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 AMENAZA A LA SEGURIDAD NACIONAL

JULIO 2020 – JUNIO 2021

ift
INSTITUTO FEDERAL DE TELECOMUNICACIONES

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 2020 - Junio 2021**. Los resultados de los estudios e investigaciones tienen como 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.

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 los servicios de mayor penetración a nivel mundial, constituyéndose 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 y 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.

Octavo. El 11 de marzo de 2020, la Organización Mundial de la Salud calificó al brote del nuevo coronavirus como una "pandemia", debido a que la cantidad de casos de personas infectadas con el coronavirus se habían incrementado significativamente. El día 19 de marzo de 2020, el Consejo de Salubridad General acordó que el COVID-19 es una enfermedad grave y de atención prioritaria en México.

En consistencia con las recomendaciones del Gobierno Federal en materia de sana distancia y para prevenir una mayor propagación del virus en lugares concurridos, como lo son el edificio sede de este Instituto y sus sedes alternas, a efecto de proteger el derecho humano a la salud de todas las personas servidoras públicas del Instituto o aquellas que acudan a sus instalaciones, publicó el 31 de marzo de 2020 en el DOF, el "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones declara la suspensión de labores por causa de fuerza mayor, con motivo de las medidas de contingencia de la pandemia de coronavirus COVID-19 y determina las funciones esenciales a cargo del propio Instituto, **cuya continuidad deberá garantizarse para coadyuvar, en su ámbito de competencia, en la mitigación y control de los riesgos para la salud que implica la enfermedad por el virus SARS-COV2 (COVID-19)"** así como sus subsecuentes Acuerdos modificatorios de fechas 7 de abril y 29 de abril del mismo año.

El 8 de mayo del 2020, el IFT publicó en el DOF el "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones **declara la suspensión de labores por causa de fuerza mayor, con motivo de las medidas de contingencia por la pandemia de coronavirus COVID-19**, y determina las funciones esenciales a cargo del propio Instituto para garantizar la continuidad y calidad en la prestación de los servicios de telecomunicaciones y radiodifusión", y posteriormente su Acuerdo modificatorio el 5 de junio del mismo año.

Noveno. El 3 de julio del 2020, el IFT publicó en el DOF el "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"**.

Por lo anteriormente mencionado, se presenta el siguiente Informe Anual de Resultados del Comité Especializado de Estudios e Investigaciones, para el periodo julio 2020 a julio 2021.

A) Sesiones ordinarias.

Del mes de junio de 2020 a julio de 2021 se llevaron a cabo de manera remota y por medios electrónicos cinco sesiones ordinarias. 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 cinco 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	Sesión de trabajo	Medio por el cual se llevó a cabo la reunión
Vigésima Cuarta reunión ordinaria	13 de agosto de 2020	11:00 a 14:00 horas.	De manera remota por medios electrónicos
Vigésima Quinta reunión ordinaria	15 de octubre de 2020		
Vigésima Sexta reunión ordinaria	17 de diciembre de 2020		
Vigésima Séptima reunión ordinaria	18 de febrero de 2021		
Vigésima Octava sesión ordinaria	22 de abril de 2021		

B) Estudios Concluidos en el periodo

En el período reportado, los integrantes del Comité presentaron dos estudios:

1) El primero de ellos, titulado **"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. CUARTA EDICIÓN"**, es una actualización del trabajo que se ha venido desarrollando, y que permite monitorear a través del tiempo la evolución del problema que trata, y que ahora se presenta con datos del 2020; fue realizado por Asociación Nacional de Telecomunicaciones (ANATEL), en representación de los Autorizados y Concesionarios que representa en el seno del Comité.

2) El segundo estudio, titulado **"ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE INFORMACIÓN"**, fue desarrollado por el grupo formado por MAXCOM TELECOMUNICACIONES S.A. DE C.V., AXTEL, S.A.B. DE C.V., AVANTEL S. DE R.L. 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, CABLE Y COMUNICACIÓN DE CAMPECHE S.A. DE C.V., TV CABLE DE ORIENTE S.A. DE C.V., TELE AZTECA S.A. DE C.V., CABLEVISIÓN RED S.A. DE C.V., TELEVISIÓN INTERNACIONAL S.A. DE C.V., BESTPHONE S.A. DE C.V., OPERBES S.A. DE C.V, MÉXICO RED DE TELECOMUNICACIONES DEL NORTE S.A. DE C.V., COMUNICABLE S.A. DE C.V. Y TELECABLE DE MATEHUALA, 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 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. El texto íntegro de ambos estudios puede consultarse en el Anexo II.

c) Estudios en proceso

Actualmente los integrantes del Comité de Estudios se encuentran en proceso de elaboración de dos estudios, a saber:

1) Estudio en materia de ciberseguridad y privacidad de la información. Recomendaciones de medidas para la concientización de usuarios finales de servicios de telecomunicaciones en materia de seguridad de información. Elaborado por los concesionarios Axtel, S.A.B. de C.V., Alestra Servicios Móviles S.A. de C.V, Marcatel Com, S.A. de C.V., Maxcom Telecomunicaciones, S.A.B. de C.V., Grupo Televisa y Megacable Comunicaciones de México, S.A. de C.V., Directo Telecom, S.A. de C.V. y Celmax Móvil, S.A. de C.V.

2) "Estudio estadístico del número de terminales móviles, de llamados de móviles y de casetas telefónicas públicas que operan dentro de una muestro de penales en el país. Quinta edición", investigación que presenta la ANATEL.

ANEXO I

ACTAS DE LAS SESIONES

Fecha, 13 de agosto de 2020

ACTA RELATIVA A LA VIGÉSIMA CUARTA 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 agosto del año dos mil veinte, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la Vigésima Cuarta 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 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 3 de julio de 2020, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

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

   La Presidenta del Comité Especializado, Rebeca Escobar Briones, solicitó la presentación de los asistentes, a efecto de verificación del quórum.

   En uso de la palabra el Secretario del Comité Especializado, Ricardo Morán González, mencionó que se registró una asistencia a la sesión de 16 representantes de Concesionarios y Autorizados, por lo que se tiene el quórum 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 Presidenta del Comité Especializado dio inicio a 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. Exposición de los avances de los estudios en proceso.
   - Estudio en materia de ciberseguridad y privacidad de información. Responsables: MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.
   - Estudio estadístico del número de terminoles móviles y de llamadas de móviles y de casetas telefónicos públicas que operan dentro de una muestra de penoles en el país. Responsable: ANATEL.
5. Informe de la integración del informe de Resultados del Comité.
6. Asuntos Generales.

3. Aprobación del Orden del Día

El Orden del día se aprobó por unanimidad en los términos presentados.

4. Exposición de los avances de los estudios en proceso.

En uso de la palabra la Presidenta del Comité Especializado solicitó a los Concesionarios y Autorizados presenten los avances de los estudios en desarrollo para el período 2019-2020, así como los objetivos, campo de aplicación y estructura básica de los mismos, con el propósito de dar claridad a los referidas estudios.

Los Concesionarios y Autorizados presentaron ante los miembros del Comité el avance de sus estudios en desarrollo para el periodo 2019-2020 que son los siguientes:

1. **Nombre del estudio:** "ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE INFORMACIÓN".
   Responsable: El grupo integrado por MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.

   El representante comentó que se encuentran en la última etapa del estudio en desarrollo y están recabando información de los concesionarios y ya se encuentran en la etapa final. En la siguiente sesión del Comité prevén circular el estudio para recibir comentarios de los miembros de este comité. Asimismo, comento que tienen un avance de entre el 80 al 85%.

   ANATEL comentó que están preocupados y en espera de los textos del estudio ya que este será presentado al Congreso de la Unión.

   IZZI comentó que están siendo muy cuidadosos en el contenido del estudio asimismo están cuidando que no incluya cargas que no puedan cumplir los concesionarios.

2. **Nombre del estudio:** "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 – CUARTA EDICIÓN".
   Responsable: ANATEL.

   El representante mencionó que tienen un avance del 100% para telefonía móvil y un 80% para telefonía fija del estudio en desarrollo. Asimismo, comento que los resultados muestran un retroceso respecto de los estudios anteriores. Además, comento que consideran que los inhibidores no están funcionando en los penales e insta al Instituto a realizar una vigilancia y en su caso sancionar o aquellos que están incumpliendo.

   Asimismo, la Presidenta del Comité Especializado solicitó a ANATEL enviar el estudio ya integrado a más tardar el 1 de septiembre del presente, al correo del Secretario Técnico para poderlo circular al resto de los miembros y así emitir, en su caso, comentarios al respecto.

5. **Informe de la integración del Informe de Resultados del Comité.**

La versión final del informe anual de resultados del Comité del periodo julio 2019 – junio 2020 se hará circular entre todos los miembros del Comité para la recepción de comentarios. Este envío se realizará mediante correo electrónico el lunes próximo (17 de agosto) y se establece como

fecha límite para la recepción de comentarios el lunes 31 de agosto de 2020. Pasado este periodo y con la integración de los comentarios del Comité, se procederá a iniciar el proceso para el envío del informe a las autoridades correspondientes.

6. Asuntos Generales.

El Secretario técnico, reitero la petición a los miembros del Comité relativo a que deberán ratificar su participación mediante un formato que fue circulado mediante el correo electrónico del Secretario Técnico.

ACUERDOS GENERALES.

PRIMERO. Los Concesionarios y Autorizados del grupo encabezado por el grupo integrado por MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA, mencionaron que se encuentron en la última etapa del estudio en desarrollo. Señalaron que en la siguiente sesión del Comité prevén circular el estudio para recibir comentarios.

SEGUNDO. El representante de los Concesionarios y Autorizados del grupo encabezado por la ANATEL, señaló que tienen un avance del 100% para telefonía móvil y un 80% para telefonía fija del estudio en desarrollo. ANATEL enviará el avance del estudio hasta el momento, al correo del Secretario Técnico para poderlo circular al resto de los miembros y así emitir, en su caso, comentarios al respecto.

TERCERO. La versión final del informe anual de resultados del Comité del periodo julio 2019 – junio 2020 se hará circular entre todos los miembros del Comité para la recepción de comentarios. Este envío se realizará mediante correo electrónico el lunes 17 de agosto y se establece como fecha límite para la recepción de comentarios el lunes 31 de agosto de 2020. Pasado este periodo y con la integración de los comentarios del Comité, se procederá a iniciar el proceso para el envío del informe a las autoridades correspondientes.

CUARTA. Los miembros del Comité deberán ratificar su participación mediante un formato que fue circulado mediante el correo electrónico del Secretario Técnico.

