERVICIOS MOVILES, S.A. DE C.V., MEGACABLE COMUNICACIONES DE MÉXICO, S.A. DE C.V., MARCATEL COM, S.A. DE C.V., COORDINADORA DE CARRIER´S, S.A. DE C.V., CABLEMÁS TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN RED, S.A. DE C.V., TV CABLE DE ORIENTE, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN, S.A. DE C.V., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., CELMAX MOVIL S.A. DE C.V. Y OPENIP COMUNICACIONES, S.A. DE C.V. han decidido agruparse para la contratación de un tercero al cual encomendarle la realización del siguiente estudio que ha sido aceptado por el Comité Especializado de Estudios e Investigaciones.

3. Antecedente de proyecto.

Conforme al artículo 190 fracciones XII de la Ley Federal de Telecomunicaciones y Radiodifusión, los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

> *"XII. Realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal."*

Los concesionarios AXTEL, S.A.B. DE C.V., ALESTRA SERVICIOS MOVILES, S.A. DE C.V., MEGACABLE COMUNICACIONES DE MÉXICO, S.A. DE C.V., MARCATEL COM, S.A. DE C.V., COORDINADORA DE CARRIER´S, S.A. DE C.V., CABLEMÁS TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN RED, S.A. DE C.V., TV CABLE DE ORIENTE, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., CABLEVISIÓN, S.A. DE C.V., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., CELMAX MOVIL S.A. DE C.V. Y OPENIP COMUNICACIONES, S.A. DE C.V., se presenta el Resultado de la elaboración el estudio de seguridad y colaboración con la justicia.

4. Objetivo general.

La presentación de un documento que tiene por objeto el establecimiento de recomendaciones para mitigación de amenazas mediante la identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos.

El objetivo del estudio es analizar la eficiencia del uso de herramientas tecnológicas que contribuyan a mitigar la comisión de fraudes y robo de identidad en por medio de los equipos de usuario final como por ejemplo laptops y/o desktops.

5. Objetivos del proyecto.

a) Identificación de las principales herramientas tecnológicas en equipos de usuario final que permitan detectar correos maliciosos como prevención de vectores de ataque en la comisión de fraudes o robos de identidad.
b) Identificación de las principales herramientas tecnológicas en equipos de usuario final que permitan identificar mensajes maliciosos como prevención de vectores de ataque en la comisión de fraudes o robos de identidad.
c) Identificación de las principales herramientas tecnológicas en equipos de usuario final que brinden la posibilidad de bloquear el dispositivo de usuario final.
d) Identificación de las principales herramientas tecnológicas en equipos de usuario final que proporcionen la capacidad de borrar de manera remota la información contenida en el dispositivo.
e) Mecanismos en equipos de usuario final para certificar material gráfico y direcciones de páginas web.

6. Metodología del estudio.

Para el presente estudio de medidas para la identificación de aplicaciones y recursos tecnológicos para mitigar la comisión de delitos, se realizó una investigación sobre diferentes herramientas tecnológicas.

Los controles con los que cuentan los usuarios finales de manera directa son aquellos que protegen sus dispositivos y computadoras móviles y equipos de escritorio y son conocidos tradicionalmente como antivirus tradicional, también conocido como EPP (*Endpoint Protection Platform*) así como la evolución de estos elementos de control conocidos como sistema EDR, acrónimo en inglés de Endpoint Detection Response.
Dentro de la metodología se identificarán cuáles son los sistemas EDP con mayor nivel de penetración en el mercado y se ejecutarán un grupo de pruebas para identificar y analizar la eficiencia de estos.

Ilustración 1 Metodología del estudio de recomendaciones de medidas para la concientización de usuarios.

7. Herramientas evaluadas

Un sistema EDR, es un sistema de protección de los equipos e infraestructuras de la empresa hacia los usuarios finales. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

Los antivirus NGAV acrónimo en ingles de *Next Generation Antivirus* utilizan la inteligencia artificial y el machine learning para aprender y analizar a partir de miles de datos los patrones de comportamiento de las nuevas amenazas, pudiendo incluso descubrir nuevas tácticas de los ciberdelincuentes. Además, están conectados permanentemente a un sistema cloud (en la nube), por lo que la actualización es constante.

Gracias a esta conjunción de elementos y tecnologías es posible detectar todos aquellos riesgos y amenazas que pueden provocar de forma silenciosa e inadvertida un incidente de seguridad, poniendo en riesgo la viabilidad de la empresa.

7.1. Características de un Sistema EDR[1] y NGAV

Un sistema EDR y NGAV se caracterizan por aunar varios elementos de detección y de tecnologías, por ejemplo, la inteligencia artificial y el Big Data, que permiten mejorar de forma programada y autónoma la detección y prevención de amenazas complejas, así como su posterior eliminación o mitigación.

Aunque comparte cometidos con el antivirus tradicional, también conocido como EPP (Endpoint Protection Platform), como son la detección, identificación y la prevención de los efectos de malware, exploits, y en algunos casos, ransomware, esta herramienta además puede detectar amenazas avanzadas, como pueden ser malware de tipo polimórfico, vulnerabilidades 0-day, ataques de ingeniería social, amenazas persistentes o APT, cuentas comprometidas, etc. En caso de detectar una amenaza o comportamiento anómalo, permite actuar de forma inmediata y casi automática para poder eliminar la amenaza o mitigar sus efectos.

Entre las aplicaciones y herramientas que incorpora, además del antivirus tradicional destacan:

- Herramientas de análisis apoyadas en el uso del aprendizaje automático (machine learning) para mejorar la detección de amenazas.
- Sandbox: el sistema virtual y aislado de pruebas para comprobar el comportamiento de los archivos descargados, por ejemplo.
- Escaneo de identificadores de compromiso (IOC) y reglas YARA[2], que permiten analizar y detectar las amenazas provocadas por amenazas complejas en tiempo real.
- El uso de listas blancas y negras de correos electrónicos, páginas web e IP.
- Interoperatibilidad e interacción con otras herramientas de seguridad, como SIEM, IPS/IDS o herramientas antimalware.

Los principales fabricantes del mercado de soluciones de seguridad ofrecen este tipo de sistemas en su portafolio de aplicaciones. En el caso de que una empresa no cuente con técnicos o con un Departamento de Informática, siempre tiene la posibilidad de subcontratar este servicio a un proveedor o contratar el servicio completo con el fabricante.

---

[1] INCIBE: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

[2] YARA: Herramienta de código abierto que fue desarrollada por la plataforma VirusTotal para identificar los elementos de un *malware* por medio de un análisis estático automatizado

7.2. Ventajas e inconvenientes de un Sistema EDR y NGAV

Esta herramienta contiene una serie de ventajas y fortalezas frente a los antivirus tradicionales o EPP, por ejemplo:

- Recopila información exhaustiva y detallada de las características del dispositivo, como información del sistema operativo, del hardware o los procesos activos, entre otros datos.
- Permite recopilar y almacenar información de forma automática, así como crear patrones de detección automatizados, facilitando el trabajo de detección.
- Monitoriza la integridad de los sistemas y de los archivos de configuración claves, avisando en caso de modificación o acceso a los mismos por actores sospechosos.
- Permite localizar en un solo punto toda la información, posibilitando en caso de incidente, la realización de una investigación de forma rápida.

Por el contrario, esta herramienta muestra las siguientes debilidades:

- En algunos casos no permite evaluar y comprobar aquellos dispositivos con sistemas operativos no soportados por la herramienta.
- Su configuración y puesta en marcha es más complicada de realizar que en el caso de un antivirus tradicional.
- Su uso puede provocar perdida de eficiencia, debido al constante flujo de información y notificación de las propias alertas configuradas, así como de los falsos positivos y negativos que puedan darse.
- En ocasiones no permite monitorizar y analizar las conexiones cifradas.
- La inversión para implantar esta herramienta supone un importe más elevado que en el caso del antivirus tradicional o EPP.

7.3. Diferencias entre un Sistema EPP y un Sistema EDR y NGAV

Respecto a los antivirus tradicionales, aunque han evolucionado de forma considerable en los últimos años, solo se localizan amenazas de *malware* tradicional, es decir, virus, troyanos y gusanos. Son ineficaces ante la detección de ataques más complejos, en los que se mezclan la ingeniería social junto con los fallos humanos de los empleados, así como las técnicas más complejas (vulnerabilidades *0-day*, *ransomware*, cuentas comprometidas, amenazas persistentes, entre otras.) en las redes de la empresa, lo que puede provocar que sean más difíciles de detectar y controlar, con los consecuentes daños económicos y reputacionales para la empresa.

En definitiva, usar este tipo de herramientas, aunque puede suponer un gasto inicial más elevado, ofrece una serie de ventajas que permiten amortizar dicha inversión rápidamente gracias a sus características y tecnologías incorporadas, reduciendo así ostensiblemente los efectos perniciosos de ataques más sofisticados contra la información personal, así como contra las infraestructuras digitales de las empresas.

8. Panorama actual en materia de Sistemas EDR y NGAV

El mercado de Soluciones de detección y respuesta de punto final (EDR) y Antivirus de nueva Generación (NGAV) [3] se define como soluciones que registran y almacenan comportamientos a nivel de sistema de punto final, utilizan varias técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, brindan información contextual, bloquean actividades maliciosas y brindan sugerencias de

remediación para restaurar sistemas afectados. Las soluciones de EDR deben proporcionar las siguientes cuatro capacidades principales:

- Detectar incidentes de seguridad
- Contener el incidente en el punto final
- Investigar incidentes de seguridad
- Proporcionar orientación para la corrección

Se toma como base para la identificación de las herramientas en el mercado al cuadrante mágico de Gartner. Gartner Inc., es una empresa consultora y de investigación de las tecnologías de la información, está considerada una de las empresas consultoras y de investigación de las tecnologías de la información más importantes a nivel mundial. Se dedica de forma exclusiva a investigar y analizar las tendencias del mercado. Cada año se publica el Cuadrante Mágico de Gartner, que incluye las empresas TIC más relevantes a nivel internacional.

Para formar parte de él, las empresas tienen que pasar un proceso de selección muy riguroso. Estar en el Cuadrante Mágico garantiza la alta calidad de los servicios ofrecidos en materia tecnológica y un amplio conocimiento de las necesidades reales del mercado.

El Cuadrante Mágico es una culminación de la investigación en un mercado específico que brinda una visión panorámica de las posiciones relativas de los actores del mercado a través de un ranking de proveedores con las mejores soluciones y productos. Esta calificación se construye mediante las opiniones de los clientes en cuanto a los servicios ofrecidos por los proveedores.

El método utilizado por Gartner para presentar sus resultados en el Cuadrante Mágico se realiza a través de un gráfico de dos ejes:

El vertical se refiere al conocimiento de mercado mientras que el horizontal indica la habilidad de ejecución. En ellos, se posicionan los cuatro tipos de proveedores de tecnología, según sus capacidades:

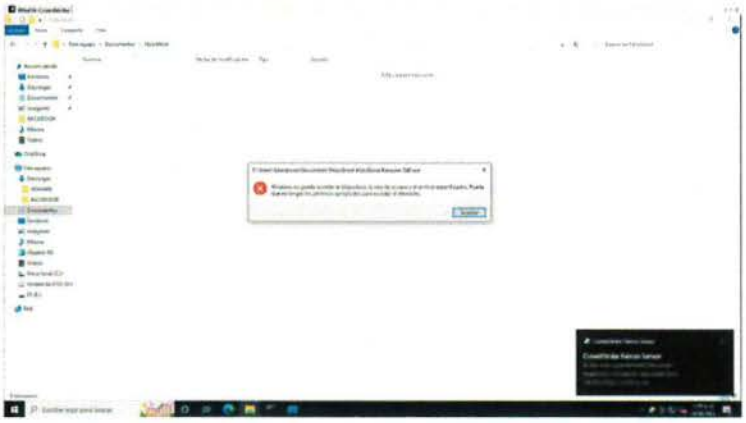
1. Los Visionarios, están relacionados con la capacidad de innovación técnica que aportan a sus clientes.
2. Los Retadores y Líderes, destacan por su capacidad de gestionar un alto número de usuarios para grandes cuentas con escala de servicio y costes. Cuentan con una oferta madura y centralizada sin soluciones personalizadas.
3. Los Proveedores de nicho buscan ofrecer una mayor calidad en el servicio y tienen una mayor flexibilidad para adaptarse a las necesidades concretas de cada negocio. Se caracterizan por una alta orientación al usuario, contacto local, alcance y recursos en cada territorio donde ofrece servicio.

[3] NGAV: Que es un Antivirus de nueva Generación NGAV
https://www.sophos.com/en-us/content/what-is-ngav

CONEXIONES A INTERNET

NA

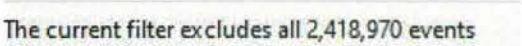
CAPTURA DE PANTALLA:



15.8. McAfee Backdoor

INFORMACIÓN GENERAL:

Durante la ejecución de los backdoor no lograron ejecutarse, dado que MCAFFEE los bloqueaba.



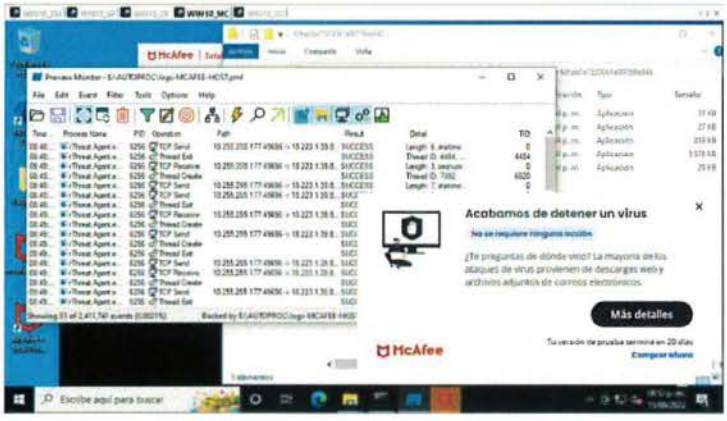
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.9. McAfee Adware

INFORMACIÓN GENERAL:

15.5. Crowdstrike Virus

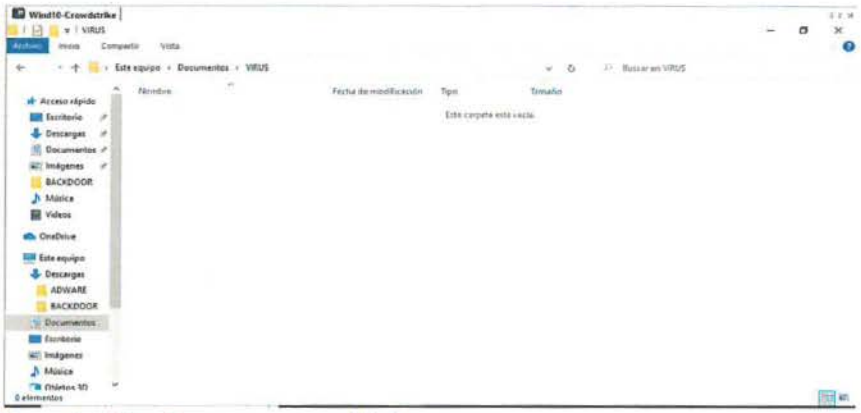
INFORMACIÓN GENERAL:

El malware fue eliminado al ser escrito en disco, por lo que no puede ejecutarse

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.6. Crowdstrike Ransomware Nokoyawa

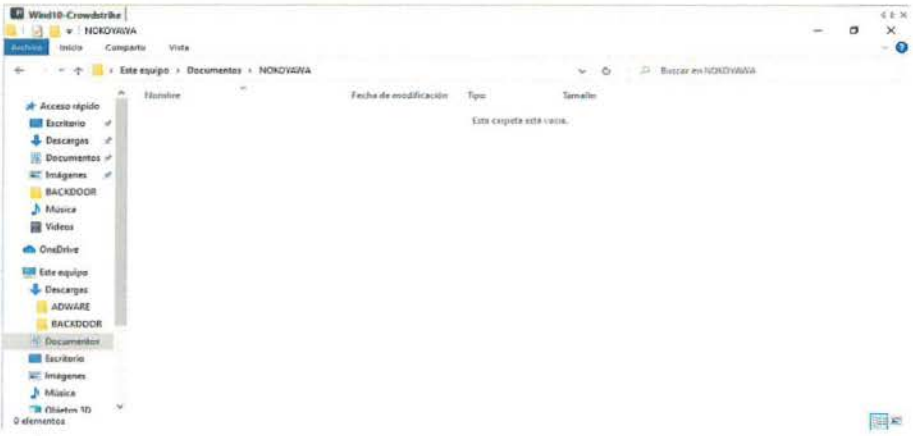
INFORMACIÓN GENERAL:

El malware fue eliminado al ser escrito en disco, por lo que no puede ejecutarse

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



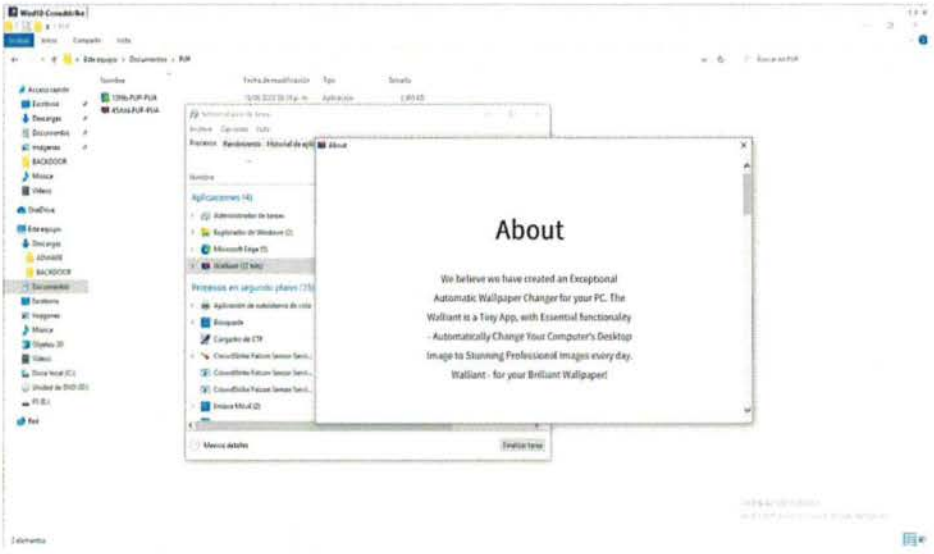
15.7. Crowdstrike Ransomware Ghost

INFORMACIÓN GENERAL:

El malware fue eliminado al momento de la ejecución, como se observa en la imagen

Process Name	PID	CPU	File Events	Registry Events	Network Events
HolyGhost.Ransom.Obf.exe	2372	0	27	0	0

ÁRBOL DE PROCESOS:



15.4. Crowdstrike Trojan

INFORMACIÓN GENERAL:

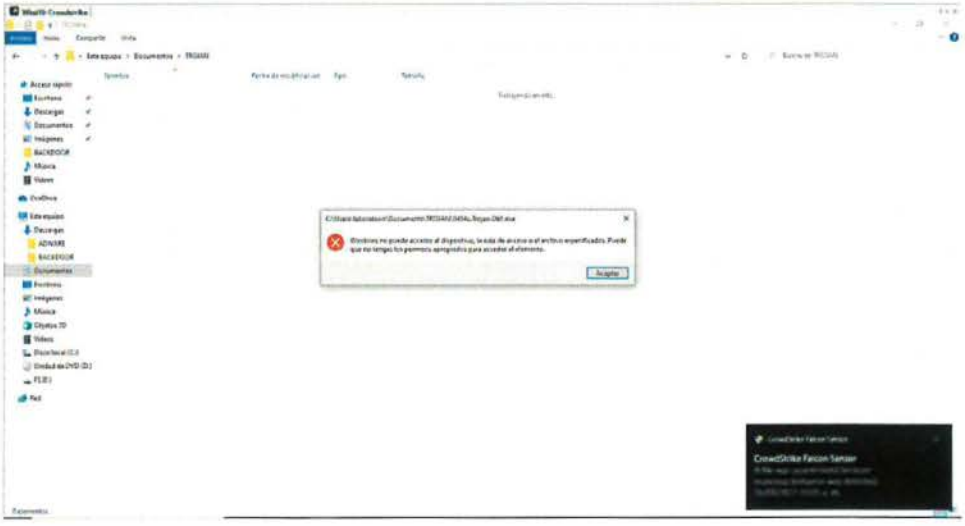
Process Name	PID	CPU	File Events	Registry Events	Network Events
0454c.Trojan.Obf.exe	8132	0	31	0	0

ÁRBOL DE PROCESOS:

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.3. Crowdstrike PUP

INFORMACION GENERAL:

12f6b.PUP-PUA.exe

Es detenido durante la ejecución por Crowdstrike

45ddd.PUP-PUA.exe

Logra instalarse sin ser detenido

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
walliant.exe	7604	2.59375	6,347	19,501	72
45ddd.PUP-PUA.tmp	7232	2.15625	3,247	11,430	20

ARBOL DE PROCESOS:

CONEXIONES A INTERNET

Total Events	Send Bytes	Receive Bytes	Path	No. de Flags maliciosas
14	483	3,486	104.16.124.96:https	0
37	1,906	8,478	104.21.57.77:https	0
34	4,949	4,608	172.67.223.121:https	0
7	472	1,478	72.21.91.29:http	0

CAPTURA DE PANTALLA:

15. Anexo A: Evidencia Resultados Herramientas

15.1. Crowdstrike BACKDOOR

ÁRBOL DE EJECUCIÓN:

El malware fue eliminado al ser escrito en disco, por lo que no puede ejecutarse.

CONEXIONES A INTERNET

NA

RESULTADOS DE FICHEROS ESCRITOS EN EL DISCO:

15.2. Crowdstrike ADWARE

INFORMACIÓN GENERAL:

Todos los procesos fueron cortados por Crowdstrike al momento de la ejecución.

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
62043.Adware.Obf.exe	3104	0	31	0	0

ÁRBOL DE PROCESOS:

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:

14. Bibliografía

A continuación, un listado de las referencias de documentos utilizados para la elaboración del presente estudio:

1. Sistemas EDR: Qué son u como ayudan a proteger la seguridad de tu empresa (27/04/2021) https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa
2. YARA: Herramienta de código abierto que fue desarrollada por la plataforma VirusTotal para identificar los elementos de un *malware* por medio de un análisis estático automatizado https://support.virustotal.com/hc/en-us/articles/115002178945-YARA
3. NGAV: Que es un Antivirus de nueva Generación NGAV https://www.sophos.com/en-us/content/what-is-ngav
4. Gartner Peer Insigths: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions
5. Crowdstrike: Software empresarial con licenciamiento EDR y NGAV con las políticas mas agresivas https://www.crowdstrike.com/latam/
6. McAfee: Software de grado "Home" con todas las políticas de seguridad activadas. https://www.mcafee.com/es-mx/index.html
7. Microsoft Defender: Software con licenciamiento empresarial. https://www.microsoft.com/es-mx/microsoft-365/microsoft-defender-for-individuals
8. Sentinel One: Software empresarial con licenciamiento EDR y NGAV con las políticas más agresivas. https://www.sentinelone.com/
9. Sophos: Software EDR empresarial. https://www.sophos.com/es-es
10. Trend Micro: Software con licenciamiento empresarial. https://www.trendmicro.com/es_mx/about.html
11. Troyanos: Kaspersky: https://encyclopedia.kaspersky.es/knowledge/trojans/
12. Backdoor: Kaspersky: https://encyclopedia.kaspersky.es/knowledge/backdoor/
13. Ransomware: Kaspersky: https://encyclopedia.kaspersky.es/knowledge/trojan-ransom/
14. PUP-PUA: Kaspersky:https://encyclopedia.kaspersky.es/knowledge/adware-pornware-and-riskware/
15. Adware: Kaspersky: https://encyclopedia.kaspersky.es/knowledge/adware/
16. Virus: Kaspersky: https://encyclopedia.kaspersky.es/knowledge/viruses-and-worms/

Control: El medio de gestionar el riesgo, que incluye políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

Detección de intrusos: El proceso de monitorear los eventos que ocurren en un sistema o red informático para detectar señales de accesos no autorizados o ataques.

Impacto: El efecto neto positivo o negativo, del logro de los objetivos de negocio.

Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que ocasiona o puede ocasionar, una interrupción o una reducción en la calidad del servicio.

IDS: Sistema para de detección de intrusiones no autorizadas a una red.

Incidente de seguridad de información: todo evento que ocasione pérdida parcial o total de información, interrupción en los sistemas de procesamiento y almacenamiento de información, intrusiones lógicas o físicas no autorizadas que atenten contras las políticas de seguridad de información.

Ingeniería social: Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Integridad: La precisión de integridad y validez de la información.

IPS: Sistema de prevención de intrusiones a la red.

Listas blancas de aplicaciones: Es una lista o registro de aplicaciones permitidas que pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento.

Políticas: Declaraciones de alto nivel sobre la intención y la dirección de la gerencia.

Procedimientos: Un documento que contiene una descripción detallada de los pasos necesarios para realizar operaciones especificas conforme a las normas aplicables. Los procedimientos se definen como parte de los procesos.

Riesgo: La combinación de la probabilidad de un evento y sus consecuencias. El riesgo tradicionalmente se expresa como Amenazas por Vulnerabilidades es igual al riesgo.

Seguridad de Información: Garantiza que solo los usuarios autorizados (confidencialidad) puedan tener acceso a la información precisa y completa (integridad) cuando sea necesario (disponibilidad).

SIEM: Sistema de gestión de eventos de seguridad.

Software: software de aplicación, software del sistema y utilidades.

Vulnerabilidad: Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

Con base en las conclusiones del estudio se establecen las siguientes recomendaciones hacia los usuarios finales:

1. Contar con antimalware que incorporen funcionalidades de EDR y NGAV donde se utilice inteligencia artificial y aprendizaje de máquina para aprender y analizar los patrones de comportamiento tanto de los usuarios como de las nuevas amenazas.
2. Habilitar escaneo en tiempo real, o dejar programado actividades de escaneo en un periodo no mayor a una semana.
3. Habilitar configuración de bloqueo y pregunta de conectividad reputacionales, hacia aplicaciones y navegación en pagina web.
4. No se recomienda el uso de antimalware de uso libre, por la cantidad de noticias que se han liberado por el mal uso de las mismas por las empresas, como el uso de datos para fines de marketing.

13. Glosario y Términos

Para la siguiente información de términos y definiciones se han utilizado principalmente fuentes de internet como el glosario de términos de ciberseguridad de INCIBE (Incibe, 2017) y otras fuentes de referencia previamente mencionadas en el presente documento.

Activo: Cualquier información y/o componente relacionado tales como los dispositivos en los que se almacena, procesan o realiza cualquier otro tratamiento, que tienen valor para la organización y que por lo tanto requieren protección.

Alerta: El análisis automatizado de eventos correlacionados y producción de alertas, para notificar a los destinatarios sobre problemas inmediatos.

Amenaza: Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano, etc.) que es capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado (ISO/IEC 13335).

Antivirus: Un software de aplicación implementado en múltiples puntos en una arquitectura de TI. Está diseñado para detectar y eliminar potencialmente el código de virus antes de que ocurra un daño y reparar o colocar en cuarentena los archivos que ya están infectados.

Arquitectura: Descripción del diseño subyacente fundamental de los componentes del sistema de negocios, o de uno de los elementos del sistema empresarial (ej., la tecnología), las relaciones entre ellos y la manera en la que apoyan los objetivos de los operadores de telecomunicaciones.

Cibercriminales: Persona(s) que se valen de internet para cometer delitos de índole diversa.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

Cifrado de información: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.

12. Recomendaciones

Con base en las conclusiones del estudio se establecen las siguientes recomendaciones hacia los empresas:

1. Establecer una política de antimalware donde se identifique la implementación, activación, actualización, operación y gestión de soluciones antimalware en los componentes de usuario Final.
2. Contar con antimalware que incorporen funcionalidades de EDR y NGAV donde se utilice inteligencia artificial y aprendizaje de máquina para aprender y analizar los patrones de comportamiento tanto de los usuarios como de las nuevas amenazas.
3. Habilitar escaneo en tiempo real, o dejar programado actividades de escaneo en un periodo no mayor a una semana.
4. Contar con alertamiento del comportamiento anómalo de los clientes de EDR y NGVA, como desconexión o perdida de sincronización, ya que puede ser indicio de un ataque más elaborado.
5. Establecer antimalware de tráfico red que soporte y apoye a los antimalware de equipos de usuario final.
6. Contar con protocolos de atención de malware y revisarlos periódicamente al menos una vez al año.
7. Analizar de manera activa todo archivo a respaldar o almacenar, incluso previo al cifrado.
8. Analizar de manera activa todo correo que ingrese a los servidores o servicios de correo.
9. Establecer medidas de concientización que sensibilicen a los usuarios en el comportamiento de un malware, su detección, reporte y acciones.
10. Es altamente recomendable no depender solamente de los controles de punto final, por los resultados encontrados, por lo que se debe realizar labores de mejora continua en:
    a. Buenas prácticas en configuraciones.
        i. La organización CIS libera de forma periódica recomendaciones y buenas practica para implementar de forma más ágil y rápida configuraciones ideales según la función del equipo:
        ii. https://www.cisecurity.org/cis-benchmarks
    b. Control de identidades.
        i. Se debe limitar bajo esquemas de confianza cero los accesos, así como los permisos en cada equipo, para ello se debe llevar un correcto manejo bajo sistemas de directorio activo, o controles complementarios del tipo PAM (Gestión del acceso con privilegios)
    c. Control de la red:
        i. Se debe limitar el acceso de equipos a nivel local, mediante segmentación de redes por medio de equipos como Firewall.

11. Los beneficios que representan los EDR y NGAV son:
    - Detectar incidentes de seguridad
    - Contener el incidente en el punto final
    - Investigar incidentes de seguridad
    - Proporcionar orientación para la corrección.

- Por lo que recomendamos a los usuarios que realicen trabajos alrededor de los sistemas Linux, como realizar buenas practicas en configuraciones, control de identidades, y limitar el acceso a nivel red de los equipos.

GENERALES:

- De las herramientas evaluados en el cuadrante de líderes de Gartner el 83 % (5 de 6) permitieron que software malicioso interactuara con los sistemas.
- Los tipos de malware que lograron interactuar con los sistemas fueron:
    1. PUP
    2. Virus /gusano
    3. Adware
    4. Troyano

CROWDSTRIKE:

- Logró tener un excelente desempeño con las pruebas, en los ámbitos de seguridad en EPP y seguridad en EDR, dejando escribir en disco poca cantidad de malware, permitiendo solo la ejecución de software PUP.

MCAFFE:

- Su desempeño fue bueno, aunque no detuvo de forma tan rápida como sus competidores el malware del tipo PUP, troyano y adware.

Microsoft Defender:

- Desempeño bueno, le afecta mucho el exceptuar procesos, dado que llega a permitir procesos de alto impacto como Ransomware cuando es un proceso fijo de una excepción.

SENTINEL ONE:

- Su desempeño se divide en dos partes, con excepciones y sin excepciones, dado que sin excepciones se encontró que logro detener gran parte del malware, pero en pruebas con excepciones la herramienta deja de monitorear a los procesos hijo de la excepción, abriendo un hueco de seguridad importante.

SOPHOS:

- Desempeño excelente, no permitió ninguna ejecución de malware, el único punto de mejora es el vector de EPP.

TRENDMICRO:

- Desempeño muy bueno, permitió poca cantidad de malware, uno de los pocos puntos a mejorar es el escaneo del EPP por dejar escribir en mayor parte al malware en disco.