QUINTA. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de octubre de 2020, a las 11:00 horas por el medio que el Instituto establezca.

7. Cierre de la sesión.

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 15 de octubre de 2020, a las 11 horas.

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

Siendo las 12:42 horas del día 13 de agosto de 2020 se dio por terminada la Vigésima Cuarta 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

Ricardo Moran Gonzalez

Ricardo Moran Gonzalez
Secretario técnico del Comité

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

Lista de asistencia de la Vigésima Cuarta Reunión Ordinaria del Comité Especializado - 13 de agosto de 2020

1	Gabriel Szekely	*gabriel szekely*	szek@yahoo.com	ANATEL
2	Kathia Garcia	*Kathia Garcia*	kgarcia@anatel.org.mx	ANATEL
3	Alejandro Rodriguez	*Alejandro Rodriguez*	arodriguezm@axtel.com.mx	Axtel
4	Hugo Martinez	*Hugo Mtz. - CANIETI*	admin@canieti.mx	CANIETI
5	Oscar Reyes	*Oscar Reyes*	oreyes@vobitelecom.com	Calmex Móvil
6	Klaus de Uranga Langer	*Klaus de Uranga Langer*	ku@clear.com.mx	Clear com comunicaciones
7	Georgina Reyes	*GEORGINA REYES*	georgina.reyes@directo.com	Directo Telecom
8	Rafael Gómez Martínez	*Rafael Gómez Martínez*	gogatel@gogatel.mx	Gogatel
9	Jose Martin Figueroa	*Jose Martin Figueroa*	mfigueroa@hkmexico.com	HK México
10	Rebeca Escobar	*rebeca.escobar*	rebeca.escobar@ift.org.mx	IFT
11	Ricardo Moran	*ricardo.moran*	ricardo.moran@ift.org.mx	IFT
12	Rodrigo Jimenez	*Rodrigo Jimenez*	rodrigo.jimenez@ift.org.mx	IFT
13	Oscar Cruz	*oscar.cruz*	oscar.cruz@ift.org.mx	IFT
14	Sergio Vázquez	*sergio.vazquez*	sergio.vazquez@ift.org.mx	IFT
15	Jorge Alberto Velázquez	*Jorge Alberto Velázquez Olvera*	jorge.velazquez@ift.org.mx	IFT
16	José Luis Cuevas	*jose.cuevas*	jose.cuevas@ift.org.mx	IFT
17	Amador Ramón Pérez	*Ramón Pérez Amador*	rperezm@tzi.mx	tzi
18	Francisco Clairin	*francisco clairin*	fclairin@tzi.mx	tzi
19	Jose Luis Cruz Velazquez	*Lic. Jose Luis Cruz Velazquez*	mexnex2@konecte.mx	Konecte de México
20	Nancy Hernández	*NANCY*	nancy.hernandez@banda-ancha.com.mx	Logitel
21	Daniel Castañeda	*Daniel Castañeda | Marcatel*	dcastaneda@marcatel.net	Marcatel
22	Susana Morales	*Susana Morales/ Marcatel*	practjuridico@marcatel.net	Marcatel
23	Alberto Alfaro Ramirez	*Alberto Alfaro Ramirez*	aalfaro@maxcom.com	Maxcom
24	Carlos Manzano	*Carlos*	carlosmanzano@maxcom.com	Maxcom
25	Raúl Ramírez Paniagua	*Raúl Ramírez Paniagua*	ramirez@maxcom.com	Maxcom
26	Sofía Guerrero	*Sofía Guerrero (Maxcom)*	sguerrero@maxcom.com	Maxcom
27	Juan Gonzalez	*Juan Gonzalez*	jgonzalez@mcmtelecom.com.mx	MCM Telecom
28	Raúl Jauregui	*RAUL JAUREGUI*	RAUL.JAUREGUI@SECNESYS.COM	Secnesys
29	Omar Palmas	*omar.palmas*	omar.palmas@tselectron.com	Tselectron
30	Oscar Aranda	*oscar.aranda*	oscar.aranda@americamovil.com	Telcel
31	Miguel Jorge Luis Calderón	*M Calderon*	mcalderon@telefonica.com	Telefónica
32	Ana de Sarracho	*ANA DE SARACHO*	ana.desaracho@telefonica.com	Telefónica
33	Celia Castillo	*CCASTILL*	ccastill@telmexmasi.com	Telmex
34	Esteban Morales	*EMGRUNER*	emgruner@telmex.com	Telmex
35	Fernanda Quiroz	*Fernanda Quiroz*	maria.quiroz@tokamovil.mx	Toka Internacional
36	Daniel Urbina	*Daniel Urbina*	hurbina@totalplay.com.mx	Total Play

Fecha: 15 de octubre de 2020

ACTA RELATIVA A LA VIGÉSIMA QUINTA 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 quince de octubre del año dos mil veinte, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la Vigésima Quinta 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 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 3 de julio de 2020, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

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

   La Presidenta del Comité Especializado, solicitó la presentación de los asistentes, a efecto de verificación del quórum.

   En uso de la palabra el Secretario del Comité Especializado, mencionó que se registró una asistencia a la sesión de 12 representantes de Concesionarios y Autorizados, por lo que se tiene el quórum necesario para declarar válida la presente sesión.

Fecha: 15 de octubre de 2020

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 Presidenta del Comité Especializado dio inicio a 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. Información de la integración y envío del Informe de Resultados del período julio 2019- junio 2020.
5. Actualización de los avances de los estudios en proceso.
   - Estudio en materia de ciberseguridad y privacidad de información.
     Responsables: MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.
   - 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.
6. Recordatorio de la elaboración de nuevas propuestas de estudio para el período Julio 2020-junio 2021.
7. Informe de la fecha de la siguiente Sesión Ordinaria del Comité.
8. Asuntos Generales.

3. Aprobación del Orden del Día

El Orden del día se aprobó por unanimidad en los términos presentados.

4. Información de la integración y envío del Informe de Resultados del período julio 2019- junio 2020.

Fecha: 15 de octubre de 2020

La presidenta del Comité informó que fue integrado, aprobado y entregado a las siguientes dependencias: Instituto Federal de Telecomunicaciones, Secretaria de Gobernación, Cámara de Diputados y Senado de la Republica.
Lo anterior en cumplimiento a lo previsto en el artículo 190, fracción XII, de la Ley Federal de Telecomunicaciones y Radiodifusión, y las disposiciones Quincuagésima y Quincuagésima Cuarta de los Lineamientos de Colaboración en Materia de Seguridad y Justicia, publicados en el Diario Oficial de la Federación el 02 de diciembre de 2015

5. Actualización de los avances de los estudios en proceso.

En uso de la palabra la Presidenta del Comité Especializado solicitó a los Concesionarios y Autorizados presenten la actualización de los avances de los estudios en desarrollo correspondientes al período julio 2019- junio 2020, con el propósito de dar una actualización de los referidos estudios.

Los Concesionarios y Autorizados presentaron ante los miembros del Comité el avance de sus estudios en desarrollo del período julio 2019- junio 2020, que son los siguientes:

1. **Nombre del estudio:** "ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE INFORMACIÓN".
   Responsable: El grupo integrado por MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.

   El representante de Axtel comentó que tienen un avance 100%, por lo que se considera concluido y fue revisado por los concesionarios responsables del estudio y se compartirá el estudio por los medios oficiales. El estudio se presentará en formato de documento, así como en presentación ejecutiva, la cual fue presentada ante los miembros del Comité la actualización de dicho estudio.

   Konecta de México, comentó que considera que el estudio es mayormente de ámbito administrativo, más que técnico.
   A lo cual Axtel respondió que efectivamente es un estudio de recomendaciones de carácter administrativo y legal, así como enfocado a la mitigación de ciberataques, así como también buenas prácticas sobre seguridad cibernética.
   Telcel felicitó a los integrantes del grupo MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA por su estudio.
   La Presidenta comentó que, en función de lo presentado, le parece adecuado el contenido tal como las recomendaciones que se encuentran dentro del marco legal mexicano.

Señalaron que compartirá dicho estudio el día 16 de octubre, al correo del Secretario Técnico en formato de documento y presentación ejecutiva, los cuales serán circulados mediante correo electrónico el día 16 de octubre, para recibir comentarios de los miembros del Comité.

2. **Nombre del estudio:** "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 – CUARTA EDICIÓN".
Responsable: ANATEL.

La representante mencionó que el estudio se encuentra concluido.

ANATEL presento el estudio final del estudio a los miembros del Comité, mismo que se puso a consideración para comentarios, durante el periodo de comentarios no se recibieron comentarios al respecto.

El representante del IFT enviaría comentarios de forma para mejorar y robustecer el estudio. Asimismo, la Presidenta del Comité Especializado solicitó a ANATEL enviar el estudio integrado a más tardar en una semana posterior a esta reunión, al correo del Secretario Técnico para poderlo circular al resto de los miembros.

6. **Recordatorio de la elaboración de nuevas propuestas de estudio para el período Julio 2020-junio 2021.**

La Presidenta del Comité realizó una invitación extensiva a todos los asistentes a que se incorporen otros operadores a la realización de estudio.

El Secretario Técnico del Comité, recordó lo señalado en los Lineamientos de Colaboración en materia de Seguridad y Justicia referente a dichas propuestas las cuales deben estar alineadas al objetivo del Comité, e indicó la necesidad de la participación activa de todos los Concesionarios y Autorizados.

El Secretario Técnico del Comité invito a los presentes que no estén integrados en alguno de los grupos de ANATEL o MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA, el envío de nuevos temas de investigación.

Fecha: 15 de octubre de 2020

7. Informe de la fecha de la siguiente Sesión Ordinaria del Comité.

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de diciembre de 2020, a las 11 horas.

8. Asuntos Generales.

Sin asuntos generales.

ACUERDOS GENERALES

PRIMERO. Los Concesionarios y Autorizados del grupo integrado por MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA, mencionaron que el estudio se encuentra concluido al 100%. Señalaron que compartirá dicho estudio el día 16 de octubre, al correo del Secretario Técnico en formato de documento y presentación ejecutiva, los cuales serán circulados mediante correo electrónico a más tardar el día 16 de octubre, para recibir comentarios de los miembros del Comité.

SEGUNDO. El representante de los Concesionarios y Autorizados del grupo encabezado por la ANATEL, señaló que tienen un avance del 100% del estudio, por lo cual se considera concluido. ANATEL enviará nuevamente el estudio con, en su caso, las consideraciones de mejora propuestas, al correo del Secretario Técnico al cabo de una semana posterior a esta reunión para poderlo circular posteriormente al resto de los miembros y así emitir, en su caso, comentarios al respecto.

TERCERO. La Presidenta del Comité solicitó a ANATEL y al grupo integrado de MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA, así como al resto de los participantes del Comité sobre nuevas propuestas de estudio e investigaciones, las cuales se recibirán a más tardar el 10 de noviembre del presente año.

CUARTA. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de diciembre de 2020, a las 11:00 horas por el medio que el Instituto establezca.

9. Cierre de la sesión.

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

Siendo las 13:20 horas del día 15 de octubre de 2020 se dio por terminada la Vigésima Quinta 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.

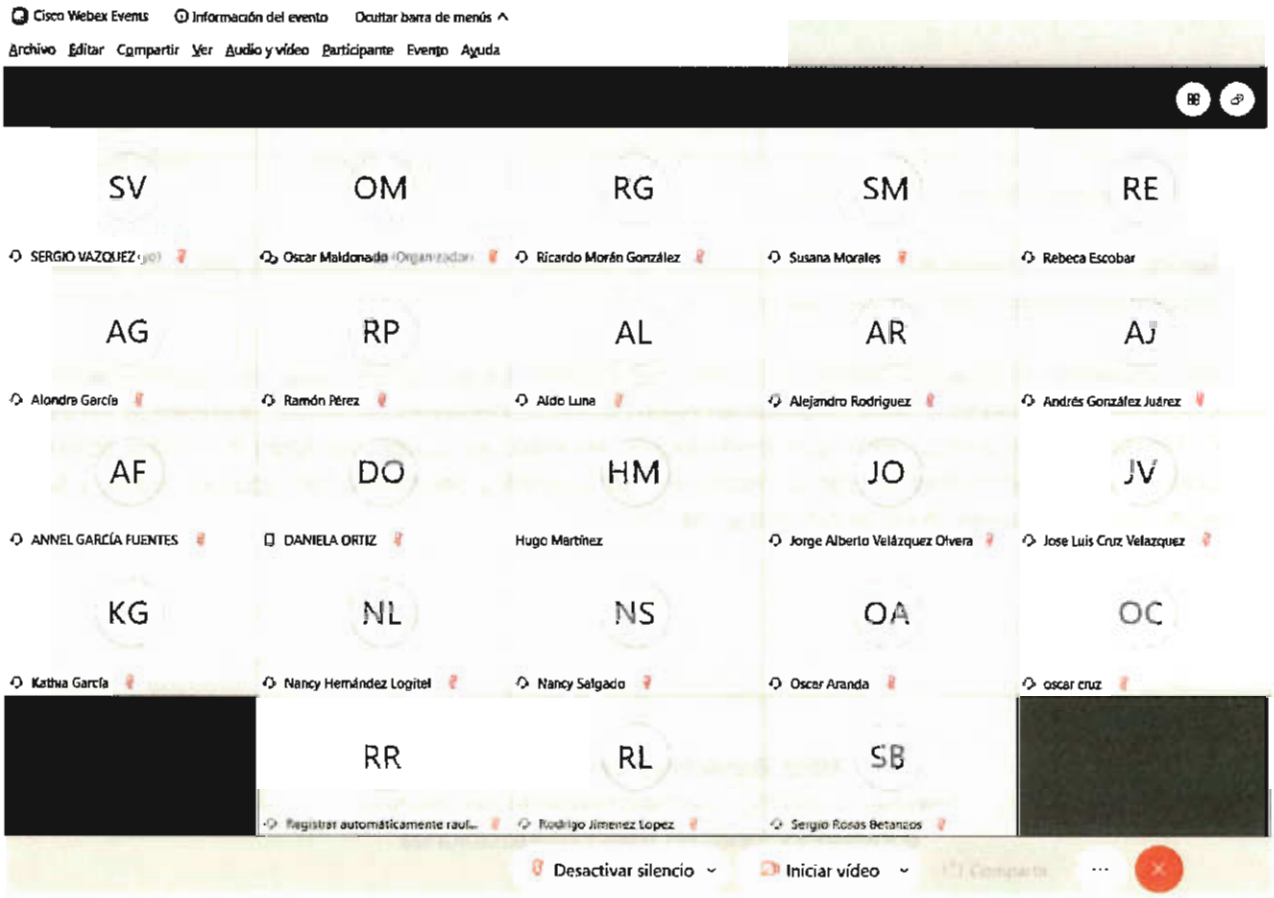
Mtra. Rebeca Escobar Briones
Presidenta del Comité Especializado de Estudios
e Investigaciones en Telecomunicaciones

Ricardo Morán González

Ricardo Moran Gonzalez
Secretario Técnico del Comité

Fecha: 15 de octubre de 2020

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



Fecha: 15 de octubre de 2020

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

Nombre del evento: *Vigésima Quinta Reunión Ordinaria del Comité Especializado* - 15 de octubre de 2020								
ID del evento: 175108022683575294								
N°	*Nombre*	*Apellido*	*Correo electrónico*	*Registrado*	*Asistido*	*ID de registro*	*Empresa*	*Teléfono*
1	Andrés	González Juárez	*andres.gonzalezj@totalsec.com.mx*	Sí	Sí	548 409	*Totalplay*	52-5574077145
2	Valeria	Hernández	*vhernandez@marcatel.net*	Sí	Sí	408 648	*Marcatel*	52-8112409162
3	Paula	Arce	*paula.arce@banda-ancha.com.mx*	Sí	No	869 346	*LOGITEL*	1-5540802334
4	Georgina	Reyes	*georgina.reyes@directo.com*	Sí	No	411 663	*Directo Telecom*	52-555537319889
5	Registrar automáticamente	cfpaniagua@marcatel.com	*cfpaniagua@marcatel.com*	Sí	No	768 034		

6	Rafael	Gomez Martinez	*rafaelgm68@hotmail.com*	Sí	No	178 275	***Gogatel***	1-555541904970
7	Nancy Hernández	Logitel	*nancy.hernandez@banda-ancha.com.mx*	Sí	Sí	597 356	***Logitel***	1-5541760657
8	Jose Manuel	Tolentino Medrano	*jt789j@att.com*	Sí	No	231 624	***AT&T***	1-5530304999
9	Aldo	Luna	*aldo.luna@siselectron.com*	Sí	Sí	342 370	***SISELECTRON***	1-5544843138
10	Registrar automáticamente	raul.jauregui@secnesys.com	*raul.jauregui@secnesys.com*	Sí	Sí	647 666		
11	CELIA	CASTILLO	*ccastill@telmexomsasi.com*	Sí	No	405 977	***TELMEX***	1-5552221751
12	Alondra	García	*agarciac@maxcom.com*	Sí	Sí	261 286	***Maxcom Telecomunicaciones, S. A. B. de C. V.***	1-5524097278
13	Hugo	Martínez	*hugo.martinez@canieti.mx*	Sí	Sí	280 231	***CANIETI***	52-5552640808

14	Fernanda	Quiroz	*maria.quiroz@tokamovil.mx*	Sí	Sí	484 901	***OpenIp Comunicaciones***	1-5536789026
15	Daniel Castañeda	Marcatel | Cca	*dcastaneda@marcatel.net*	Sí	Sí	566 568	***Marcatel / Coordinadora Carriers***	1-5547778642
16	Kathia	García	*kgarcia@anatel.org.mx*	Sí	Sí	608 091	***ANATEL***	1-2281322986
17	Laura	Juárez Ruiz	*ljuarez@mcmtelecom.com.mx*	Sí	No	369 284	***MCM TELECOM***	1-5570518822
18	Oscar	Aranda	*oscar.aranda@americamovil.com*	Sí	Sí	535 696	***Telcel***	1-5510108479
19	Ricardo	Morán González	*ricardo.moran@ift.org.mx*	Sí	Sí	352 930	***Instituto Federal de Telecomunicaciones***	52-5550154500
20	Susana	Morales	*practjuridico@marcatel.net*	Sí	Sí	455 535	***Marcatel / CCa***	1-5559042271
21	SERGIO	VAZQUEZ	*sergio.vazquez@ift.org.mx*	Sí	Sí	442 879	***IFT***	52-7821349532

Fecha: 15 de octubre de 2020

22	ANNEL	GARCÍA FUENTES	*annel.gfuentes@gmail.com*	Sí	Sí	151 165	***MEGACABLE , TV CABLE DEL GUADIANA, MYC RED, SETIT***	1-5527276284
23	Jorge Alberto	Velázquez Olvera	*jorge.velazquez@ift.org.mx*	Sí	Sí	320 634	***Instituto Federal de Telecomunicaciones***	52-5520877531
24	Rebeca	Escobar	*rebeca.escobar@ift.org.mx*	Sí	Sí	102 757	***IFT***	1-5550154814
25	Alberto	Razo	*arazo@axtel.com.mx*	Sí	Sí	811 013	***AXTEL***	1-5577234577
26	Sergio	Rosas Betanzos	*sergiorosas@masred.mx*	Sí	Sí	118 037	***MASRed Telecomunicaciones***	1-9511284330
27	Jose Luis	Cruz Velazquez	*mexmex2@konecta.mx*	Sí	Sí	265 447	***Konecta de Mexico***	52-6862210635
28	Ramón	Pérez	*rperezam@izzi.mx*	Sí	Sí	651 631	***Izzi***	1-5526908104

29	Rodrigo	Jimenez Lopez	*rodrigo.jimenez@ift.org.mx*	Sí	Sí	636 215	***IFT***	52-55 5015 4000
30	Alejandro	Rodriguez	*arodriguezra@axtel.com.mx*	Sí	Sí	733 667	***AXTEL***	1-5536140487
31	oscar	cruz	*oscar.cruz@ift.org.mx*	Sí	Sí	860 906	***Instituto Federal de Telecomunicaciones***	1-5591920368
32	DANIELA	ORTIZ	*daniela.ortiz@inaece.com*	Sí	Sí	884 710	***GUGA TELECOM, WIMOTELECOM, ALISTEL, SAYCO.***	52-5554549710

ACTA RELATIVA A LA VIGÉSIMA 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 05 minutos del día diecisiete de diciembre del año dos mil veinte, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la Vigésima 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 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 los 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 3 de julio de 2020, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

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

   La Presidenta del Comité Especializado, solicitó la presentación de los asistentes, a efecto de verificación del quórum.