Comparativa con otros estudios comerciales:

EVALUACIONES A SOLUCIONES EMPRESARIALES:

En la actualidad las evaluaciones de antimalware no entregan reportes detallados, entregan reportes generales de la eficiencia de diferentes marcas de controles empresariales:

https://selabs.uk/reports/enterprise-advanced-security-edr-2022-q2-detection/

EVALUACIONES A SOLUCIONES NO EMPRESARIALES:

Las evaluaciones de misma forma para soluciones abiertas al publico general no aparece información específica, solo resultados generales, uno de los más conocidos es:

https://www.av-test.org/es/antivirus/usuarios-finales-windows/

Lista de malware utilizado en pruebas dinámicas		
Nombre de malware	**Familia**	**HashSHA 256**
BLUESHELL	Backdoor	68ADB6D033C764B04FEADA6F2242AAB0D6DDA2C589F723EA742C4FB99E65EA28
CONTI	Ransomware	9DF50122830F7C2265024013F2A2BADF53E5F6DBC5C7A5974C110A2E3CA41AED
KSMDR	Miner	B7A3C891E6F280FE93E5F6967FFCE01E8954E93E85E5AF02DC682DF94106D80D
reverse_meterpreter_https	Backdoor / Metasploit	13989819D470301939817F68212A69E5BE78181400C2E3D14C4D40D2A19021A0
reverse_meterpreter_tcp	Backdoor / Metasploit	55DD00FAAA4DBAE6B0DA31A8C72B407A63A2DEA98ED639EA10615BCD766CA599
reverse_nc.sh	Backdoor / LivingOfTheLand	394EC690C22BEF056EDE42DE031A953077AD0FBA0D0FD0D6459F99C52FAD0BA9

Tabla 23 Hash de Malware utilizado en las pruebas con los sistemas Fedora

RESUMEN DE MALWARE QUE LOGRÓ INTERACTUAR CON LOS SISTEMAS:

	BLUESHELL		CONTI		M HTTPS		MET TCP		NC NO SSL		KSMDR		Totales	
Hostname	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**
SENTINEL ONE FEDORA	1	1	1	1	1	1	1	1	1	1	1	1	6	6
DEFENDER FEDORA	1	1	1	1	1	1	1	1	1	1	1	1	6	6
SOPHOS FEDORA	1	1	1	1	1	1	1	1	1	1	1	1	6	6
MCAFFE FEDORA	1	1	1	1	1	1	1	1	1	1	1	1	6	6

Tabla 24 Resumen de Malware que logro interactuar con los sistemas Fedora

TERMINOLOGIA:	
Logró escribirse	WR
Logró ejecutarse	EXEC
Success	1
Fail	0

Tabla 25Terminología tabla 24

11. Conclusiones

MITIGACION DE DELITOS CON HERRAMIENTAS DE PUNTOS FINAL:

- En la actualidad los controles de tipo antimalware se han convertido en la forma de menor costo y accesible para todo tipo de usuarios y empresas, dado que otros tipos de controles como los de email, firewall, entre otros, son controles que tienen costos mayores y pueden limitar el nivel de madurez en ciberseguridad de las empresas.
- Por lo que este tipo de controles de punto final son el ultimo punto de defensa para prevenir que los delincuentes efectúen robo, suplantación y modificación de nuestros datos.

PUNTOS DE MEJORA EN MITIGACION DE DELITOS:

- Los controles han demostrado que en sistemas operativos Windows ya cuentan con un gran y robusto sistema de monitoreo de comportamiento malicioso, pero en sistemas Linux aun necesitan desarrollarse, por la cantidad de malware que lograron ejecutarse en los equipos.

RESUMEN DE MALWARE QUE LOGRÓ INTERACTUAR CON LOS SISTEMAS:

	BLUESHELL		CONTI		M HTTPS		MET TCP		NC NO SSL		KMSDR		Totales	
Hostname	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**	**WR**	**EXEC**
CROWDSTRIKE UBUNTU	1	0	1	0	1	0	1	0	1	1	0	0	5	1
SENTINEL ONE UBUNTU	1	1	1	1	1	1	1	1	1	1	1	1	6	6
DEFENDER UBUNTU	1	1	1	1	1	1	1	1	1	1	1	1	6	6
SOPHOS UBUNTU	1	1	1	1	1	1	1	1	1	1	1	1	6	6
MCAFFE UBUNTU	1	1	1	1	1	1	1	1	1	1	1	1	6	6

Tabla 20 Resumen de Malware que logro interactuar con los sistemas Ubuntu

TERMINOLOGIA:	
Logró escribirse	WR
Logró ejecutarse	EXEC
Success	1
Fail	0

Tabla 21Terminología tabla 20

10.4. Resultado de Pruebas sobre imagen Fedora

PRIMERA FASE (ENVÍO DE MALWARE):

2. Validar si llegó integro el fichero después de 15 segundos.

SEGUNDA FASE (EJECUCIÓN):

3. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo o tener interacción (lectura, escritura, o modificación de registros, así como la ejecución de procesos) con el sistema.
4. Análisis de comportamiento del malware en la máquina.

CONSIDERACIONES DE LOS RESULTADOS:

1. Validar si llegó integro el fichero después de 15 segundos.
2. Validar si después de 15 segundos no se borra de una carpeta sin excepciones
3. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo. (En algunas capturas veremos un fichero llamado autoruns.exe este es un fichero no malicioso enviado para validación).

MALWARE UTILIZADO EN LAS PRUEBAS CON LOS SISTEMAS:

Lista de malware utilizado en pruebas dinámicas		
Nombre de malware	**Familia**	**Descripción**
BLUESHELL	Backdoor	Encontrado en internet y ofuscado en secnesys
CONTI	Ransomware	Encontrado en internet y ofuscado en secnesys
KSMDR	Miner	Encontrado en internet y ofuscado en secnesys
reverse_meterpreter_https	Backdoor / Metasploit	Compilado y ofuscado en secnesys
reverse_meterpreter_tcp	Backdoor / Metasploit	Compilado y ofuscado en secnesys
reverse_nc.sh	Backdoor / LivingOfTheLand	Creado sin ofuscación en secnesys

Tabla 22 Malware utilizado en las pruebas con los sistemas Fedora

10.3. Resultado de Pruebas sobre imagen Ubuntu

PRIMERA FASE (ENVÍO DE MALWARE):

1. Validar si llegó integro el fichero después de 15 segundos.

SEGUNDA FASE (EJECUCIÓN):

1. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo o tener interacción (lectura, escritura, o modificación de registros, así como la ejecución de procesos) con el sistema.
2. Análisis de comportamiento del malware en la máquina.

CONSIDERACIONES DE LOS RESULTADOS:

1. Validar si llegó integro el fichero después de 15 segundos.
2. Validar si después de 15 segundos no se borra de una carpeta sin excepciones
3. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo.
    1. En algunas capturas veremos un fichero llamado autoruns.exe este es un fichero no malicioso enviado para validación.

MALWARE UTILIZADO EN LAS PRUEBAS CON LOS SISTEMAS:

Lista de malware utilizado en pruebas dinámicas		
Nombre de malware	**Familia**	**Descripción**
BLUESHELL	Backdoor	Encontrado en internet y ofuscado en secnesys
CONTI	Ransomware	Encontrado en internet y ofuscado en secnesys
KSMDR	Miner	Encontrado en internet y ofuscado en secnesys
reverse_meterpreter_https	Backdoor / Metasploit	Compilado y ofuscado en secnesys
reverse_meterpreter_tcp	Backdoor / Metasploit	Compilado y ofuscado en secnesys
reverse_nc.sh	Backdoor / LivingOfTheLand	Creado sin ofuscación en secnesys

Tabla 18 Malware Utilizado en las pruebas con los sistemas UBUNTU

Lista de malware utilizado en pruebas dinámicas		
Nombre de malware	**Familia**	**Hash SHA 256**
BLUESHELL	Backdoor	68ADB6D033C764B04FEADA6F2242AAB0D6DDA2C589F723EA742C4FB99E65EA28
CONTI	Ransomware	9DF50122830F7C2265024013F2A2BADF53E5F6DBC5C7A5974C110A2E3CA41AED
KSMDR	Miner	B7A3C891E6F280FE93E5F6967FFCE01E8954E93E85E5AF02DC682DF94106D80D
reverse_meterpreter_https	Backdoor / Metasploit	13989819D470301939817F68212A69E5BE78181400C2E3D14C4D40D2A19021A0
reverse_meterpreter_tcp	Backdoor / Metasploit	55DD00FAAA4DBAE6B0DA31A8C72B407A63A2DEA98ED639EA10615BCD766CA599
reverse_nc.sh	Backdoor / LivingOfTheLand	394EC690C22BEF056EDE42DE031A953077AD0FBA0D0FD0D6459F99C52FAD0BA9

Tabla 19 Hash de Malware Utilizado en las pruebas con los sistemas UBUNTU

- Los PUP logran instalar paquetes, hacer conexiones hacia IP externas o escribir archivos temporales.

10.2.4. Resultado de Pruebas sobre imagen Windows 11: Sentinel One

	Backdoor:	Troyanos:	Ransom:	PUP:	Adware:	Virus:
SENTINEL ONE	3	1	1	2	4	2

Tabla 15 Resultado de Pruebas sobre imagen Windows 11: Sentinel One

Comentarios:

- Backdoors logran escribir registros y hacer comunicaciones a IP externas, si bien no todas están catalogadas como maliciosas, los artefactos son bien catalogados como maliciosos.
- El ransomware Nokoyawa logra cifrar archivos del dispositivo, sin posibilidad de restaurar.

10.2.5. Resultado de Pruebas sobre imagen Windows 11: Sophos

	Backdoor:	Troyano:	Ransom:	PUP:	Adware:	Virus:
SOPHOS	0	0	0	0	0	0

Tabla 16 Resultado de Pruebas sobre imagen Windows 11: Sophos

Comentarios:

- Sophos presentó consistencia en su manera de analizar las amenazas, si bien todos los artefactos son permitidos en disco, su capacidad de detener amenazas al momento de ejecutarse se ve muy acertada.

10.2.6. Resultado de Pruebas sobre imagen Windows 11: TrendMicro

	Backdoor:	Troyano:	Ransom:	PUP:	Adware:	Virus:
TRENDMICRO	0	0	0	1	2	0

Tabla 17 Resultado de Pruebas sobre imagen Windows 11: TrendMicro

Comentarios:

- En este caso el PUP logró hacer conexiones hacia IP externas y posteriormente detuvo los procesos orígenes.
- El adware logró escribir archivos temporales que posteriormente pueden ser ejecutados para continuar un ataque.

Microsoft Defender	0	0	1	3	2	3
SENTINEL ONE	3	1	1	2	4	2
SOPHOS	0	0	0	0	0	0
TRENDMICRO	0	0	0	1	2	0

Tabla 11 Resultado de Pruebas sobre imagen Windows 11

10.2.1. Resultado de Pruebas sobre imagen Windows 11: Crowdstrike

	Backdoor:	Troyanos:	Ransom:	PUP:	Adware:	Virus:
CROWDSTRIKE	0	0	0	2	0	0

Tabla 12 Resultado de Pruebas sobre imagen Windows 11: Crowdstrike

Comentarios:

- 1 PUP (Programa potencialmente no deseado por sus siglas en inglés) logró instalar 2 paquetes en el equipo.
- 1 PUP logró hacer peticiones y recibir información a través de internet.

10.2.2. Resultado de Pruebas sobre imagen Windows 11: McAfee

	Backdoor:	Troyanos:	Ransom:	PUP:	Adware:	Virus:
McAfee	2	0	0	1	0	0

Tabla 13 Resultado de Pruebas sobre imagen Windows 11: McAfee

Comentarios:

- Similar a otra tecnología, los artefactos Backdoor logran enviar y recibir información desde IP externas algunas catalogadas como maliciosas.
- Un Software potencialmente no deseado (PUP) logra hacer peticiones hacia un par de direcciones externas sin ser detenidas por la herramienta.

10.2.3. Resultado de Pruebas sobre imagen Windows 11: Windows Defender

	Backdoor:	Troyanos:	Ransom:	PUP:	Adware:	Virus:
Windows Defender	0	0	1	3	2	3

Tabla 14 Resultado de Pruebas sobre imagen Windows 11: Windows Defender

Comentarios:

- El ransomware nokoyawa logro cifrar archivos dentro de este HOST.

Comentaros segunda fase:

- No hubo malware que lograra realizar cambios o lecturas importantes en el sistema.

10.1.6. Resultado de Pruebas sobre imagen Windows 10: Trendmicro

	Backdoor:	Troyanos:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	10	10	1	1	10	10	10
SEGUNDA FASE	0	0	0	0	2	0	0

Tabla 10 Resultado de Pruebas sobre imagen Windows 10: Trendmicro

Comentarios primera fase:

- Se escribieron todos los ficheros maliciosos en el sistema, después de unos minutos se eliminaron un par.

Comentarios segunda fase:

- **PUP:** 13f6b.PUP-PUA y 45ddd.PUP-PUA logro instalarse en el sistema, además de haber muchas conexiones a sitios catalogados como sospechosos.

10.2. Resultado de Pruebas sobre imagen Windows 11

PRIMERA FASE (ENVÍO DE MALWARE):

1. Validar si llegó integro el fichero después de 15 segundos.

SEGUNDA FASE (EJECUCIÓN):

1. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo o tener interacción (lectura, escritura, o modificación de registros, así como la ejecución de procesos) con el sistema.
2. Análisis de comportamiento del malware en la máquina.

CONSIDERACIONES DE LOS RESULTADOS:

1. Validar si llegó integro el fichero después de 15 segundos.
2. Validar si después de 15 segundos no se borra de una carpeta sin excepciones
3. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo.
    1. En algunas capturas veremos un fichero llamado autoruns.exe este es un fichero no malicioso enviado para validación.

RESUMEN DE MALWARE QUE LOGRO INTERACTUAR CON LOS SISTEMAS:

	Backdoor:	Troyanos:	Ransom:	PUP:	Adware:	Virus:
CROWDSTRIKE	0	0	0	2	0	0
MCAFFE	2	0	0	1	0	0

- Pup: 13f6b.PUP-PUA logro instalarse en el sistema
- Adware: 3e1c3.Adware.Obf y 9637b.Adware.Obf lograron leer varios ficheros de sistema, además de 3e1c3.Adware.Obf haber tenido interacción con varios IP catalogadas como maliciosas.
- Virus: Nemim.Virus.Obf y 458c6.Virus.Obf tuvieron una carga importante en el sistema en el CPU. ficheros y escrituras en el registro.

10.1.4. Resultado de Pruebas sobre imagen Windows 10: Sentinel One

	Backdoor:	Troyano:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	0	1	0	1	5	0	0
SEGUNDA FASE	0	0	0	0	1	0	0

Tabla 8 Resultado de Pruebas sobre imagen Windows 10: Sentinel One

Comentarios primera fase:

- Fue la solución tecnológica mejor posicionada en eliminar el malware al momento de moverse a una carpeta que no tenía protección, además, varios minutos después, logro eliminar archivos PUP y al Ransomware Ghost.

Comentarios segunda fase:

- PUP: Instalación del software no deseado llamado, IObitUnlocker.exe que, aunque logró ser catalogado como sospechoso por Sentinel One, parecía necesitar de una desinstalación para eliminar todos los ficheros maliciosos.
- GHOST: Se cortó después de alcanzar a cifrar un par de ficheros, que fueron regresados a como estaban por Sentinel one.

10.1.5. Resultado de Pruebas sobre imagen Windows 10: Sophos

	Backdoor:	Troyanos:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	10	10	1	1	10	10	10
SEGUNDA FASE	0	0	0	0	0	0	0

Tabla 9 Resultado de Pruebas sobre imagen Windows 10: Sophos

Comentarios primera fase:

- Se escribieron todos los ficheros maliciosos en el sistema, después de unos minutos se eliminaron un par.

10.1.2. Resultado de pruebas sobre imagen Windows 10: McAfee

Número de elementos maliciosos que llegaron a interactuar con el Sistema a pesar de la protección de la solución tecnológica instalada y en operación.

	Backdoor:	Troyano:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	10	10	1	1	10	10	10
SEGUNDA FASE	0	1	0	0	2	1	3

Tabla 6 Resultado de pruebas sobre imagen Windows 10: McAfee

Comentarios primera fase:

- Se escribieron todos los ficheros maliciosos en el sistema, después de unos minutos se eliminaron un par.

Comentarios segunda fase:

- troyanos: 9637b.Adware.Obf logró leer parte de sistema, aunque no logró hacer cambios importantes.
- PUP: 13f6b.PUP-PUA logró instalarse por complete en el Sistema Operativo, el segundo leyó, pero no hizo cambios importantes.
- Adware: 9637b.Adware.Obf logró escribir en registro y leer ficheros del Sistema.
- Virus: 3 Virus lograron interactuar con el Sistema y registros.

10.1.3. Resultado de pruebas sobre imagen Windows 10: Windows Defender

	Backdoor:	Troyanos:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	10	10	1	1	10	10	10
SEGUNDA FASE	0	1	0	0	1	2	3

Tabla 7 Resultado de pruebas sobre imagen Windows 10: Windows Defender

Comentarios primera fase:

- Se escribieron todos los ficheros maliciosos en el sistema, después de unos minutos se eliminaron un par.

Comentarios segunda fase:

- Troyanos: 73854.troyano.Obf logró leer varios ficheros de sistema, además de escritura en registro.
- Noko: Logró escribir los ficheros de rescate y leer librerías de cifrado, antes de ser cortado.

RESUMEN DE MALWARE QUE LOGRÓ INTERACTUAR CON LOS SISTEMAS:

Número de elementos maliciosos que llegaron a interactuar con el Sistema a pesar de la protección de la solución tecnológica instalada y en operación.