   En uso de la palabra el Secretario del Comité Especializado, mencionó que se registró una asistencia a la sesión de 13 representantes de Concesionarios y Autorizados, por lo que se tiene el quórum 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 Presidenta del Comité Especializado dio inicio a 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 y aprobación del Orden del Día.
3. Se informa de la recepción de las versiones finales de los estudios elaborados durante el período actual:
   - Estudio en materia de ciberseguridad y privacidad de información.

   Responsables: MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.
   - Estudio estadístico del número de terminales móviles y de llamadas de móviles y de casetas telefónicas públicos que operan dentro de una muestra de penales en el país. Cuarta edición.

   Responsable: ANATEL.
4. Presentación de nuevos proyectos de estudio.
   - Estudio en materia de ciberseguridad y privacidad de información.

   Responsables: AXTEL, MARCATEL, MAXCOM, GRUPO TELEVISA, MEGACABLE, DIRECTO TELECOM Y CELMAX MÓVIL.
   - 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.

   Responsable: ANATEL.
5. Invitación a la elaboración de nuevas propuestas de estudio para el período julio 2020-junio 2021.
6. Presentación del calendario de reuniones para el año 2021.
7. Asuntos Generales.

El Orden del día se aprobó por unanimidad en los términos presentados.

3. Información de la integración y envío del Informe de Resultados del período julio 2019- junio 2020.

La Presidenta del Comité informó sobre la recepción de las versiones finales de los estudios elaborados durante el periodo actual:

- Estudio en materia de ciberseguridad y privacidad de información.
  Responsables: MAXCOM, MCM, IZZI, AXTEL, AVANTEL, MARCATEL y ALESTRA.

Los miembros del Comité no manifestaron cambios, modificaciones o propuestas de cambio por lo que se aprobó el estudio en su versión final.

- 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. Cuarta edición.
  Responsable: ANATEL.

Los miembros del Comité no manifestaron cambios, modificaciones o propuestas de cambio por lo que se aprueba el estudio en su versión final.

Se aprueban ambos estudios sin observaciones.

4. Presentación de nuevos proyectos de estudio.

En uso de la palabra la Presidenta del Comité Especializado solicitó a los Concesionarios y Autorizados presenten los proyectos de estudio propuestos para el siguiente periodo:

Los Concesionarios y Autorizados presentaron ante los miembros del Comité el avance de sus estudios en desarrollo del próximo período, que son los siguientes:

1. Nombre del estudio: "ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE INFORMACIÓN".
   Responsable: El grupo integrado por AXTEL, MARCATEL, MAXCOM, GRUPO TELEVISA, MEGACABLE, DIRECTO TELECOM Y CELMAX MÓVIL.

   El Secretario Técnico del Comité recordó el objeto del Comité de Estudios por lo que preguntó sobre los elementos o soluciones tecnológicas de acuerdo con el objeto del Comité. El representante mencionó que el estudio incluye información tanto para tecnología móvil como fija. Asimismo, el proyecto versa sobre habilitadores e inhibidores de concientización.
   La Presidenta del Comité solicitó que los estudios se enfoquen al objeto técnico del Comité.

Por su parte, Telcel solicitó que éste estudio no diera lugar a una sobre regulación, recalcó el fundamento de la LFTR sobre la participación de los concesionarios y autorizados de coadyuvar en materia de seguridad, además señaló la conveniencia de que no se promueva más regulaciones, que impongan obligaciones innecesarios a los concesionarios, autorizados, y regulador (IFT) por no tener este facultades en temas de datos personales.

Finalmente, la Presidenta acepta el estudio recordando el objetivo del Comité de Estudios y pide a las presentes su opinión sobre este estudio. No se recibieron comentarios al respecto, por lo que se acepta el estudio propuesto para iniciar con los avances de la metodología propuesta.
Se anexa la presentación a la presente acta.

2. **Nombre del estudio:** "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 – QUINTA EDICIÓN".
Responsable: ANATEL.

   ANATEL presentó el objeto del estudio a los miembros del Comité, mismo que se puso a consideración para comentarios.

   La Presidenta solicitó a ambas propuestas, enviar al correo del Secretario Técnico la estructura, metodología y descripción breve del estudio propuesto.

5. **Invitación a la elaboración de nuevas propuestas de estudio.**
   La Presidenta del Comité realizó una invitación extensiva a todos los asistentes a que se incorporen a la realización de estudios.

   La Presidenta del Comité le dio el uso de la palabra al Dr. José Luis Cuevas, del Centro de Estudios del IFT quien presentó algunos temas de estudio como nuevas propuestas para que los concesionarios y autorizados consideren para ser elaborados.

Invitación a la elaboración de nuevas propuestas de estudio

Título	Objetivo
Uso de infraestructura pasiva de redes públicas de telecomunicaciones, por personas no autorizadas	Establecer una metodología para conformar una estadística que permita conocer la evolución en el tiempo del uso de infraestructura pasiva de telecomunicaciones por personas no autorizadas. La infraestructura pasiva utilizada incluye torres, postes, casetas, ductos registros o cualquier otra. La información será proporcionada por la persona física o moral que sea propietaria o que administre la infraestructura de que se trate
Comisión de delitos Financieros cibernéticos	Analizar e integrar recomendaciones tecnológicas para prevenir y combatir la comisión de delitos financieros cibernéticos
Delitos y fraudes en E-comerce. Estrategias y medios tecnológicos para combatirlos	Identificación de los recursos tecnológicos disponibles en las redes de Telecomunicaciones para la prevención y combate en e-comerce
Estrategias y lineamientos de seguridad en el acceso a internet.	Describir y analizar las mecanismos de seguridad implementados por los concesionarios en el acceso a internet ofertado a los usuarios
Regulación de la privacidad de datos y seguridad en las redes de Telecomunicaciones	Llevar a cabo un análisis comparativo del marco regulatorio (normas técnicas) y mejores prácticas en seguridad y privacidad de datos en las redes de Telecomunicaciones en el mundo en relación con el vigente en México

6. Presentación del calendario de reuniones para el año 2021.

Presentación del calendario de reuniones para 2021.

Reunión	Fecha propuesta	Inicio sesión de trabajo
27°	18/02/2021	11:00 a 14:00
28°	22/04/2021	11:00 a 14:00
29°	17/06/2021	11:00 a 14:00
30°	12/08/2021	11:00 a 14:00
31°	14/10/2021	11:00 a 14:00
32°	16/12/2021	11:00 a 14:00

Sin comentarios para el calendario propuesto para las reuniones del Comité especializado para el 2021, se aprueba.

7. Asuntos Generales.

Se recibió un oficio de Konecta de México con solicitudes ante el Comité, sin embargo, al no estar disponible el representante de Konecta por problemas de salud se agendará para la próxima reunión.

ACUERDOS GENERALES

PRIMERO. Los Concesionarios y Autorizados del grupo integrado por AXTEL, MARCATEL, MAXCOM, GRUPO TELEVISA, MEGACABLE, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de información" y la ANATEL responsable del "Estudio estadística 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. Quinta edición" enviarán al correo del Secretario Técnico la estructura, metodología y descripción breve del estudio propuesto de manera formal.

SEGUNDO. Se presentaron ante miembros del Comité nuevas propuestas de estudios para ser considerados para llevarse a cabo:

Invitación a la elaboración de nuevas propuestas de estudio

Título	Objetivo
Uso de infraestructura pasiva de redes públicas de telecomunicaciones, por personas no autorizadas	Establecer una metodología para conformar una estadística que permita conocer la evolución en el tiempo del uso de infraestructura pasiva de telecomunicaciones por personas no autorizadas. La infraestructura pasiva utilizada incluye torres, postes, ductos, registros o cualquier otra. La información será proporcionada por la persona física o moral que sea propietaria o que administre la infraestructura de que se trate
Comisión de delitos financieros cibernéticos	Analizar e integrar recomendaciones tecnológicas para prevenir y combatir la comisión de delitos financieros cibernéticos
Delitos y fraudes en E-comerce. Estrategias y medidas tecnológicas para combatirlos	Identificación de los recursos tecnológicos disponibles en las redes de Telecomunicaciones para la prevención y combate en e-comerce
Estrategias y lineamientos de seguridad en el acceso a internet	Describir y analizar los mecanismos de seguridad implementados por los concesionarios en el acceso a internet ofertado a los usuarios
Regulación de la privacidad de datos y seguridad en las redes de Telecomunicaciones	Llevar a cabo un análisis comparativo del marco regulatorio (normas técnicas) y mejores prácticas en seguridad y privacidad de datos en las redes de Telecomunicaciones en el mundo en relación con el [illegible] gente en México

TERCERO. El Secretario Técnico presentó el calendario de las reuniones del próximo año 2021:

Presentación del calendario de reuniones para 2021.

Reunión	Fecha propuesta	Inicio sesión de trabajo
27°	18/02/2021	11:00 a 14:00
28°	22/04/2021	11:00 a 14:00
29°	17/06/2021	11:00 a 14:00
30°	12/08/2021	11:00 a 14:00
31°	14/10/2021	11:00 a 14:00
32°	16/12/2021	11:00 a 14:00

CUARTA. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 18 de febrero de 2021, a las 11 horas.

QUINTA. Las solicitudes de Kanecta de México ante el Comité, se agendarán para la próxima reunión.

8. Cierre de la sesión.

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

Siendo las 12:54 horas del día 17 de diciembre de 2020 se dio por terminada la Vigésima 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

Ricardo Morán González
Secretario Técnica del Comité

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

SV	OM	RG	JC	RE
OA	KG	AR	AG	AR
AJ	AF	CH	DC	FQ
FC	FV	GR	HM	JM
MS	NL	OC	OR	RG

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

Todas las sesiones en Hora estándar de México (Ciudad de México, GMT-06:00)					
Información detallada de la sesión para 'Vigésima Sexta Reunión Ordinaria del Comité Especializado':					
N°	Nombre	Correo electrónico	Fecha	Empresa	Número de teléfono
1	Kathia García	kgarcia@anatel.org.mx	17/12/2020	ANATEL	1-2281322986
2	Carlos Hirsch	ch581s@att.com	17/12/2020	AT&T	52-5555000418
3	Francisco Villafuerte	fv3730@att.com	17/12/2020	AT&T	1-5530307874
4	Jose Manuel Tolentino Medrano	jt789j@att.com	17/12/2020	AT&T	52-5530304999
5	Alberto Razo	arazo@axtel.com.mx	17/12/2020	AXTEL	1-5577234577
6	Hugo Martínez	hugo.martinez@canieti.mx	17/12/2020	Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información	1-5552640808
7	Oscar Reyes	oreyes@yobitelecom.com	17/12/2020	Celmax	52-5553202664
8	GEORGINA REYES	georgina.reyes@directo.com	17/12/2020	DIRECTO TELECOM	1-5537319889
9	Rafael Gomez	rafaelgm68@hotmail.com	17/12/2020	Gogatel	1-5541904970
10	YESSICA ALVARADO	gogatel@gogatel.mx	17/12/2020	GOGATEL, SA DE CV	1-5513533493
11	Oscar Maldonado	dgtic.externo.92@ift.org.mx	17/12/2020	IFT	
12	SERGIO VAZQUEZ	sergio.vazquez@ift.org.mx	17/12/2020	IFT	
13	Ricardo Martinez	ricardo.martinez@ift.org.mx	17/12/2020	IFT	
14	jose luis cuevas	jose.cuevas@ift.org.mx	17/12/2020	IFT	1-5510487693
15	Ricardo Morán González	ricardo.moran@ift.org.mx	17/12/2020	IFT	
16	oscar cruz	oscar.cruz@ift.org.mx	17/12/2020	IFT	
17	Rebeca Escobar	rebeca.escobar@ift.org.mx	17/12/2020	IFT	
18	Rodrigo Jimenez Lopez IFT	rodrigo.jimenez@ift.org.mx	17/12/2020	IFT	
19	Jorge Alberto Velázquez Olvera	jorge.velazquez@ift.org.mx	17/12/2020	IFT	
20	Francisco Clairin	fclairin@izzi.mx	17/12/2020	Izzi	52-5563471528
21	Ramón Pérez Izzi	rperezam@izzi.mx	17/12/2020	izzi	1-5526908104
22	Nancy Hernández Logitel	noncy.hernandez@banda-ancha.com.mx	17/12/2020	Logitel	1-5541760657
23	Daniel Castañeda Marcatel | Cca	dcastaneda@marcatel.net	17/12/2020	Marcatel | Coordinadora Corriers	1-5547778642
24	Susana Morales	practjuridico@marcatel.net	17/12/2020	Marcatel/CCa	1-5559042271

25	Andrea Marina Pedrozo Rodriguez	apedrozo@maxcom.com	17/12/2020	Maxcom	52-7773529888
26	Alondra García	agarciac@maxcom.com	17/12/2020	Maxcom Telecomunicaciones	1-5524097278
27	ANNEL GARCÍA FUENTES	annel.gfuentes@gmail.com	17/12/2020	MEGACABLE, TV CABLE DEL GUADIANA, MYC RED, SETIT	1-5527276284
28	Fernanda Quiroz	maria.quiroz@tokamovil.mx	17/12/2020	Openip comunicaciones	52-5536789026
29	RAUL JAUREGUI HIDALGO	raul.jauregui@secnesys.com	17/12/2020	Secnesys	52-8126051507
30	Jose Martin Figueroa Cardona	martín.figueroa@secnesys.com.mx	17/12/2020	Secnesys	1-8180889825
31	Oscar Aranda	oscar.aranda@americamovil.com	17/12/2020	Telcel	1-5510108479
32	Miguel Sanchez	msbarqui@telmex.com	17/12/2020	Telmex	1-5552221215
33	Andrés González Juárez	andres.gonzalezj@totalsec.com.mx	17/12/2020	Totalplay	52-5567834078

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

ACTA RELATIVA A LA VIGÉSIMA 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 05 minutos del día dieciocho de febrero del año dos mil veintiuno, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la Vigésima 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 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 motiva 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 3 de julio de 2020, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

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

   La Presidenta del Comité Especializado, solicitó la presentación de los asistentes, a efecto de verificación del quórum.

   En uso de la palabra el Secretario del Comité Especializado, mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quórum necesaria 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 Presidenta del Comité Especializado dio inicio a 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 y aprobación del Orden del Día.
3. Informe del cumplimiento del Acuerdo Primero adoptado en la Vigésima Sexta sesión del Comité.
4. Exposición de los avances de los estudios en proceso:
    a. Grupo integrado por AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de la información", y
    b. ANATEL responsable del "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. Quinta edición".
5. Se solicita a los integrantes del Comité que no están participando en algún estudio la integración de propuestas para que sean sometidas a la consideración del Comité.
6. Se informa de la fecha de la siguiente Sesión Ordinaria.
7. Asuntos Generales.

El Orden del día se aprobá por unanimidad en los términos presentados.

3. Informe del cumplimiento del Acuerdo Primero adoptado en la Vigésima Sexta sesión del Comité.

El Secretario Técnico citó el Acuerdo Primero adoptado en la Vigésima Sexta sesión del Comité:

"PRIMERO. Los Concesionarios y Autorizados del grupo integrado por AXTEL, MARCATEL, MAXCOM, GRUPO TELEVISA, MEGACABLE, DIRECTO TELECOM Y CELMAX MÓVIL

responsables del "Estudio en materia de ciberseguridad y privacidad de información" y la ANATEL responsable del "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" enviarán al correo del Secretario Técnico la estructura, metodología y descripción breve del estudio propuesto de manera formal."

Asimismo, informó que con fechas 17 de diciembre de 2020 y 11 de febrero de 2021, se recibieron respectivamente de manera formal, la estructura, metodología y descripción breve de los siguientes estudios:

- "Estudio en materia de ciberseguridad y privacidad de información".
  Responsables: Grupo integrado por AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de la información",

- "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. Quinta edición".
  Responsable: ANATEL.

4. Exposición de los avances de los estudios en proceso

La Presidenta del Comité solicitó a los representantes de los estudios propuestos, expusieran los avances:

- "Estudio en materia de ciberseguridad y privacidad de información".
  Responsables: Grupo integrado por AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de la información".

El representante de este grupo de trabajo señaló que tendrán un nuevo avance en el mes de abril del presente año.
El Secretario Técnico recordó el objetivo de los estudios que emanan del Comité Especializado.

Por otro lado, Axtel solicitó integrar a Alestra Servicios Móviles coma parte del grupo de trabajo.

Los miembros del Comité no manifestaron comentarios, preguntas, modificaciones o propuestos de cambio.

- "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. Quinta edición".
  Responsable: ANATEL.

Los representantes señalaron que se ha concluido el monitoreo en penales y se ha terminado la fase de integración de datos. Tendrán algunos resultados preliminares, así como un avance en la próxima reunión del Comité.

Los miembros del Comité no manifestaron comentarios, preguntas, modificaciones o propuestas de cambio.

Se consideran como formalmente recibidos ambos estudios sin observaciones.

4. Solicita a los integrantes del Comité que no están participando en algún estudio la integración de propuestas para que sean sometidas a la consideración del Comité.

La Presidenta del Comité realizó una invitación extensiva a todos los asistentes a que se incorporen a la realización de estudios 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.

5. Fecha de la siguiente Sesión Ordinaria

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 22 de abril de 2021, a las 11 horas.

Sin comentarios al respecto de la fecha establecida para la próxima reunión del Comité, se aprueba.

6. Asuntos Generales.

Sobre el escrito recibido el 27 de octubre de 2020, por parte de Konecta de México, se recibió una petición de su representante con fecha del 22 de enero de 2021 para retirar dicho oficio enviado ante el Comité ya que lo presentará nuevamente, más adelante.

ACUERDOS GENERALES

PRIMERO. Los Concesionarios y Autorizados del grupo integrado por AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de información" y la ANATEL responsable del "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. Quinta edición" presentaron el avance de sus estudios por lo que se consideran formalmente recibidos sin observaciones por parte de los miembros del Comité, ya que no manifestaron comentarios, preguntas, modificaciones o propuestas de cambio.

SEGUNDO. Se reiteró la invitación a los miembros del Comité para participar con nuevas propuestas de estudios.

TERCERO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 22 de abril de 2021, a las 11 horas.

CUARTA. El escrito de Konecta de México presentado el 27 de octubre de 2020 queda en calidad de retirado ante el Comité.

7. Cierre de la sesión.

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

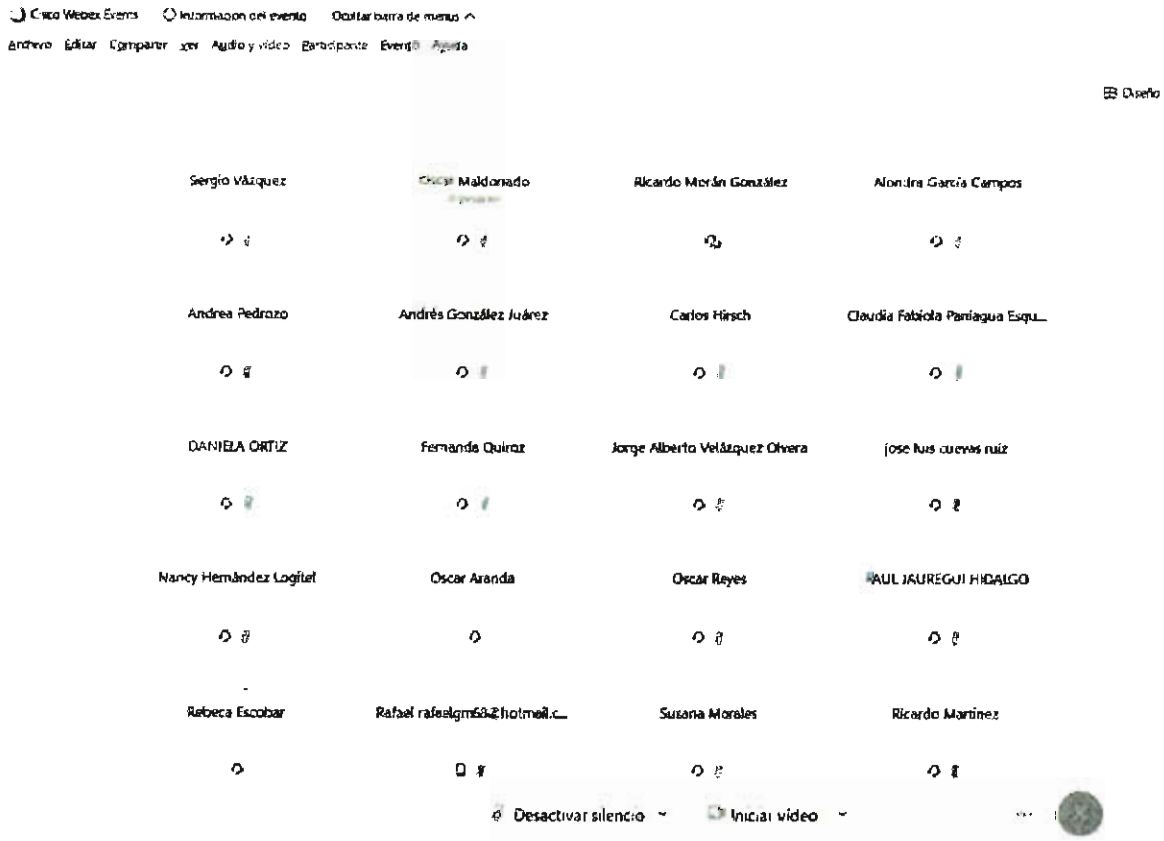
Siendo las 12:22 horas del día 18 de febrero de 2021 se dio por terminada la Vigésima Séptima Reunión Ordinaria del Comité Especializado.