	Backdoor:	Troyano:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
CROWDSTRIKE	0	0	0	0	1	0	0
MCAFFEE	0	1	0	0	2	1	3
Microsoft Defender	0	1	0	0	1	2	3
SENTINEL ONE	0	0	0	0	1	0	0
SOPHOS	0	0	0	0	0	0	0
TRENDMICRO	0	0	0	0	2	0	0

Tabla 4 Resultado de Pruebas sobre imagen Windows 10

10.1.1. Resultado de pruebas sobre imagen Windows 10: Crowdstrike

Número de elementos maliciosos que llegaron a interactuar con el Sistema a pesar de la protección de la solución tecnológica instalada y en operación.

	Backdoor:	Troyano:	Ransom Noko:	Ransom Ghost:	PUP:	Adware:	Virus:
PRIMERA FASE	0	1	0	1	2	1	0
SEGUNDA FASE	0	0	0	0	1	0	0

Tabla 5 Resultado de pruebas sobre imagen Windows 10: Crowdstrike

Comentarios primera fase:

- Fue el único EDR que no permitió usar el emulador de ataques, dado que reinicia el proceso, aunque tenía excepciones, por lo que se envió malware a mano.
- El envío de malware fue usando un fichero comprimido a través de una página web.

Comentarios segunda fase:

- Solo se permitió la instalación del software PUP Walliant catalogado como aplicación potencialmente no deseada por varios medios.

9.3.4. Descripción de Pruebas en escenarios de Fedora

Se enviaron un total de 6 elementos de objetos de malware a cada equipo con Sistema Fedora (6 escenarios, 1 para cada solución de EDR) durante los días 12 al 26 de septiembre del 2022.

f) Backdoor – 1 elemento
g) Ransomware – 1 elemento
h) Miner – 1 elemento
i) Backdoor / Metasploit – 2 elemento
j) Backdoor / LivingOfTheLand – 1 elemento

Nota: La diferencia en cantidad de malware respecto a sistemas Windows es porque este sistema operativo es solo afectado por ciertas familias de malware, teniendo una menor cantidad en la herramienta de evaluación, así como apegándonos a ambientes reales en las empresas y usuarios.

9.4. Descripción de los parámetros de la pruebas.

Las variables que determinaron la eficiencia de cada control frente a diferentes familias de programas malignos:

a) WINDOWS:
    a) Encontraremos dos tablas, una para Windows 10 y otra para Windows 11, cada una esta dividida en los controles a la izquierda y parte superior a la familia de programas malignos.
        a) Los números que aparecen dentro son la cantidad de malware que lograron ejecutarse por al menos 15 segundos e interactuar con el sistema operativo, realizando cambios en registros o archivos.
b) LINUX:
    a) Encontraremos una tabla por sistema operativo Fedora y Ubuntu, cada una está dividida en los controles a la izquierda y parte superior a la familia de programas malignos.
        a) Los criterios fueron dos, escritura y ejecución, en la cual podremos apreciar la nomenclaturas WR(escritura) y EXEC(Ejecución).
        b) En el cual un uno significa que fue exitoso el ataque por parte del malware en la etapa de escritura o ejecución, así mismo con la de ejecución, en caso contrario aparece un 0 que significa fallido.

10. Resultado de Pruebas

10.1. Resultado de Pruebas sobre imagen Windows 10

PRIMERA FASE (ENVÍO DE MALWARE):

1. Validar si llegó íntegro el fichero después de 15 segundos.

SEGUNDA FASE (EJECUCIÓN):

1. Validar si el exe se logra ejecutar por menos 15 segundos en el equipo o tener interacción (lectura, escritura, o modificación de registros, así como la ejecución de procesos) con el sistema.
2. Análisis de comportamiento del malware en la máquina.

9.3. Descripción de Pruebas

Para la ejecución de las pruebas, se ejecutó el siguiente procedimiento para cada uno de los escenarios

1. **Primer paso (ENVIO DE MALWARE):**
   1.1. Se validó si el objeto de malware llegó integro después de 15 (quince) segundos.
2. **Segundo paso (EJECUCIÓN):**
   2.1. Se validó si el objeto de malware se logró ejecutar por menos 15 (quince) segundos en el equipo o tener interacción (lectura, escritura, o modificación de registros, así como la ejecución de procesos) con el sistema.
   2.2. Análisis de comportamiento del malware en el equipo.

9.3.1. Descripción de Pruebas en escenarios de Windows 10

Se enviaron un total de 52 elementos de objetos de malware al equipo con Sistema Microsoft Windows 10 (6 escenarios, 1 para cada solución de EDR) durante los días 1 al 5 de agosto del 2022.

a) Backdoor – 10 elementos
b) Troyano – 10 elementos
c) Ransomware – 2 elementos
d) PUP-PUA – 10 enviados
e) Adware – 10 enviados
f) Virus – 10

9.3.2. Descripción de Pruebas en escenarios de Windows 11

Se enviaron un total de 52 elementos de objetos de malware al equipo con Sistema Microsoft Windows 11 (6 escenarios, 1 para cada solución de EDR) durante los días 1 al 5 de agosto del 2022.

a) Backdoor – 10 elementos
b) Troyano – 10 elementos
c) Ransomware – 2 elementos
d) PUP-PUA – 10 enviados
e) Adware – 10 enviados
f) Virus - 10

9.3.3. Descripción de Pruebas en escenarios de Ubuntu

Se enviaron un total de 6 elementos de objetos de malware a cada equipo con Sistema Ubuntu (6 escenarios, 1 para cada solución de EDR) durante los días 12 al 26 de septiembre del 2022.

a) Backdoor – 1 elemento
b) Ransomware – 1 elemento
c) Miner – 1 elemento
d) Backdoor / Metasploit – 2 elemento
e) Backdoor / LivingOfTheLand – 1 elemento

Nota: La diferencia en cantidad de malware respecto a sistemas Windows es porque este sistema operativo es solo afectado por ciertas familias de malware, teniendo una menor cantidad en la herramienta de evaluación, así como apegándonos a ambientes reales en las empresas y usuarios.

a) **Troyano** [5]

Los troyanos son programas maliciosos que realizan acciones no autorizadas por el usuario: eliminan, bloquean, modifican o copian datos, y alteran el funcionamiento de los equipos y las redes de computadoras. A diferencia de los virus y los gusanos, las amenazas que entran en esta categoría son incapaces de auto-replicarse. Los troyanos se clasifican según el tipo de acción que realizan en un equipo infectado.

b) **Backdoor** [6]

Los Backdoors (troyanos de puerta trasera) están diseñados para dar a los usuarios maliciosos el control de un equipo infectado. En términos de funcionalidad, las "puertas traseras" son similares a muchos sistemas de administración diseñados y distribuidos por desarrolladores de programas legítimos.

Este tipo de programas maliciosos permiten que el operador del troyano haga lo que quiera en el equipo infectado: enviar y recibir archivos, ejecutar archivos o eliminarlos, mostrar mensajes, borrar datos, reiniciar la computadora, entre otras.

En general, los programas de esta categoría se utilizan para agrupar un número de equipos infectados y formar una botnet o red zombi. Esto ofrece a los usuarios maliciosos el control centralizado de un ejército de equipos infectados que luego podrán ser utilizados con fines delictivos.

c) **Ransomware** [7]

El Ransomware incluye todos aquellos programas maliciosos que impiden el acceso normal a ciertos datos o interrumpen el funcionamiento de un equipo y cuya instalación fue realizada sin el consentimiento del usuario. Tales programas son utilizados por los cibercriminales para extorsionar a los usuarios y exigir el pago de un rescate.

d) **PUP-PUA** [8]

PUA es el acrónimo de "Potentially Unwanted Application" (Aplicación potencialmente no deseada), mientras que PUP es el acrónimo de "Potentially Unwanted Program" (Programa potencialmente no deseado).

Un PUP es un programa potencialmente indeseable que suele instalarse cuando se instala otro software en la computadora. Normalmente, un PUP funciona como una herramienta de marketing y suele modificar la configuración del navegador o mostrar publicidad no deseada. La forma más común de PUP es el adware.

e) **Adware** [9]

El adware es una categoría de programas diseñados para mostrar publicidad (por lo general, en forma de banners), así como para redirigir solicitudes de búsqueda a sitios web de publicidad y recopilar datos de marketing sobre los usuarios (por ejemplo, qué tipos de sitios web visita) con el fin de mostrarles una publicidad personalizada.

f) **Virus**[10]

Los virus y gusanos son todos aquellos programas maliciosos capaces de auto-replicarse en los sistemas, a través de redes de computadoras sin conocimiento del usuario. A su vez, cada copia de estos programas maliciosos es también capaz de auto-replicarse.

---

[5]Kaspersky: https://encyclopedia.kaspersky.es/knowledge/trojans/

[6] Kaspersky: https://encyclopedia.kaspersky.es/knowledge/backdoor/

[7] Kaspersky: https://encyclopedia.kaspersky.es/knowledge/trojan-ransom/

[8]Kaspersky:https://encyclopedia.kaspersky.es/knowledge/adware-pornware-and-riskware/

[9]Kaspersky: https://encyclopedia.kaspersky.es/knowledge/adware/

[10] Kaspersky: https://encyclopedia.kaspersky.es/knowledge/viruses-and-worms/

Características Técnicas	Windows		Linux	
Memoria Ram	8 GB	8 GB	8 GB	8 GB
Disco Duro	70 GB	70 GB	70 GB	70 GB
Tarjeta grafica	No	No	No	No
¿Acceso a internet?	Sí	Sí	Sí	Sí
Hash de imagen de sistema operativo (SHA-256)	7824187bd8efefc2ec022cd5b89c6b5d2669f54f6727cae96bd70c91e80e8a4e	ec8d625c3329d84e4d458c975619a761187e874b5bbacd0d46bf7beab5bc8d9a	f92f7dca5bb6690e1af0052687ead49376281c7b64fbe4179cc44025965b7d1c	85d9d0c233d560e401e2ad824aa8e6d5614e8b977dfe685396bfb2eb3ba5b253

Tabla 3 Características Técnicas de equipos víctimas

9.1. Elementos de integridad en Laboratorio de Pruebas

Como parte de controles de integridad para las pruebas se consideraron los siguientes controles:

a) El laboratorio se encuentra en un ambiente controlado y virtualizado para la ejecución de pruebas.
b) El laboratorio se encuentra en una red controlada y asilada de otras redes.
c) El laboratorio cuenta con acceso controlado hacia internet.
d) El laboratorio cuenta con software necesario para la ejecución de pruebas.
e) Cada maquina víctima se ejecutó desde una imagen limpia con un valor de integridad Hash de imagen de sistema operativo (SHA-256).
f) Las pruebas son realizadas por personal certificado y calificando en materia de seguridad de información (CEH, CHFI).
g) Las pruebas son documentadas mediante grabaciones y generación de archivos, las cuales se agregan como evidencia anexa al presente estudio.

9.2. Selección de Pruebas

Se estableció un mismo grupo de pruebas, el cual fue enviado a cada una de las maquinas víctimas con cada uno de las soluciones EDR instaladas para revisar su eficacia.
Las pruebas enviadas contemplan los siguientes escenarios:

a) Prueba de envío de correos y/o mensajes maliciosos.
b) Pruebas para brindar la posibilidad de bloquear el dispositivo de usuario final.
c) Pruebas para borrar de manera remota la información contenida en el dispositivo.
d) Pruebas para certificar material gráfico y direcciones de páginas web.

Dentro de los mensajes maliciosos, se enviaron objetos de malware de las siguientes clasificaciones:

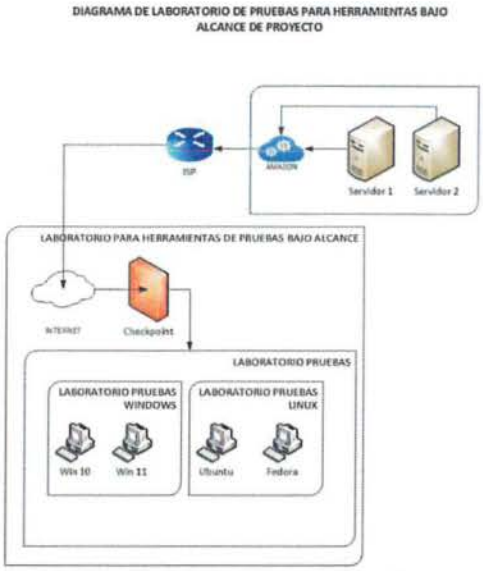


Ilustración 3Diagrama de Laboratorio de pruebas

Donde se establecieron 2 servidores atacantes desde la nube de aws (amazon web services) utilizando un emulador de ataques y de monitoreo mediante servicio de "Software as a Service", así como 4 equipos víctima con los siguientes distribuciones de sistemas Operativos:

Características Técnicas	Windows		Linux	
Sistema operativo	Microsoft Windows 10 Home	Microsoft Windows 11 Home	Ubuntu	Fedora
Versión del sistema operativo:	10.0.19044 N/A Build 19044	10.0.22000 N/A Build 22000	Ubuntu 20.04.4 LTS	Fedora Linux 35 (Workstation Edition)
Tipo del sistema	64 Bits	64 Bits	64 Bits	64 Bits
Fabricante del sistema operativo:	Microsoft Corporation	Microsoft Corporation	Ubuntu	Fedora
Procesador	Intel64 Family6 Model 158 Stepping Genuine Intel 2208 Mhz	Intel64 Family6 Model 158 Stepping Genuine Intel 2208 Mhz	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz

Tabla 2 Características Técnicas de sistema Operativo de equipos victimas

En cada sistema operativo (4 SO) se instalaron de manera independiente las 6 Soluciones de EDR, generando 24 grupos de escenarios de pruebas en las que se ejecutaron las mismas pruebas para cada escenario.

Las características de las maquinas víctimas, donde se instalaron las Soluciones EDR a probar son las siguientes:

Se identifican como lideres de mercado las soluciones de EDR de las siguientes marcas, las cuales se enlistan en orden estrictamente alfabético:

Marca		Licenciamiento
Crowdstrike	CROWDSTRIKE	• Software empresarial con licenciamiento EDR y NGAV con las políticas mas agresivas.
McAfee	McAfee	• Software de grado "Home" con todas las políticas de seguridad activadas.
Microsoft Defender	Microsoft Defender	• Software con licenciamiento empresarial.
Sentinel One	SentinelOne	• Software empresarial con licenciamiento EDR y NGAV con las políticas más agresivas.
Sophos	SOPHOS	• Software EDR empresarial.
Trend Micro	TREND MICRO	• Software con licenciamiento empresarial.

Tabla 1 Soluciones EDR lideres de mercado

9. Establecimiento de Laboratorio de Pruebas

Como parte inicial de las pruebas se estableció un laboratorio para la evaluación de las diferentes herramientas tecnológicas en el alcance de estudio. El establecimiento de laboratorio consta de la siguiente arquitectura:

- 2 Servidores atacantes (emulador de ataque y monitoreo) mediante una IP pública.
- 4 Servidores victima con segmentación local por áreas de red locales virtualizadas (VLAN) a través de un Firewall y mediante un cliente de monitoreo, con conectividad hacia el servidor de monitoreo publicado.
- Conectividad por un proveedor de servicio de internet empresarial.
- Elementos de Telecomunicaciones para el enrutamiento de los ataques.
- Elementos de Seguridad firewall para restringir la red de laboratorio.

Dentro del cuadrante mágico de Gartner[4] de los Sistemas EDR desarrollado durante 2021 y liberado en 2022 se encuentran:

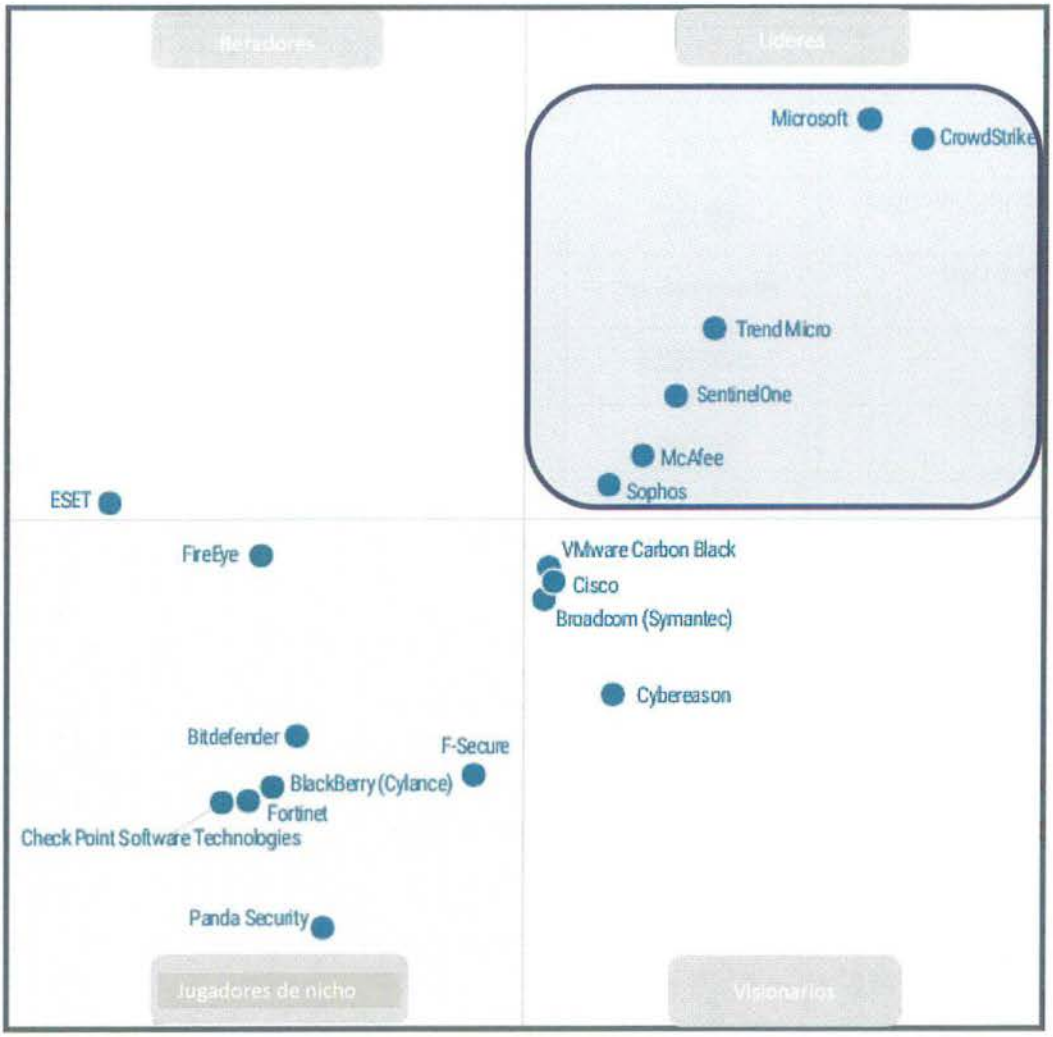


Ilustración 2 Cuadrante Mágico de Gartner sistema EDR

[4] Gartner Peer Insights: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

Los ejecutables llegaron a tener interacción con el sistema

Process Name	PID	CPU	File Events	Registry Events	Network Events
9637b.Adware.Obf.exe	1644	1.29 %	3,557	2,712	0
62043.Adware.Obf.exe	2684	0 %	1	3	0
62043.Adware.Obf.exe	3220	0.37 %	303	595	0

Total de Eventos en registro	Reads	Writes
3,310	1,596	196

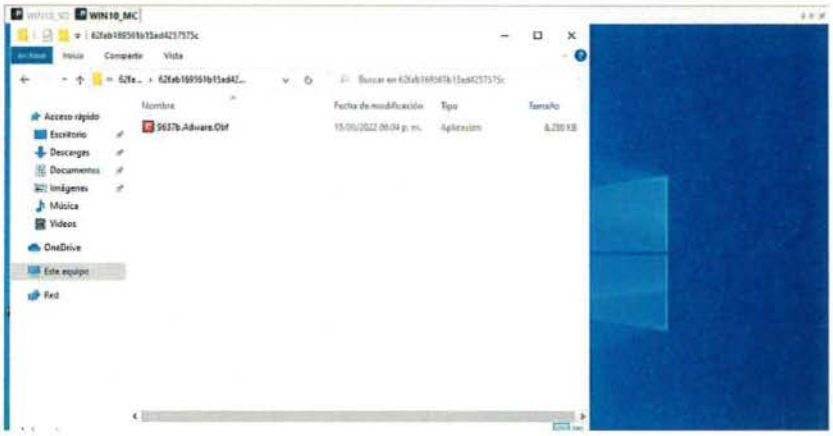
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



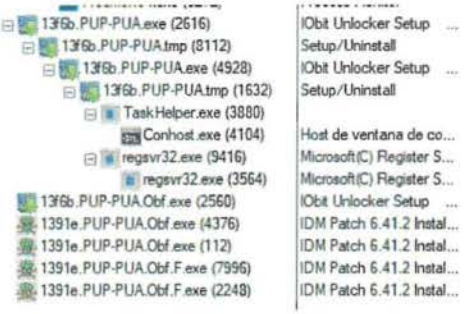
15.10. McAfee PUP

INFORMACIÓN GENERAL:

Los ejecutables llegaron a tener interacción con el sistema

Process Name	PID	% CPU	File Events	Registry Events	Network Bytes
13f6b.PUP-PUA.exe	2616	0.18	580	494	0
13f6b.PUP-PUA.tmp	8112	0.29	988	4,484	0
13f6b.PUP-PUA.exe	4928	0.1	570	473	0
13f6b.PUP-PUA.tmp	1632	1.93	3,256	7,393	0
TaskHelper.exe	3880	0	393	541	0
Conhost.exe	4104	0	106	464	0
regsvr32.exe	9416	0	280	414	0
regsvr32.exe	3564	0	281	600	0
13f6b.PUP-PUA.Obf.exe	2560	0.93	377	673	0
1391e.PUP-PUA.Obf.exe	4376	0	1	3	0
1391e.PUP-PUA.Obf.exe	112	1.18	396	622	0
1391e.PUP-PUA.Obf.F.exe	7996	0	1	3	0
1391e.PUP-PUA.Obf.F.exe	2248	0.95	395	622	0

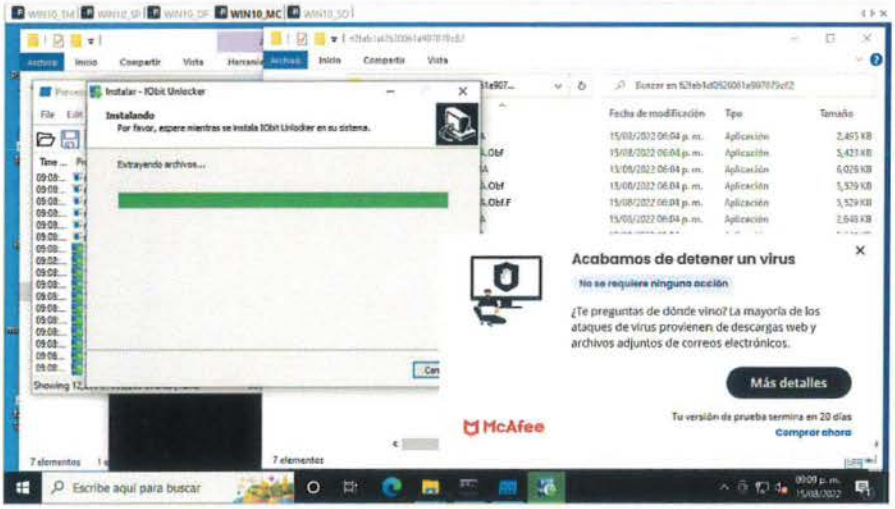
ÁRBOL DE PROCESOS:



CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.11. McAfee Trojan

INFORMACIÓN GENERAL:

Los ejecutables llegaron a tener interacción con el sistema

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
0454c.Trojan.Obf.exe	7792	0.03125	101	181	0

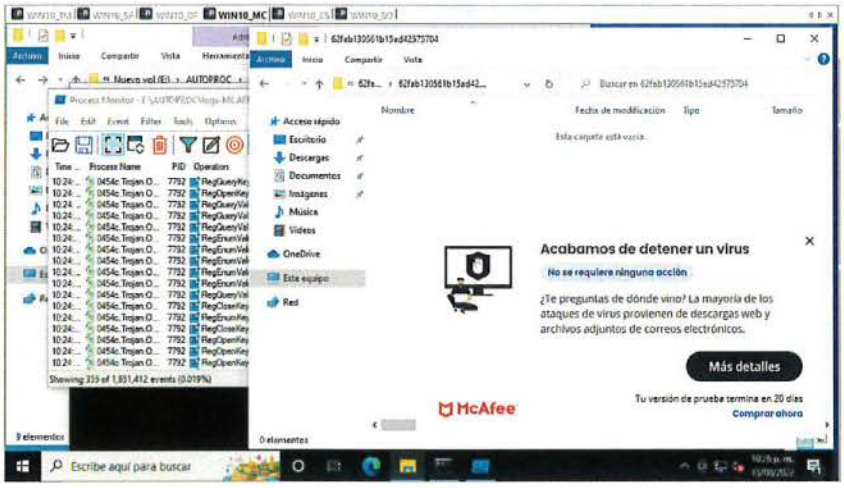
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURAS DE PANTALLA:



15.12. McAfee Virus

INFORMACIÓN GENERAL:

Los ejecutables llegaron a tener interacción con el sistema

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
69bf2.Virus.Obf.exe	2688	0	1	3	0
69bf2.Virus.Obf.exe	5360	0.484375	294	641	0
Conhost.exe	728	0.125	170	666	0
3591b.Virus.Obf.exe	6760	0.015625	118	232	0
Nemim.Virus.Obf.exe	1236	8.78125	183	303	0

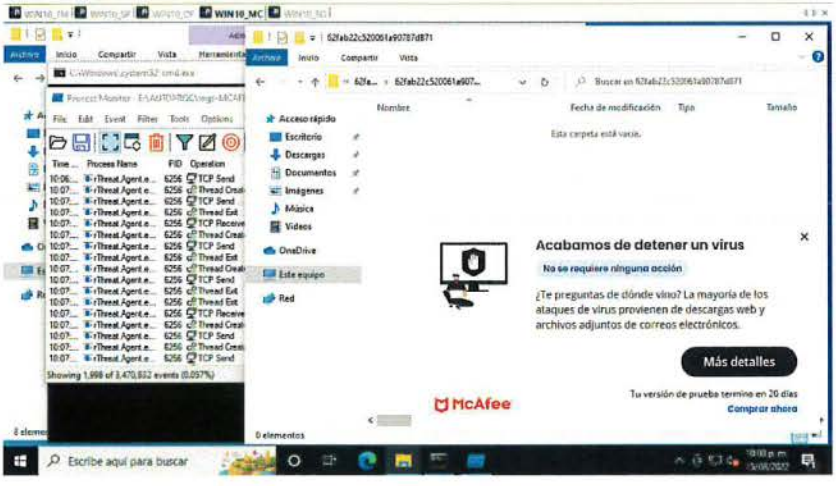
ÁRBOL DE PROCESOS:

69bf2.Virus.Obf.exe (2688)	Explorer
69bf2.Virus.Obf.exe (5360)	Explorer
Conhost.exe (728)	Host de ventana de co...
3591b.Virus.Obf.exe (6760)	
Nemim.Virus.Obf.exe (1236)	File Encryption

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.13. McAfee Ransomware Nokoyawa

INFORMACIÓN GENERAL:

El fichero no se permitía ejecutar, dado que el ransomware fue eliminado por MCAffee al momento de intentar ejecutarlo.

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
69bf2.Virus.Obf.exe	2688	0	1	3	0
69bf2.Virus.Obf.exe	5360	0.484375	294	641	0
Conhost.exe	728	0.125	170	666	0
3591b.Virus.Obf.exe	6760	0.015625	118	232	0
Nemim.Virus.Obf.exe	1236	8.78125	183	303	0

The current filter excludes all 1,049,020 events

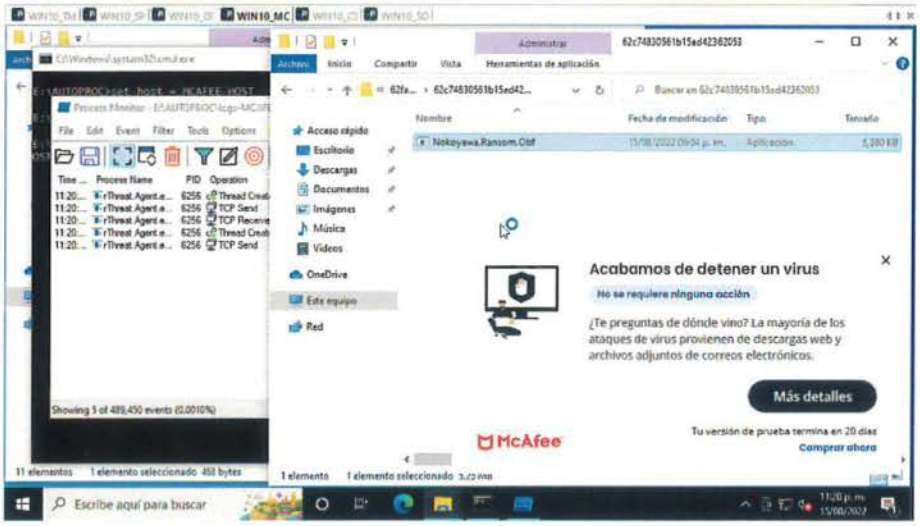
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.14. McAfee Ramsomware Ghost

INFORMACIÓN GENERAL:

El ransomware no logro ejecutarse debido a que al momento de ejecutarse se protegía de ser monitoreado por MCAffee.

El ransomware no logro escribir en el disco, solo leyó parte de fichero de sistema.

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
HolyGhost.Ransom.Obf.exe	9632	0.171875	284	452	0

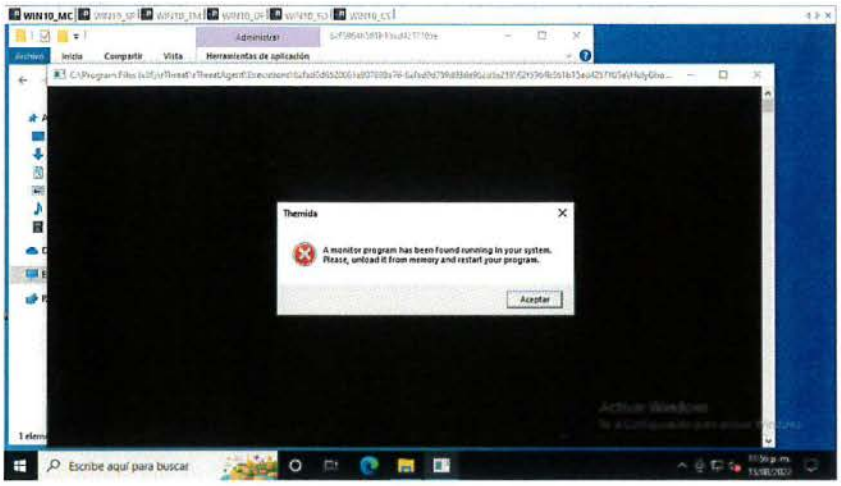
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.15. Microsoft Defender Backdoor

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

The current filter excludes all 7,545,723 events

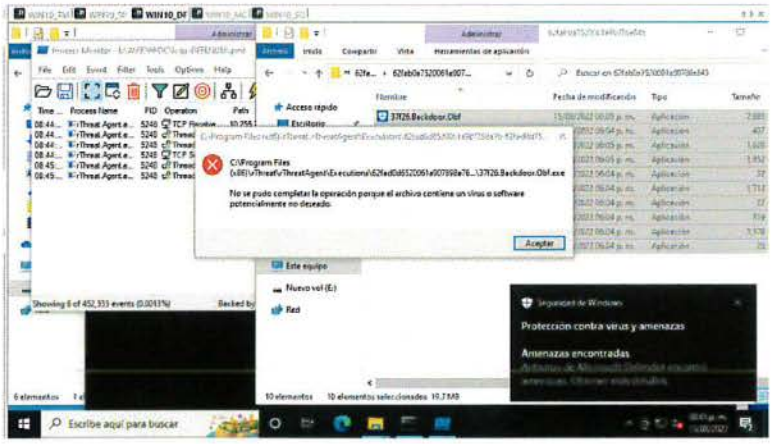
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.16. Microsoft Defender Adware

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
3e1c3.Adware.Obf.exe	644	1.82	834	1,238	0
3e1c3.Adware.Obf.exe	3092	1.93	1,211	3,925	61
3e1c3.Adware.Obf.exe	3968	0	0	0	0
9637b.Adware.Obf.exe	2344	1.17	3,914	2,712	0