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

Ricardo Morán González
Secretario Técnico del Comité

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



Fecha: 18 de febrero de 2021

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

N°	Nombre	Correo electrónico	Empresa	Número de teléfono
1	Szekely Anatel	*gszek@yahoo.com*	ANATEL	52-5514731399
2	Francisco Villafuerte	*fv3730@att.com*	AT&T	1-5530307874
3	Carlos Hirsch	*ch581s@att.com*	AT&T	52-5555000418
4	Alejandro Rodríguez	*arodriguezra@axtel.com.mx*	AXTEL	1-5536140487
5	Hugo Martínez Paz	*hugo.martinez@canieti.mx*	Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información	1-5552640808
6	Oscar Reyes	*oreyes@yobitelecom.com*	Celmax	52-5553202664
7	Daniela Ortiz	*daniela.ortiz@inaece.com*	CELMAX MÓVIL, GUGA TELECOM, WIMOTELECOM, ALISTEL	52-5554549710
8	Georgina Reyes	*georgina.reyes@directa.com*	Directo Telecom	1-5537319889
9	Rafael Rafaelgm68@Hotmail.Com	*rafaelgm68@hotmail.com*	Gogatel	52-525541904970
10	Nancy Hernández Logitel	*nancy.hernandez@banda-ancha.com.mx*	Logitel	1-5541760657
11	Claudia Fabiola Paniagua Esquive	*cfpaniagua@marcatel.net*	Marcatel / CCa	52-5537317037
12	Daniel Castañeda Marcatel | Cca	*dcastaneda@marcatel.net*	Marcatel | Coordinadora Carriers	52-5547778642
13	Susana Morales	*practjuridico@marcatel.net*	Marcatel/CCa	1-5559042271

14	Alondra García Campos	*agarciac@maxcom.com*	Maxcom Telecomunicaciones	1-5524097278
15	Andrea Pedrozo	*apedrozo@maxcom.com*	Maxcom Telecomunicaciones	1-7773529888
16	Fernanda Quiroz	*maria.quiroz@tokomovil.mx*	Openip Comunicaciones	1-5536789026
17	Raul Jauregui Hidalgo	*raul.jauregui@secnesys.com*	SECNESYS	52-8126051507
18	Oscar Aranda	*oscar.aranda@americamovil.com*	Telcel	1-5510108479
19	Ana De Saracho	*ana.desaracho@telefanica.cam*	TELEFONICA MEXICO	1-5554353030
20	Andrés González Juárez	*andres.gonzalezj@totalsec.com.mx*	Totalplay	52-5567834078
21	Rebeca Escobar	*rebeca.escobar@ift.org.mx*	IFT	1-5550154814
22	Oscar Maldonado	*dgticexterno.92@ift.org.mx*	IFT	
23	Rodrigo Jiménez López	*rodrigo.jimenez@ift.org.mx*	IFT	
24	Oscar Cruz	*oscar.cruz@ift.org.mx*	IFT	
25	Ricardo Martinez	*ricardo.martinez@ift.org.mx*	IFT	
26	Jorge Alberto Velázquez Olvera	*jorge.velazquez@ift.org.mx*	IFT	
27	Sergio Vázquez	*sergio.vazquez@ift.org.mx*	IFT	
28	Jose Luis Cuevas Ruiz	*jose.cuevas@ift.org.mx*	IFT	
29	Ricardo Morán González (Ift)	*ricardo.moran@ift.org.mx*	IFT	

La presente hoja forma parte del Acta de la Vigésima Séptima Reunión Ordinaria del Comité Especiolizado.

Fecha: 22 de abril de 2021

ACTA RELATIVA A LA VIGÉSIMA 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 05 minutos del día veintidós de abril del año dos mil veintiuno, mediante medios electrónicos (webex) proporcionados por el Instituto Federal de Telecomunicaciones (en lo sucesivo "IFT"), se llevó a cabo la **Vigésima 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 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 3 de julio de 2020, dicha Sesión se celebró de manera remota.

DESARROLLO DE LA REUNIÓN

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

   La Presidenta del Comité Especializado, solicitó la presentación de los asistentes, a efecto de verificación del quórum.

   En uso de la palabra el Secretario del Comité Especializado, mencionó que se registró una asistencia a la sesión de Concesionarios y Autorizados suficiente para contar con el quórum 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: 22 de abril de 2021

2. Lectura del Orden del Día.

La Presidenta del Comité Especializado dio inicio a la sesión y cedió lo 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. Exposición de los avances de los estudios en proceso.
   a. Grupo integrado por AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de la información".
   b. ANATEL responsable del "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. Quinta edición".
5. Participación del Ing. Gonzalo García, Director General de CLEVER TECHNOLOGIES, con la presentación "Ciberseguridad en la Industria".
6. Se informa de la fecha de la siguiente Sesión Ordinaria.
7. Asuntos Generales.

Los presentes no manifestaron temas para incluir en la Orden del día.

El Orden del día se aprobó por unanimidad en los términos presentados.

3. **Exposición de los avances de los estudios en proceso**

La Presidenta del Comité solicitó a los representantes de los estudios propuestos, expusieran los avances:

- **"Estudio en materia de ciberseguridad y privacidad de información".**
  Responsables: Grupo integrado por ALESTRA SERVICIOS MÓVILES, AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL.

  Raúl Jáuregui, representante de este grupo de trabajo presentó el avance del estudio con respecto a la reunión anterior. Asimismo, comentó que en la siguiente sesión presentaran una nueva ampliación de la propuesta de estudio, lo que significa que sería la entrega final de la información.

  El representante de Konecta preguntó ¿cuándo se atendería la parte técnica del desarrollo de aquellas herramientas que permitan materializar la propuesta de estudio? A lo que respondieron que se verá en la siguiente fase de la propuesta de estudio. Asimismo, darle amplitud a la propuesta de estudio.

  ANATEL comentó que existen lineamientos de operación del Comité y estos deben continuar siguiéndose para evitar abordar temas que desemboquen en reformas a la ley emanadas de este tipo de estudios, ya que, en muchos casos, pueden resultar costoso para los concesionarios y autorizados.

  La Presidenta del Comité, ogradeció los avances y señaló que el Comité queda atento de los siguientes puntos, incluyendo los que harán alusión a las soluciones técnicas.

  Los miembros del Comité no manifestaron ningún otro comentario, pregunta, modificaciones o propuestas de cambio.

- **"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. Quinta edición".**
  Responsable: ANATEL.

  Los representantes señalaron que se ha concluido el monitoreo en penales y se ha terminado la fase de integración de datos. Como parte del avance, mencionó resultados

preliminares, y compartirá la presentación de este estudio en los próximos días para ser compartido a los miembras del Comité, y posteriormente el documento final de su estudio.

El representante de Konecta comentó que presentará un escrito ante el Comité de Estudios.

La Presidenta, recordó que el objeto de este Comité es sobre el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualizoción de riesgos o amenazas a la seguridad nacional. Y pidió a los miembros de este, enfocar los estudios a propuestas técnicas.

Los miembros del Comité no manifestaron ningún otro comentario, pregunta, modificaciones o propuestas de cambio.

Se consideran como formalmente presentados los avances de ambos estudios.

4. **Participación del Ing. Gonzalo García, Director General de CLEVER TECHNOLOGIES, con la presentación "Ciberseguridad en la Industria".**

La Presidenta del Comité presentó al Ing. Gonzalo García, Director General de CLEVER TECHNOLOGIES, con la presentación "Ciberseguridad en la Industria". Lo anterior, con la intensión de generar nuevas propuestas de estudio para ser consideradas por los miembros del Comité.

El expositor invitado presentó lo siguiente:

- Tipos de ciberataques
- Los mas comunes
- Phishing
- Estadísticas
- En la Industria
- Pautas para protegerse
- Telecom Fraud
- Fintech e identificación biométrica
- Pronósticos

5. Fecha de la siguiente Sesión Ordinaria

La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de junio de 2021, a las 11 horas.

Sin comentarios al respecto de la fecha establecida para la próxima reunión del Comité, se aprueba.

6. Asuntos Generales.

Sin asuntos generales que atender.

ACUERDOS GENERALES

PRIMERO. Los Concesionarios y Autorizados del grupo integrado por ALESTRA SERVICIOS MÓVILES, AXTEL, MARCATEL, MAXCOM TELECOMUNICACIONES, GRUPO TELEVISA, MEGACABLE COMUNICACIONES DE MÉXICO, DIRECTO TELECOM Y CELMAX MÓVIL responsables del "Estudio en materia de ciberseguridad y privacidad de información" y la ANATEL responsable del "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. Quinta edición" presentaron el avance de sus estudios por lo que se consideran como formalmente presentados los avances de ambos estudios.

SEGUNDO. A raíz de la participación del Ing. Gonzalo García, Director General de CLEVER TECHNOLOGIES, con la presentación "Ciberseguridad en la Industria" se reiteró la invitación a los miembros del Comité para participar con nuevas propuestas de estudios.

TERCERO. ANATEL enviara una versión del estudio, para ser distribuido entre los miembros del Comité Especializado, para observaciones y comentarios.

CUARTO. La próxima reunión ordinaria del Comité Especializado se llevará a cabo el 17 de junio de 2021, a las 11 horas.

7. Cierre de la sesión.

Fecha: 22 de abril de 2021

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

Siendo las 13:30 horas del día 22 de abril de 2021 se dio por terminada la Vigésima 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

Ricardo Moran Gonzalez
Secretario Técnico del Comité

Fecha: 29 de abril de 2021

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

N°	Nombre	Apellido	correo electrónico	Empresa
1	Kathia	García	kgarcia@anatel.org.mx	ANATEL
2	Jose	Manuel Tolentino	jt789j@att.com	AT&T
3	Martha	León	ml6780@att.com	AT&T
4	Carlos	Hirsch	ch581s@att.com	AT/T
5	Alejandro	Rodriguez	arodriguezra@axtel.com.mx	AXTEL
6	Hugo	Martínez Paz	hugo.martinez@canieti.mx	CANIETI
7	Oscar	Rene Reyes Ruiz	oreyes@yobitelecom.com	CELMAX MOVIL
8	Antonio	Hernández	ovargas@clevertech.com.mx	CLEVERTECH
9	Alfredo	Florian	aflorian@clevertech.com.mx	CLEVERTECH
10	Gonzalo	Garcia Castilla	ggarcia@clevertech.com.mx	CLEVERTECH S.A. DE C.V.
11	Georgina	Reyes	georgina.reyes@directo.com	DIRECTO TELCOM
12	Rafael	Gómez	rafaelgm68@hotmail.com	GOGATEL
13	Jose	Luis Cruz	mexmex2@konecta.mx	KONECTA DE MEXICO
14	Nancy	Hernández	nancy.hernandez@banda-ancha.com.mx	LOGITEL
15	Claudia	Fobiola Paniagua Esquivel	cfpaniagua@marcatel.net	MARCATEL / CCA
16	Daniel	Castañeda	dcastaneda@marcatel.net	MARCATEL / CCA
17	Susana	Morales	practjuridico@marcatel.net	MARCATEL Y CCA
18	Alondra	García	agarciac@maxcom.com	MAXCOM TELECOMUNICACIONES Y CELMAX MÓVIL
19	Annel	García Fuentes	annel.gfuentes@gmail.com	MEGACABLE, TV CABLE DEL GUADIANA, MYC RED, SETIT
20	Fernanda	Quiroz	maria.quiroz@tokamovil.mx	OPENIP COMUNICACIONES
21	Raul	Jauregui	raul.jauregui@secnesys.com	SECNESYS
22	Michel	Herrera	michel.herrera@siselectron.com	SISELECTRON
23	Oscar	Aranda	oscar.aranda@americamovil.com	TELCEL
24	Erika	Lejsek	erika.lejsek@telefonica.com	
25	Ana	De Saracho	ana.desaracho@telefonica.com	TELEFÓNICA
26	Miguel	Sánchez	msbarqui@telmex.com	TELMEX
27	Celia	Francisca Vertiz	ccastill@telmexomsasi.com	TELMEX
28	Andres	Gonzalez Juarez	andres.gonzalezj@totalsec.com.mx	TOTALPLAY
29	Jose	Luis Cuevas	jose.cuevas@ift.org.mx	IFT
30	Virginia	Minero	virginia.minero@ift.org.mx	IFT
31	Sergio	Vazquez	sergio.vazquez@ift.org.mx	IFT
32	Rodrigo	Jimenez	rodrigo.jimenez@ift.org.mx	IFT
33	Oscar	Cruz	oscar.cruz@ift.org.mx	IFT

Fecha: 22 de abril de 2021

34	Ricardo	Morán González	ricardo.moran@ift.org.mx	IFT
35	Jorge	Velázquez	jorge.velazquez@ift.org.mx	IFT
36	Rebeca	Escobar	rebeca.escobar@ift.org.mx	IFT
37	Ricardo	Martinez	ricardo.martinez@ift.org.mx	IFT

La presente hoja forma parte del Acta de la Vigésima Octava Reunión Ordinaria del Comité Especializao.

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 MÓVILES Y DE CASETAS TELEFÓNICAS PÚBLICAS QUE OPERAN DENTRO DE UNA MUESTRA DE PENALES EN EL PAÍS. CUARTA EDICIÓN"

Estudio propuesto 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
CUARTA 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

Estudio 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.

Presentación

El estudio analizó el número de equipos celulares estimados, las tarjetas SIMs asociadas a estos, y las llamadas generadas desde una muestra de recintos penitenciaros dentro de los Estados Unidos Mexicanos. El presente estudio incorporó de manera complementaria la investigación de las llamadas provenientes de las casetas públicas ubicadas en algunos penales. 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 sus resultados.

En la primera parte, el objeto de la investigación es actualizar el estudio realizado durante 2016, 2017 y 2018 sobre el número de equipos terminales móviles estimados 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. Así mismo, 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 cobra relevancia porque esta situación afecta de manera importante 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.

> En el mes octubre 2018 entró en vigor la Disposición Técnica IFT-010-2016, la cual fue 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:
> *"Los equipos de bloqueo de señoles 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."*

Para el estudio de 2018 el periodo muestral seleccionado fue de tres semanas consecutivas durante el mes de noviembre, fecha posterior a la entrada en vigor de la DT IFT-010-2016, mientras que, para el caso del análisis del año 2019, este se realizó del 4 al 24 de noviembre, es decir, por un periodo igual de tres semanas consecutivas.

Los resultados de la investigación actual y los datos históricos nos permiten deducir si en los recintos incluidos en la muestra los bloqueadores de señal cumplen con la normatividad

Es importante señalar que los concesionarios mantienen la elaboración de reportes semanales sobre las interferencias que afectan la calidad de los servicios que prestan a sus usarios, enviándolos de manera directa o por vía de la ANATEL al Órgano Administrativo Desconcentrado de Prevención y Readaptación Social en la Comisión Nacional de Seguridad (CNS); de igual manera continúan presentando denuncias por interferencias perjudiciales ante el propio IFT, con copia a la Profeco, incluyendo sus impactos en la población que reside o transita cerca de esos recintos. A partir de 2019 son enviados a la Secretaría de Seguridad y Participación Ciudadana lo cual, como se verá más adelante, ha tenido un impacto positivo al contar por vez primera con acciones concretas de las autoridades de seguridad con base a la información que las empresas proporcionan año con año.

Como se mencionó anteriormente, la investigación aporta datos para dimensionar un problema de seguridad pública, al tiempo que cumple con uno de los criterios para llevar a cabo estudios sobre el "impacto en la actualización de riesgos", según se establece en los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 2 de diciembre del 2015.

Metodología

Se mantuvo la muestra de penales con características diversas y en distintas regiones del país. Se analizó de manera simutánea la información proveniente de cada uno de los concesionarios durante las tres semanas consecutivas. Como se podrá apreciar, los datos en los cuadros mostrados se presentan por semana, para observar claramente cómo evoluciona el número de equipos "sospechosos" así como los IMSIs.

En la primera fase de la investigación se analizaron datos a lo largo de tres semanas, las 24 horas del día. Las cifras que se presentan son el resultado de la suma de llamadas y de equipos identificados como "sospechosos" por los tres operadores móviles en cada penal.

En la segunda fase del análisis, se destinó también una elevada proporción del tiempo y recursos disponibles en el Grupo de Trabajo, puesto que la riqueza de los resultados estriba en el cruce de los datos entre 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 indentificados en sí, sino por las proporciones que guarda este indicador de intensidad 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***.

Principales resultados del análisis en Telefonía Móvil

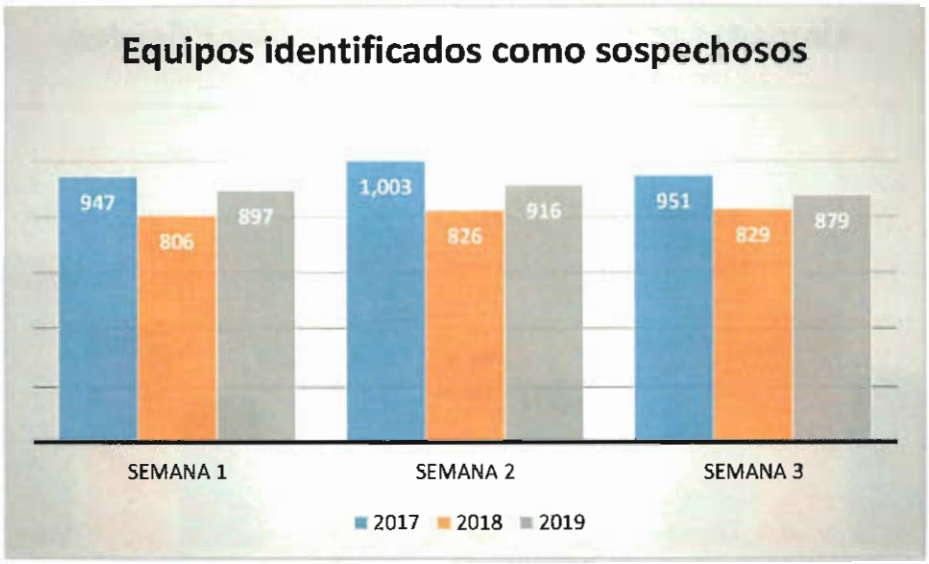
1. Los criterios para identificar a un equipo como "sospechoso" de ser utilizado para hacer llamadas desde un penal son: a) registrarse un número atípico de llamadas salientes; b) identificación de llamadas generadas desde varias tarjetas SIMs, que contienen un IMSI (Identidad Internacional de Abonado 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.
2. ***Observamos que durante 2019 se mantuvieron operando equipos con llamadas de salida en todos los penales de la muestra***, lo cual implica que aún existen algunos bloqueadores de señal que podrían funcionar mejor; sin generar además interferencias que afectan la calidad del servicio, como se reporta al Órgano Administrativo Desconcentrado de Prevención y Readaptación Social dentro de la

Comisión Nacional de Seguridad (CNS), así como al IFT mediante las denuncias de interferencia perjudicial (copia a PROFECO).

3. Para 2019 la investigación arrojó, como se ha observado en otros años, una variación semanal en el número de equipos y de IMSIs utilizados para hacer llamadas, además de un ***incremento significativo de ambos respecto a la disminución que fue observada durante el año anterior*** (2018 respecto de las cifras de 2017*)*.

   De manera conjunta se encontraron 897 equipos terminales "sospechosos" durante la primera semana de levantamiento de datos, relacionados con el uso de 1,918 IMSIs; durante la segunda semana se identificaron 916 equipos con 2,393 IMSIs asociadas; y, para la tercera semana, se hallaron 879 terminales utilizando 2,095 IMSIs. Es decir, en promedio el 78% de los equipos "sospechosos" utilizó más de una IMSI.
4. Al comparar estas cifras con las de 2018, observamos un incremento en el volumen de equipos e IMSIs para cada una de las tres semanas: 11% de equipos y 17% de IMSIs durante la primer semana; 10.8% de equipos y 41.5% de IMSIs durante la segunda semana; y, 6% en equipos y 23.9% en IMSIs durante la semana final de la investigación. Esta relación entre equipos e IMSIs y su crecimiento se observa en las gráficas 1 y 2 respectivamente.
5. Como consecuencia de la recurrente introducción de equipos terminales y la permanencia o instalación de inhibidores de señal deficientes, se registraron 158,109 llamadas durante la primera semana; 141,372 para la segunda; y 129,981 en la tercera semana. Cuando analizamos el ***Índice promedio de intensidad en el uso de un equipo para realizar llamadas***, encontramos que en 2019 dicho índice creció en promedio 30%; las gráficas 3 y 4 ilustran esta tendencia.
6. Es importante mencionar que recabar la información es un ejercicio que requiere de muchas horas-hombre en distintas etapas y de inversiones adicionales que permitan distinguir con precisión los equipos, IMSIs y 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 en 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.