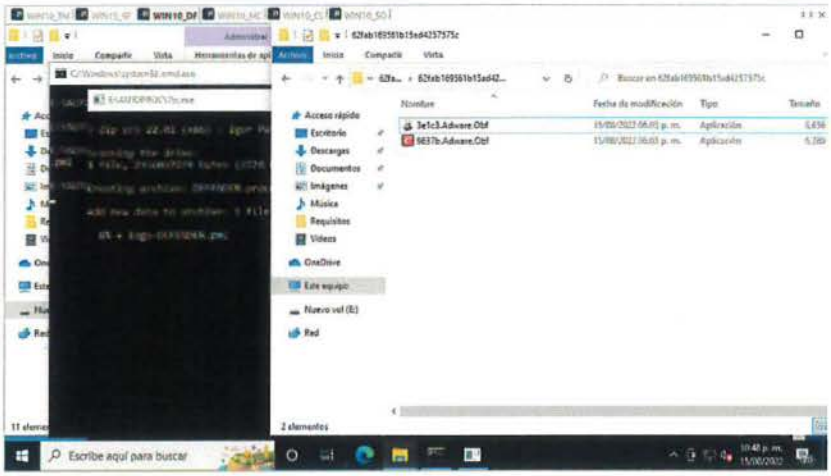
ÁRBOL DE PROCESOS:

3e1c3.Adware.Obf.exe (644)	
9637b.Adware.Obf.exe (2344)	COMODO Internet Security

CONEXIONES A INTERNET

Total Events	Send Bytes	Receive Bytes	IP	N° de Flags como malicioso
19	536	6,986	103.224.212.220:443	1
13	221	11,311	13.248.148.254:80	2
17	562	5,868	148.251.234.83:443	1
6	247	889	23.193.172.216:80	0
6	115	1,006	23.204.128.228:80	0

CAPTURA DE PANTALLA:



15.17. Microsoft Defender PUP

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
13f6b.PUP-PUA.exe	6752	0.26	831	489	0
13f6b.PUP-PUA.tmp	7764	0.4	1,714	4,492	0
13f6b.PUP-PUA.exe	7588	0.21	797	468	0
13f6b.PUP-PUA.tmp	6784	2	4,451	7,382	0
TaskHelper.exe	8268	0.01	696	536	0
Conhost.exe	6260	0.04	276	464	0
regsvr32.exe	2808	0.09	671	391	0
regsvr32.exe	6864	0	553	600	0
13f6b.PUP-PUA.Obf.exe	4788	0.9	644	673	0

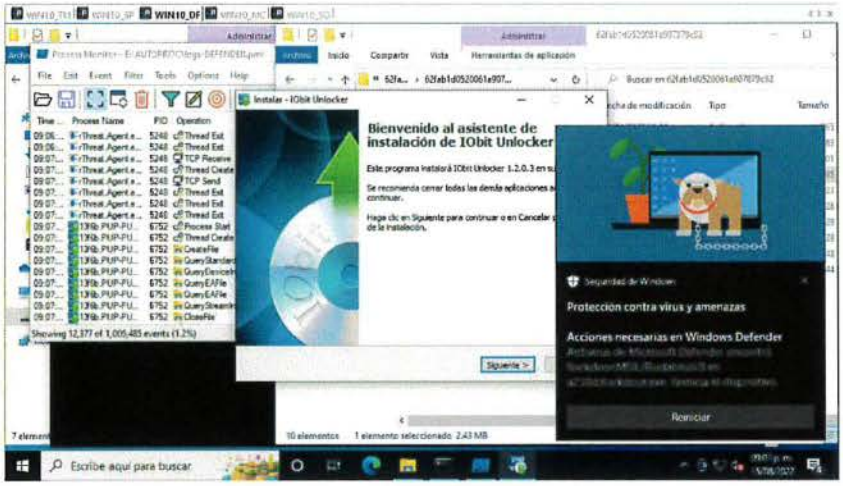
ÁRBOL DE PROCESOS:

13f6b.PUP-PUA.exe (6752)	IObit Unlocker Setup
13f6b.PUP-PUA.tmp (7764)	Setup/Uninstall
13f6b.PUP-PUA.exe (7588)	IObit Unlocker Setup
13f6b.PUP-PUA.tmp (6784)	Setup/Uninstall
TaskHelper.exe (8268)	
Conhost.exe (6260)	Host de ventana de consola
regsvr32.exe (2808)	Microsoft(C) Register Server
regsvr32.exe (6864)	Microsoft(C) Register Server
13f6b.PUP-PUA.Obf.exe (4788)	IObit Unlocker Setup

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.18. Microsoft Defender Trojan

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
73854.Trojan.Obf.exe	4464	0.25	561	597	0

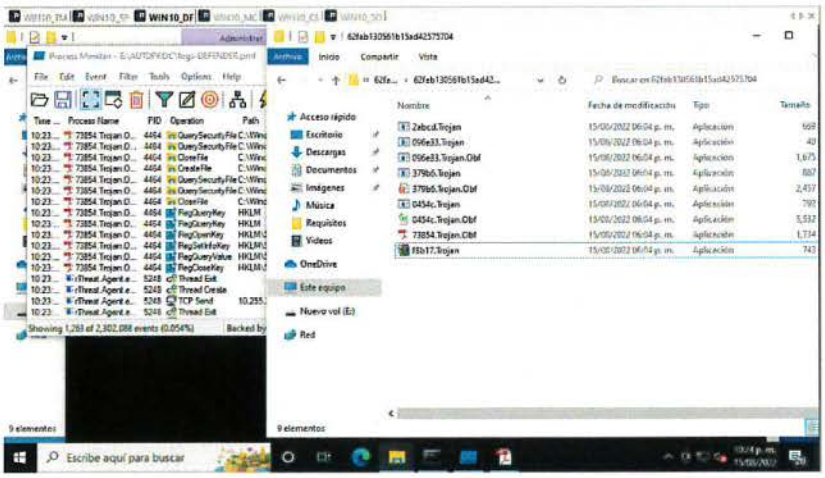
Eventos en registro	Reads	Writes
597	232	51

ÁRBOL DE PROCESOS:

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.19. Microsoft Defender Virus

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
Nemim.Virus.Obf.exe	6264	119.6	401	293	0
458c6.Virus.Obf.exe	3352	0	22	3	0
458c6.Virus.Obf.exe	7892	0.57	1,209	734	0
Nemim.Virus.Obf.exe	5356	86.73	253	272	0

Eventos de registro	Reads	Writes	Other
1,302	358	121	205

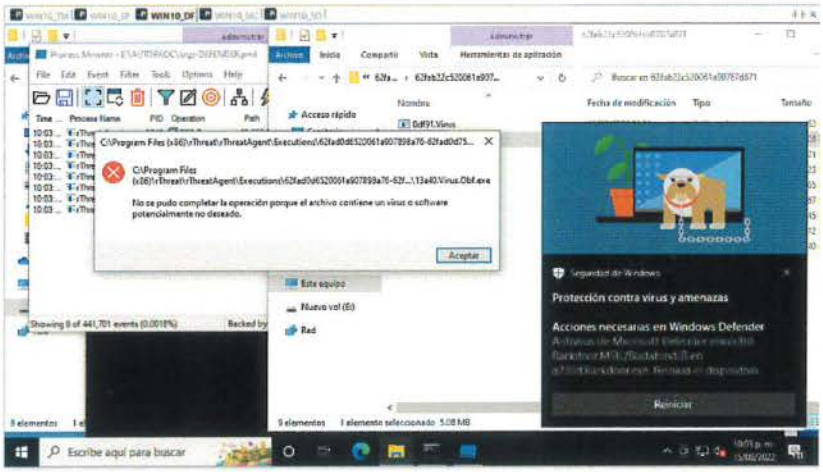
ÁRBOL DE PROCESOS:

Nemim.Virus.Obf.exe (6264)	File Encryption
458c6.Virus.Obf.exe (3352)	Microsoft Firewall Installer - Prot...
458c6.Virus.Obf.exe (7892)	Microsoft Firewall Installer - Prot...
Nemim.Virus.Obf.exe (5356)	File Encryption

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.20. Microsoft Defender Ramsomware Nokoyawa

INFORMACIÓN GENERAL:

El ransomware logro escribir ficheros de rescate en el sistema.

Además de interactuar con librerías de cifrado de Windows.

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
Nokoyawa.Ransom.Obf.exe	4772	11.57	1,080	166	0
Conhost.exe	3860	0.125	396	888	0

Name	File Time	Total Events	Opens	Closes	Reads	Writes
C:	0.1529620	1,476	642	202	25	17
ProgramData	0.1219699	750	475	70	7	16
Users	0.0007064	17	11	2	0	1
Public	0.0004900	9	6	1	0	1
Documents	0.0003655	6	3	1	0	1
NOKOYAWA_readme.txt	0.0003655	6	3	1	0	1
Desktop	0.0001245	3	3	0	0	0
NOKOYAWA_readme.txt	0.0001245	3	3	0	0	0

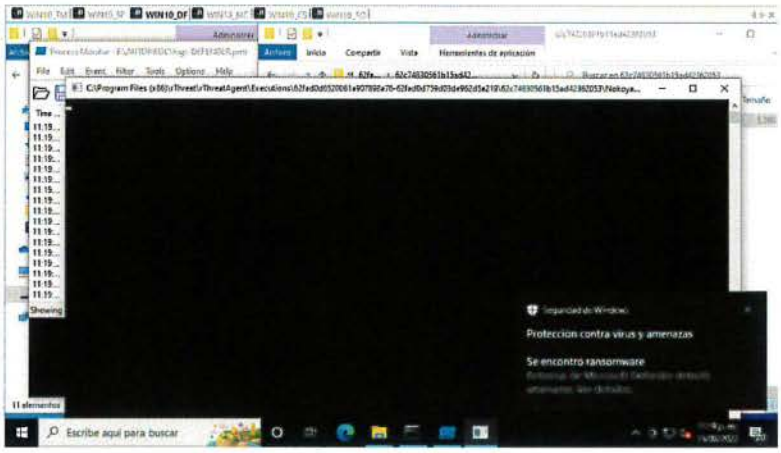
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.21. Microsoft Defender Ramsomware Ghost

INFORMACIÓN GENERAL:

El fichero fue eliminado antes de que lograra tener alguna interacción con el sistema

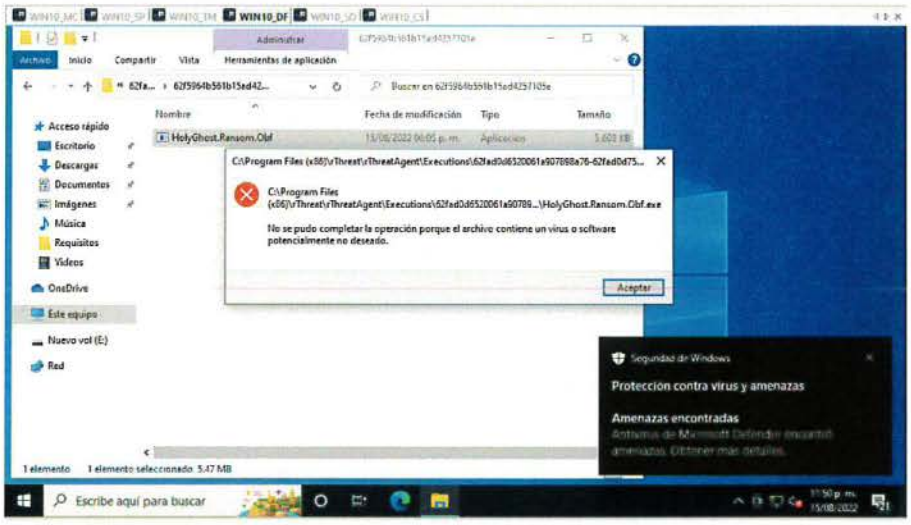
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.22. Sentinel One Backdoor

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:

15.23. Sentinel One Adware

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

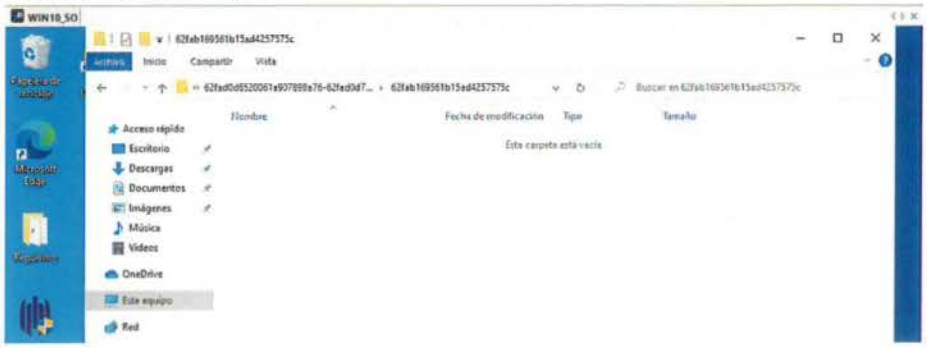
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.24. Sentinel One PUP

INFORMACIÓN GENERAL:

Process Name	File Events	Registry Events	Network Events
13f6b.PUP-PUA.exe	706	663	0
13f6b.PUP-PUA.tmp	1,039	4,793	0
13f6b.PUP-PUA.exe	896	654	0
13f6b.PUP-PUA.tmp	5,731	7,957	0
TaskHelper.exe	794	712	0
Conhost.exe	286	684	0
regsvr32.exe	696	570	0
regsvr32.exe	573	807	0
IObitUnlocker.exe	7	3	0
IObitUnlocker.exe	9,323	33,265	14
IObitUnlocker.exe	6	7	0
IObitUnlocker.exe	11,368	42,826	0

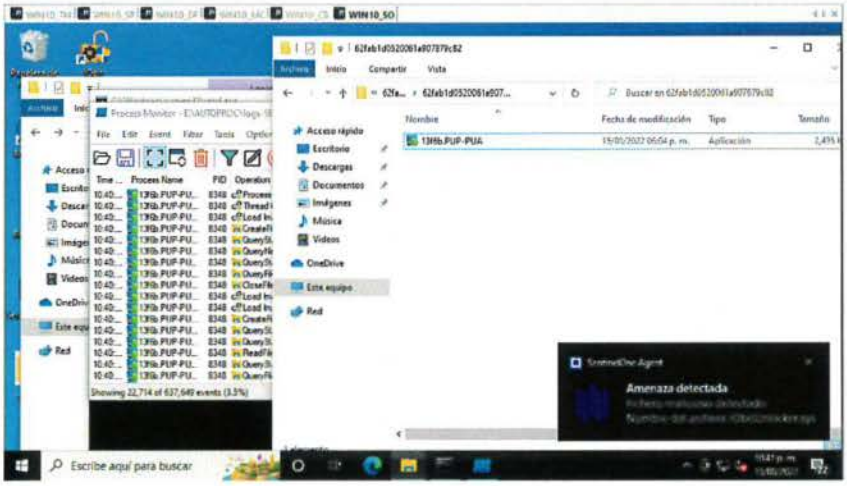
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

Total Events	Connects	Disconnects	Send Bytes	Receive Bytes	IP	N° Detecciones como Maliciosa:
4	1	1	265	465	152.195.19.156:80	0
10	2	2	466	3,645	23.54.187.27:80	1

CAPTURA DE PANTALLA:



15.25. Sentinel One Trojan

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

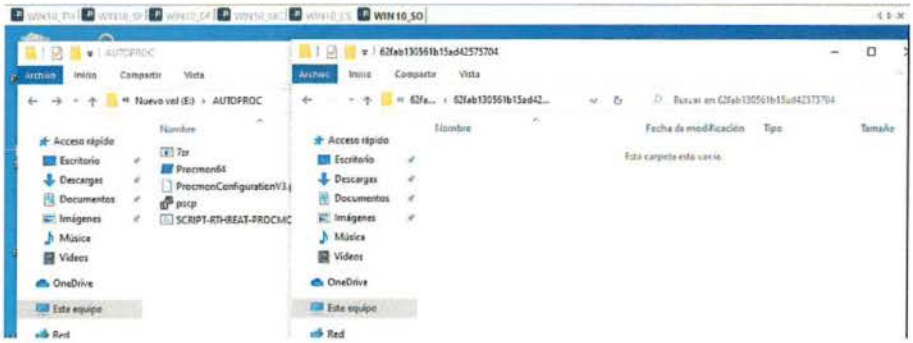
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.26. Sentinel One Virus

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

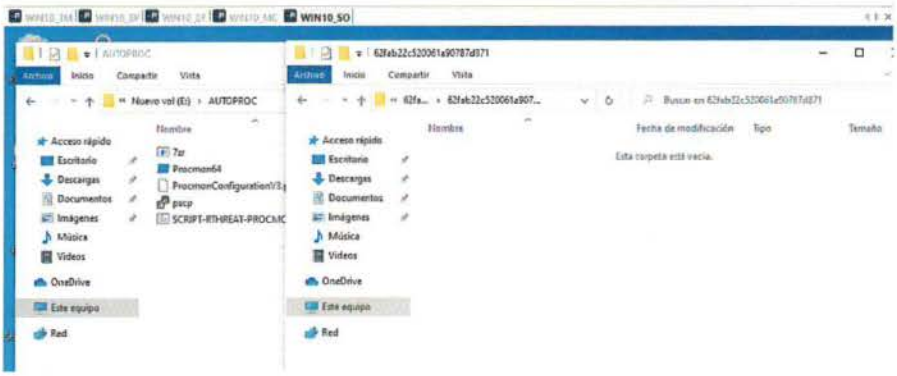
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.27. Sentinel One Virus

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

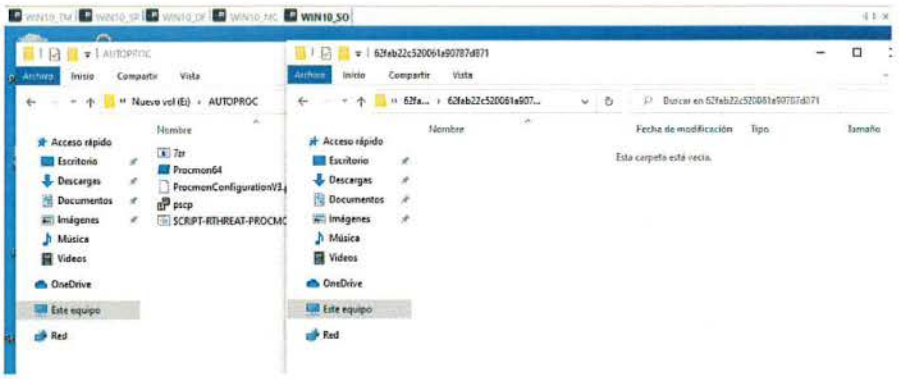
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.28. Sentinel One Ransomware Nokoyawa

INFORMACIÓN GENERAL:

Sentinel one logró eliminar todos los ficheros al ser escritos en disco por lo que no se pudo ejecutar malware.

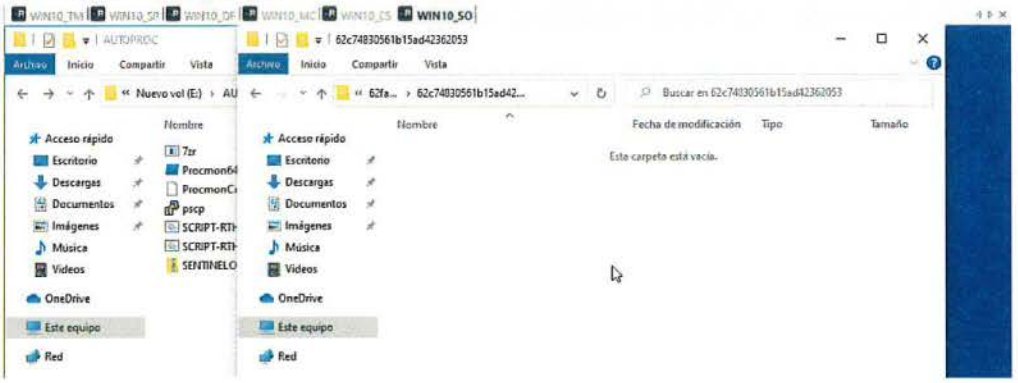
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.29. Sentinel One Ransomware Ghost

INFORMACIÓN GENERAL:

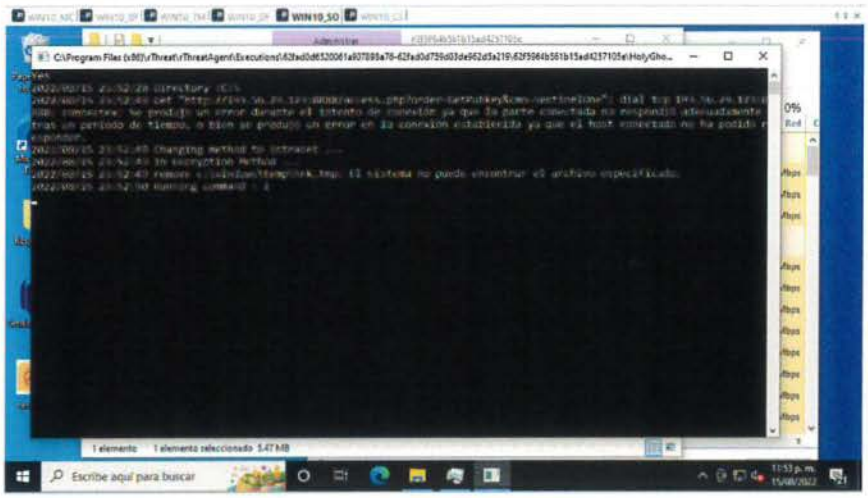
No se usó un monitoreo de sistema porque el ransomware tiene protección, sin embargo el ransomware logró cifrar algunos ficheros, antes de que Sentinel one cerrara el proceso y restaurara los ficheros.

ÁRBOL DE PROCESOS:

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.30. Sophos Backdoor

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

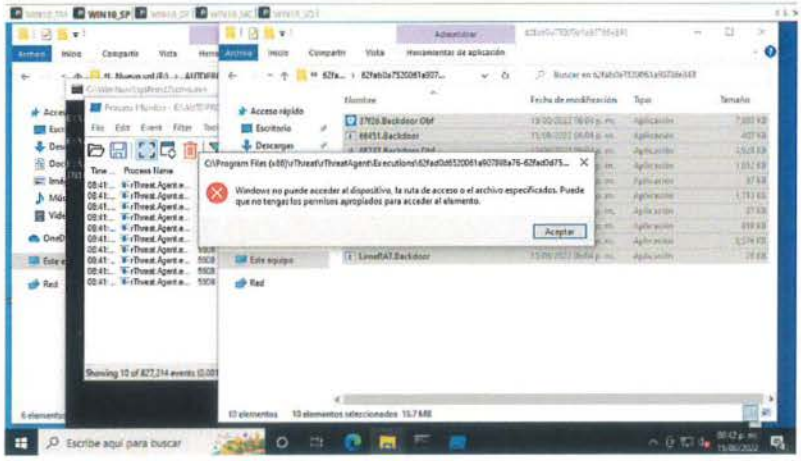
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.31. Sophos Adware

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

The current filter excludes all 3,952,065 events

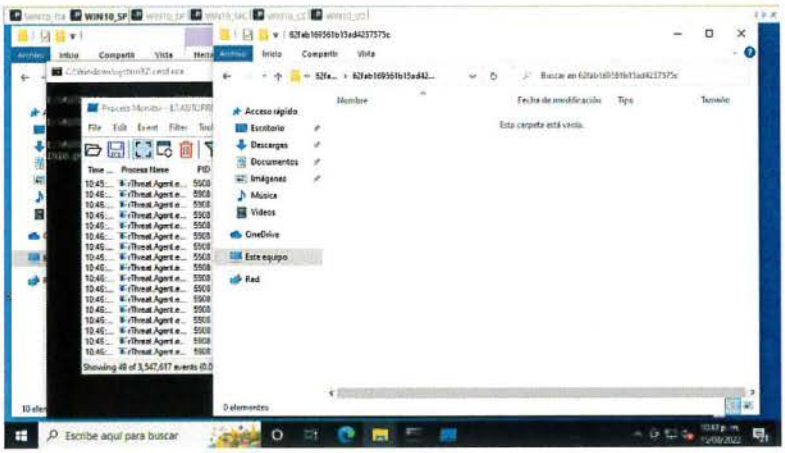
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.32. Sophos PUP

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

The current filter excludes all 5,704,068 events

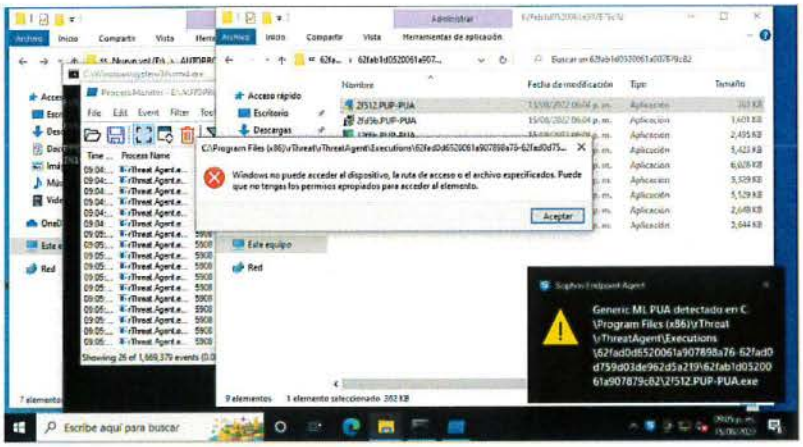
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.33. Sophos Trojan

INFORMACIÓN GENERAL:

Un troyano logró ejecutarse por breves segundos, pero fue bloqueado al momento de la ejecución.

Total Events	Read Bytes	Write Bytes	Path
1	0	0	<Total>
1	0	0	C:\Windows\Prefetch\6ADFC.TROJAN.EXE-0E08F597.pf

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
6adfc.Trojan.exe	7464	0	1	3	0

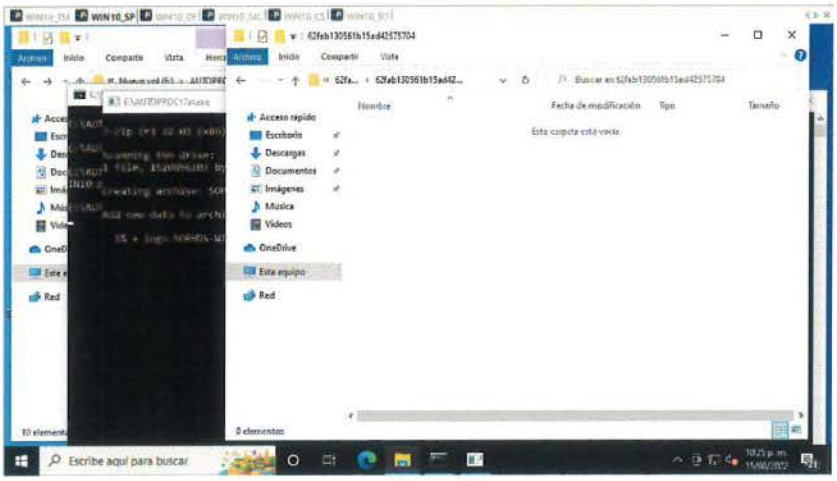
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.34. Sophos Virus

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

The current filter excludes all 4,739,261 events

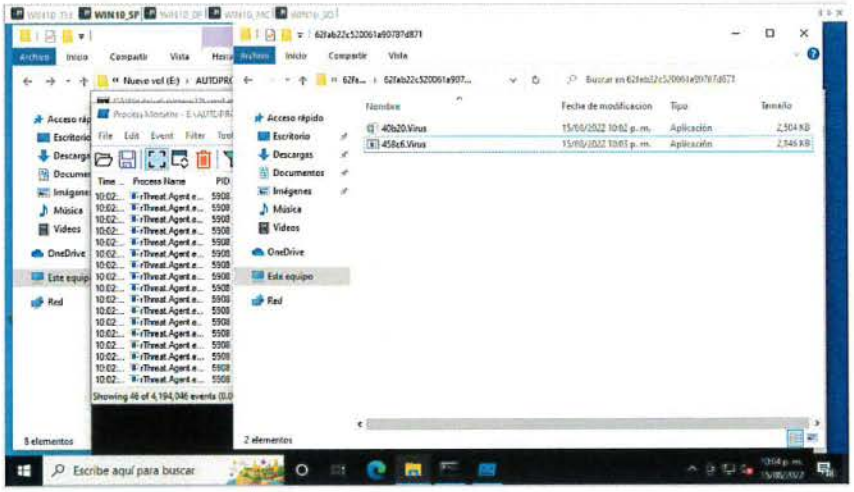
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.35. Sophos Ramsomware Nokoyana

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

The current filter excludes all 1,726,757 events

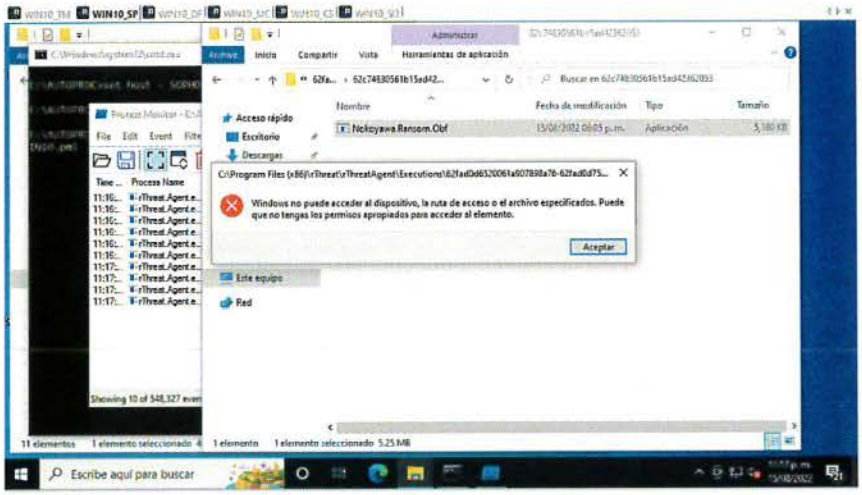
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.36. Sophos Ramsomware Ghost

INFORMACIÓN GENERAL:

Todos los ficheros fueron bloqueados al momento de la ejecución.

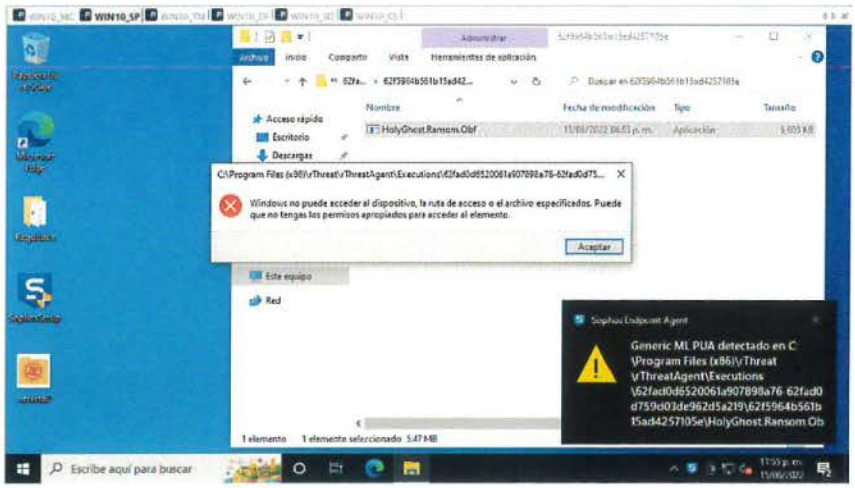
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.37. Trend Micro Backdoor

INFORMACIÓN GENERAL:

Todos los procesos solo lograron cargarse a si mismos, después fueron detenidos por la herramienta de Trendmicro.

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
37f26.Backdoor.Obf.exe	7756	0	1	0	0
37f26.Backdoor.Obf.exe	10076	0	0	0	0
98737.Backdoor.Obf.exe	6468	0	1	0	0
a28e3.Backdoor.Obf.exe	2424	0	1	0	0
a8189.Backdoor.Obf.exe	8348	0	1	0	0
c1727.Backdoor.Obf.exe	7712	0	1	0	0

ÁRBOL DE PROCESOS:

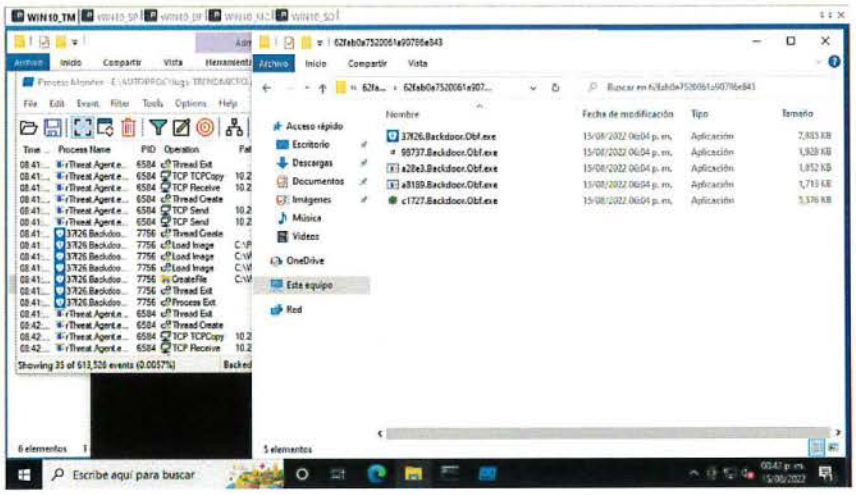
37f26.Backdoor.Obf.exe (7756)
37f26.Backdoor.Obf.exe (10076)
98737.Backdoor.Obf.exe (6468)
a28e3.Backdoor.Obf.exe (2424)
a8189.Backdoor.Obf.exe (8348)
c1727.Backdoor.Obf.exe (7712)

Synaptics Pointing Device Driver

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.38. Trend Micro Adware

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
walliant.exe	6428	4.375	6	0	1,137
3e1c3.Adware.Obf.exe	5244	0	1	0	0
88aac.Adware.Obf.exe	9680	0	1	0	0
820e6.Adware.Obf.exe	10144	0	1	0	0
9637b.Adware.Obf.exe	9328	0	1	0	0
62043.Adware.Obf.exe	1656	0	1	0	0
a39af.Adware.Obf.exe	7792	0	1	0	0

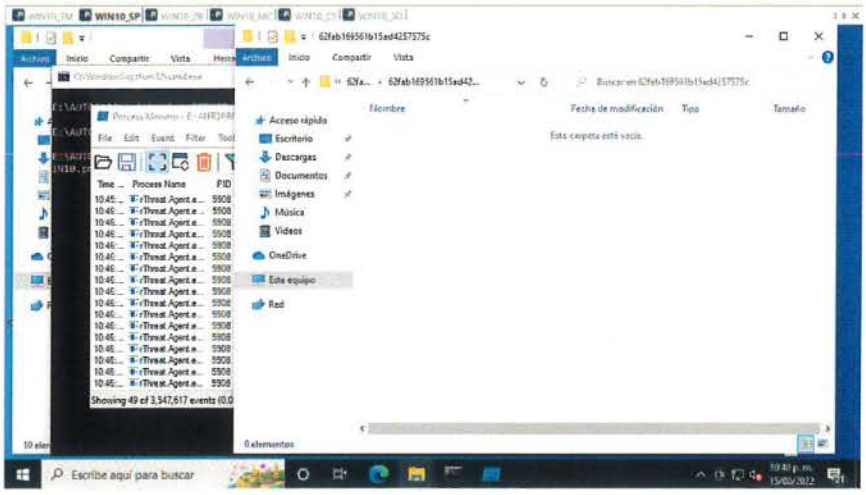
ÁRBOL DE PROCESOS:

3e1c3.Adware.Obf.exe (5244)	
88aac.Adware.Obf.exe (9680)	
820e6.Adware.Obf.exe (10144)	
9637b.Adware.Obf.exe (9328)	COMODO Internet Security
62043.Adware.Obf.exe (1656)	FileDescription
a39af.Adware.Obf.exe (7792)	
walliant.exe (6428)	Walliant

CONEXIONES A INTERNET

Total Events	Send Bytes	Receive Bytes	Other	Path	N° De detecciones como malicioso
30	966	6,964	8	104.16.124.96:443	1
550	72,480	27,118	127	104.21.83.110:443	0
337	3,856	23,935	137	104.47.57.161:25	1
2	0	0	0	13.107.42.14:443	1
8	0	450	2	18.209.118.139:25	1
152	8,978	3,135	45	47.43.18.9:25	1
29	617	10,956	10	59.82.31.244:443	1
3	0	31	1	66.225.237.157:443	0
26	4,001	6,538	6	99.86.74.49:443	0

CAPTURA DE PANTALLA:



15.39. Trend Micro PUP

INFORMACIÓN GENERAL:

Los ficheros que no fueron bloqueados al momento de la ejecución son los siguientes:

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
13f6b.PUP-PUA.exe	1492	0.14	634	555	0
13f6b.PUP-PUA.tmp	8988	0.16	1,059	4,575	0
13f6b.PUP-PUA.exe	6064	0.14	630	534	0
13f6b.PUP-PUA.tmp	8608	1.64	3,403	7,345	0
TaskHelper.exe	1276	0.02	466	602	0
Conhost.exe	3204	0.06	106	464	0
regsvr32.exe	32	0.00	346	496	0
regsvr32.exe	5756	0.00	340	668	0
13f6b.PUP-PUA.Obf.exe	4072	0.00	1	0	0
45ddd.PUP-PUA.exe	4728	0.22	814	561	0
45ddd.PUP-PUA.tmp	8224	1.22	2,592	11,355	20
walliant.exe	6428	1.84	6,053	19,300	1,948
1391e.PUP-PUA.Obf.exe	4772	0.00	1	0	0
1391e.PUP-PUA.Obf.F.exe	216	0.00	1	0	0
c3ee7.PUP-PUA.exe	9576	0.00	1	0	0
Conhost.exe	3204	0.00	49	251	0
Conhost.exe	8988	0.00	49	251	0

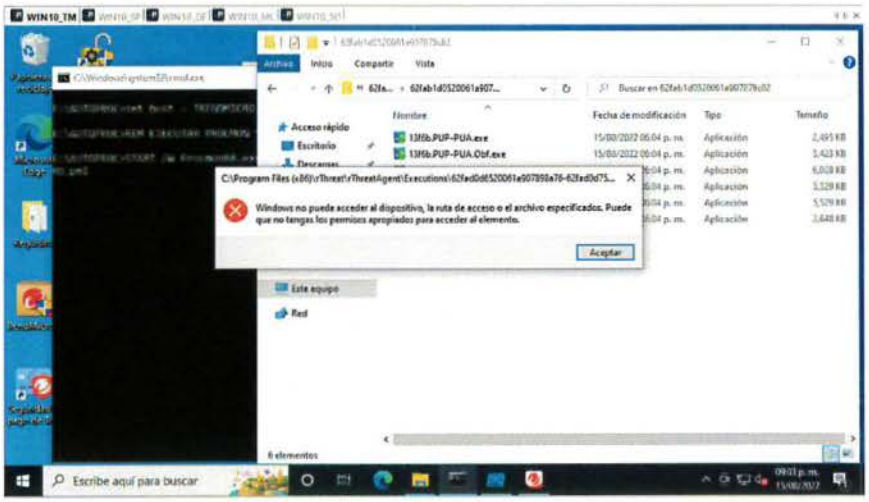
ÁRBOL DE PROCESOS:

13f6b.PUP-PUA.exe (1492)	IObit Unlocker Setup
13f6b.PUP-PUA.tmp (8988)	Setup/Uninstall
13f6b.PUP-PUA.exe (6064)	IObit Unlocker Setup
13f6b.PUP-PUA.tmp (8608)	Setup/Uninstall
TaskHelper.exe (1276)	
Conhost.exe (3204)	Host de ventana de consola
regsvr32.exe (32)	Microsoft(C) Register Server
regsvr32.exe (5756)	Microsoft(C) Register Server
13f6b.PUP-PUA.Obf.exe (4072)	IObit Unlocker Setup
45ddd.PUP-PUA.exe (4728)	Walliant Setup
45ddd.PUP-PUA.tmp (8224)	Setup/Uninstall
walliant.exe (6428)	Walliant
1391e.PUP-PUA.Obf.exe (4772)	IDM Patch 6.41.2 Installation
1391e.PUP-PUA.Obf.F.exe (216)	IDM Patch 6.41.2 Installation
c3ee7.PUP-PUA.exe (9576)	Linkvertise GmbH & Co. KG

CONEXIONES A INTERNET

Total Events	Send Bytes	Receive Bytes	Other	Path	N° De detecciones como malicioso
29	966	6,965	8	104.16.123.96:443	1
57	2,284	12,086	17	104.21.57.77:443	0
850	663,656	16,341	50	104.21.83.110:443	0
568	2,648	325,561	214	142.251.34.163:443	0
447	2,439	276,549	159	142.251.34.35:443	0
8	8	221	2	144.160.159.22:25	1
9	472	1,478	2	72.21.91.29:80	1

CAPTURA DE PANTALLA:



15.40. Trend Micro Trojan

INFORMACIÓN GENERAL:

Todos los procesos fueron cortados por trendmicro al momento de la ejecución

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
096e33.Trojan.Obf.exe	4448	0	1	0	0
379b6.Trojan.Obf.exe	3472	0	1	0	0
0454c.Trojan.Obf.exe	1208	0	1	0	0
73854.Trojan.Obf.exe	4856	0	1	0	0

ÁRBOL DE PROCESOS:

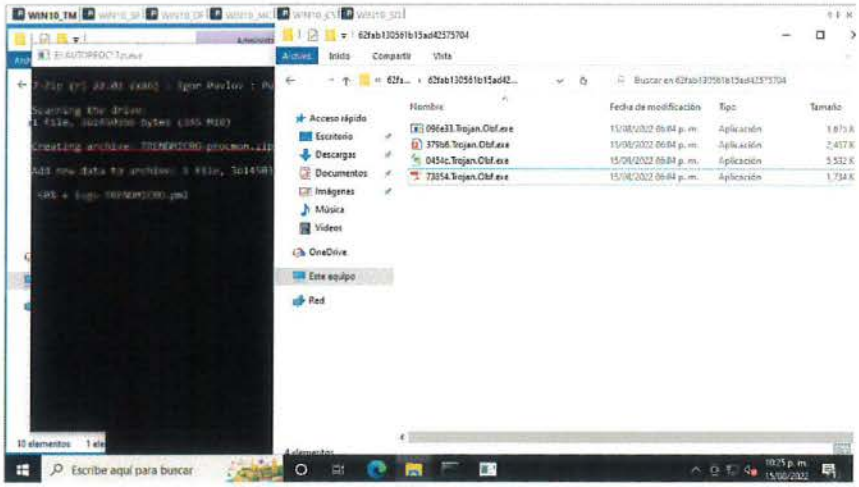
096e33.Trojan.Obf.exe (4448)
379b6.Trojan.Obf.exe (3472)
0454c.Trojan.Obf.exe (1208)
73854.Trojan.Obf.exe (4856)

ElophantClient
Digitalne dnevne ponude

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



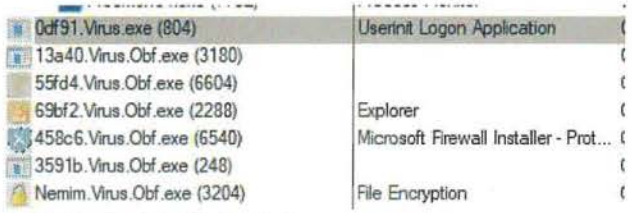
15.41. Trend Micro Virus

INFORMACIÓN GENERAL:

Todos los procesos fueron cortados por trendmicro al momento de la ejecución

Process Name	PID	CPU	File Events	Registry Events	Network Bytes
0df91.Virus.exe	804	0	1	0	0
13a40.Virus.Obf.exe	3180	0	1	0	0
55fd4.Virus.Obf.exe	6604	0	1	0	0
69bf2.Virus.Obf.exe	2288	0	1	0	0
458c6.Virus.Obf.exe	6540	0	1	0	0
3591b.Virus.Obf.exe	248	0	1	0	0
Nemim.Virus.Obf.exe	3204	0	1	0	0

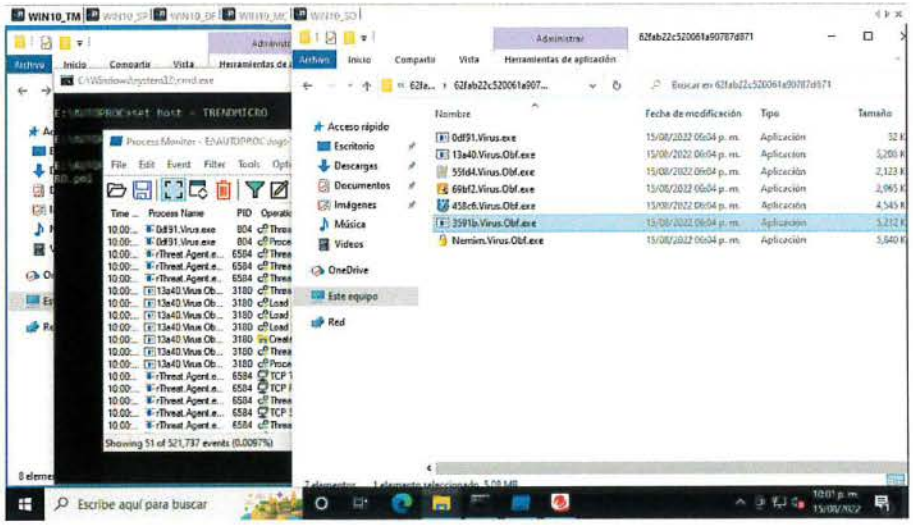
ÁRBOL DE PROCESOS:



CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.42. Trend Micro Ransomware Nokoyawa

INFORMACIÓN GENERAL:

El Ransomware no logró hacer cambios, al momento de la ejecución fue cortado por Trend Micro.

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
Nokoyawa.Ransom.Obf.exe	8416	0	1	0	0

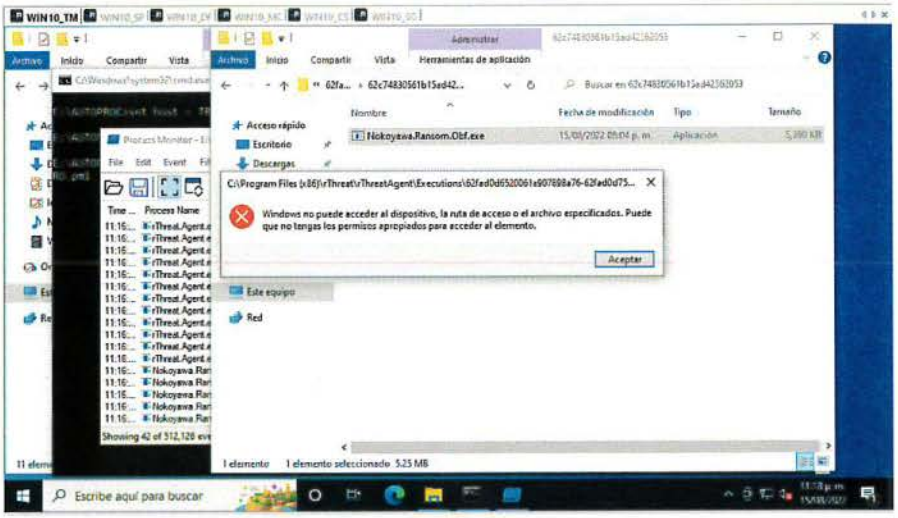
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



15.43. Trend Micro Ransomware Ghost

INFORMACIÓN GENERAL:

El Ransomware no logró hacer cambios, al momento de la ejecución fue cortado por Trend Micro.

Process Name	PID	CPU %	File Events	Registry Events	Network Bytes
HolyGhost.Ransom.Obf.exe	10084	0	1	0	0

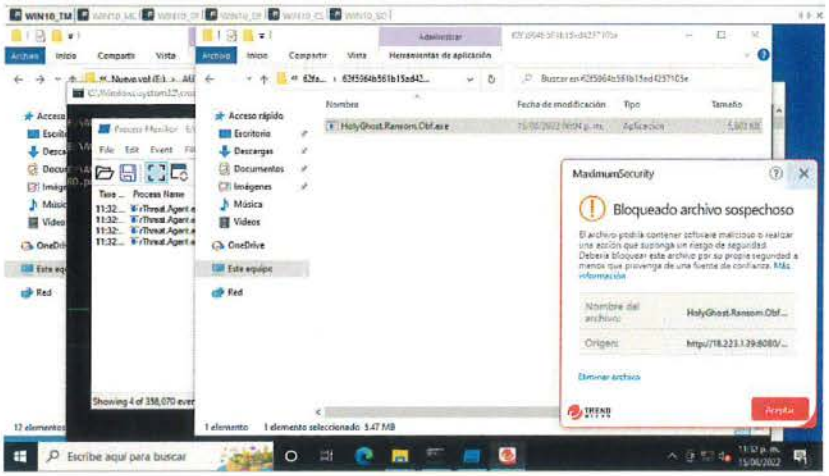
ÁRBOL DE PROCESOS:

NA

CONEXIONES A INTERNET

NA

CAPTURA DE PANTALLA:



ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

INSTITUTO FEDERAL DE TELECOMUNICACIONES

INSURGENTES SUR 1143, COL. NOCHEBUENA,
DEMARCACIÓN TERRITORIAL BENITO JUÁREZ,
C.P. 03720, CIUDAD DE MÉXICO.
TEL: 55 5015 4000 - 800 2000 120
WWW.IFT.ORG.MX