Gráfica 1



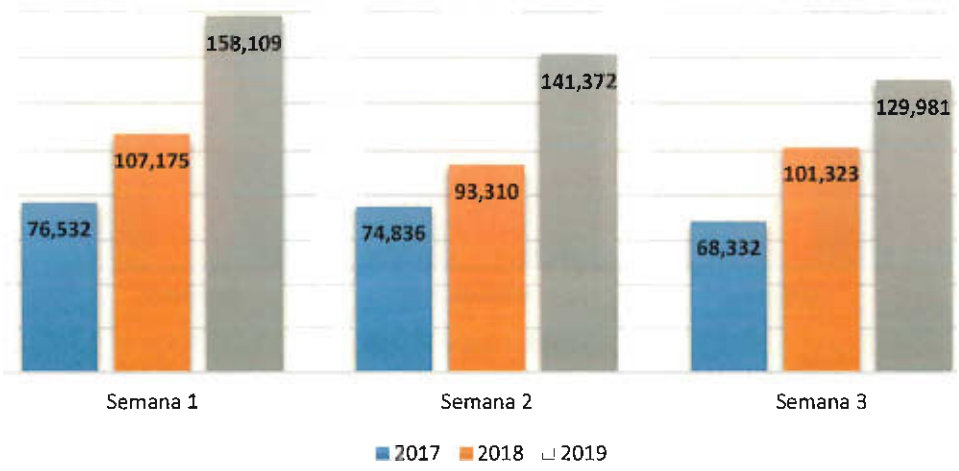
Fuente: Investigación ANATEL

Gráfica 2

Fuente: Investigación ANATEL

Gráfica 3

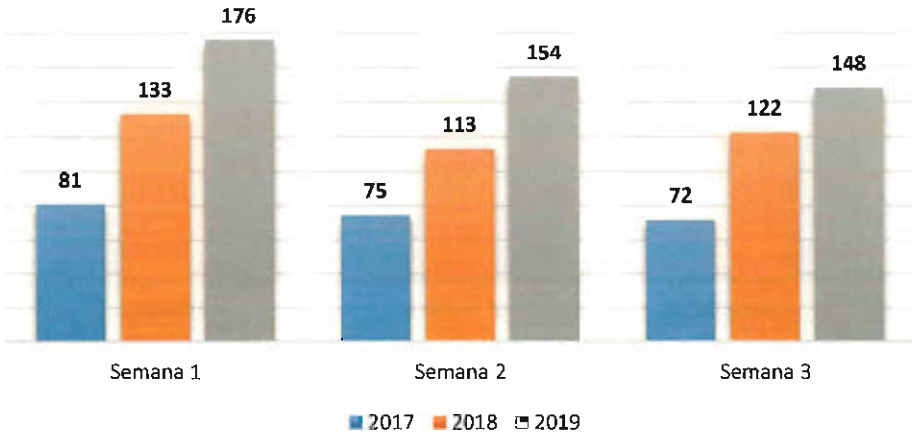
Llamadas realizadas por equipos identificados como sospechosos



Fuente: Investigación ANATEL

Gráfica 4

Índice promedio de intensidad en el uso de un equipo para realizar llamadas



Fuente: Investigación ANATEL

7. A nivel individual en cada uno de los penales, vale la pena destacar que en el año 2019, ***los penales marcados como "E" y "F" son los recintos con el moyor número***

de equipos sospechosos y con más IMSIs asociadas por semana. En dichos recintos se concentra el 73% de los teléfonos e IMSIs identificados durante el estudio.

8. ***El recinto "E" continúa siendo donde se identifican el mayor número de equipos***, 524 durante la primer semana, 583 en la segunda y 543 para la tercera. En este recinto, el índice de intensidad de llamadas es de los más altos de los 7 penales con 211 llamadas por terminal durante la primer semana, 186 durante la segunda, y 191 en la tercera. El total de llamadas generadas desde este recinto fue 322,569.
9. Por otra parte, las medidas de prevención en el recinto ***"F"*** cambiaron drásticamente. En el estudio de **2018 *"F"* destacaba por ser uno de los recintos con menor número de equipos sospechosos**, pero en 2019 se ha identificado en promedio **un incremento de 233% en el número de terminales y del 42% de IMSIs**. Este fenómeno se observa de manera similar en el recinto marcado como ***"A"***.
10. ***El caso más relevante sigue siendo el recinto "C"***, donde se hallaron en promedio 47 terminales sospechosas por semana, sin embargo, ***se registran los mayores índices de intensidad de llamadas por equipo: 559, 262 y 108***; esto es, en este recinto se registra un índice mucho mayor que el reportado para ***"E"***, aunque el total de equipos sospechosos representa solo el 8% de los equipos que operan en ese recinto.
11. ***En el recinto "G"*** estuvieron operando 101 equipos durante la primer semana, 71 en la segunda y 63 para la tercera; el índice de intensidad de llamadas por terminal durante la primer semana fue de 153, durante la segunda 154, y en la tercera 173.
12. En los recintos penitenciarios identificados como ***"B"*** y ***"D" se encuentran los equipos que realizan en promedio un volumen menor de llamadas***. Patrón idéntico al observado en los estudios anteriores.

Datos de la investigación en recintos penitenciarios por semana, 2019

Semana 1

Penal	Tipo de recinto	Equipos "sospechosos"	SIMs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas/ equipos
A	Estatal	31	87	31	12	1,987	64
B	Estatal	32	65	31	2	806	25
C	Federal	39	117	35	27	21,805	559
D	Estatal	54	83	28	3	1,650	31
E	Estatal	524	1,213	440	25	110,368	211
F	Estatal	116	192	53	2	6,076	52
G	Federal	101	161	58	4	15,417	153
Total		**897**	1,918	**676**	**NA**	158,109	**NA**

Fuente: Investigación ANATEL

Semana 2

Penal	Tipo de recinto	Equipos "sospechosos"	SIMs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas /equipos
A	Estatal	52	303	52	27	2,089	40
B	Estatal	21	43	19	4	899	43
C	Federal	45	159	40	22	11,783	262
D	Estatal	49	68	19	2	1,827	37
E	Estatal	583	1,529	509	65	108,719	186
F	Estatal	95	172	53	3	5,104	54
G	Federal	71	119	42	4	10,951	154
Total		**916**	**2,393**	**734**	**NA**	**141,372**	**NA**

Fuente: Investigación ANATEL

Semana 3

Penal	Tipo de recinto	Equipos "sospechosos"	SIMs	Equipos con más de 1 SIM	SIMs máximas	Llamadas semanales	Llamadas /equipos
A	Estatal	29	83	29	8	1,454	50
B	Estatal	25	48	23	2	730	29
C	Federal	59	180	57	36	6,346	108
D	Estatal	54	79	23	3	1,836	34
E	Estatal	543	1,415	467	74	103,482	191
F	Estatal	106	185	56	3	5,225	49
G	Federal	63	105	38	4	10,908	173
Total		**879**	**2,095**	693	**NA**	**129,981**	**NA**

Fuente: Investigación ANATEL

Implicaciones

El estudio muestra elementos importantes a considerar por las autoridades ante la solicitud permanente de los concesionarios, y de la propia sociedad, de elaborar una estrategia efectiva y de largo plazo para mejorar la seguridad de todos; así como para la atención eficiente de las interferencias que afectan de manera masiva a los usuarios de las áreas vecinas- y aún remotas- a los propios penales. Además, arroja elementos relevantes para los "Lineamientos de Colaboración entre Autoridades Penitenciarias y los Concesionarios de Servicios de Telecomunicaciones" y las "Bases Técnicas para la Instalación y Operación de Sistemas de Inhibición" del 3 de septiembre de 2012, sujetos a una posible actualización.

Las autoridades penitenciarias han hecho una labor importante de contención, pero aún con la entrada en vigor de la Disposición Técnica IFT-010-2016, se confirma que siguen operando una cantidad apreciable de equipos sospechosos en el conjunto de los penales de la muestra. Incluso donde hay pocos equipos "sospechosos" se observa que se realiza una gran cantidad de llamadas, que suponemos pueden ser con propósitos delictivos; afectando tanto a los usuarios como la calidad del servicio por las interferencias que generan los bloqueadores de señal.

Por otro lado, se observa que desde finales del año 2019 y principio del año 2020, las autoridades mencionadas 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.

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 LFTyR, reitera a las autoridades penitenciarias la recomendación de diseñar en un futuro cercano un programa que reduzca al mínimo la introducción de equipos terminales y de IMSIs en los recintos penitenciarios.

Telefonía Fija

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

Principales resultados del análisis

Se realizó un análisis estadístico 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 2019). 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) y el resto de los centros penitenciarios sin IVR[1].

Del análisis realizado se obtuvieron los siguientes resultados en el año 2019:

- En el total de la muestra se registraron 327,491 llamadas.
- De los cinco centros que cuentan con IVR habilitado el rechazo de llamadas alcanzó un 18.8% del total, lo cual muestra un decremento de más de 7 puntos porcentuales comparado con 2018, donde se observó un 26.1% de rechazo.
- Las llamadas rechazadas oscilan entre 20 y 57%, lo cual muestra un alto índice de variación por recinto penitenciario y sugiere la aversión al lugar de origen de las llamadas.
- El 17.5% del total de las llamadas aceptadas finalizó después de los primeros 10 segundos, comparado con el 16.3% durante el 2018.
- La duración promedio de cada llamada aceptada fue de 2.9 minutos, lo que sugiere que se estableció una conversación normal. Cabe mencionar que respecto a 2018, solo disminuyó 3 segundos en promedio.

[1] 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 total de llamadas, el 96% fueron realizadas entre las 7 y las 21 horas; el 4% restante (cerca de 13 mil llamadas) fueron realizadas entre las 21 horas y antes de las 7 horas del día siguiente. Comparado con el año anterior, en términos de horarios no existió una variación relevante; sin embargo, sí se observó un incremento de 11% en llamadas en dicho horario nocturno.
- Del total de las llamadas, el 73.2% se destinó a teléfonos móviles, el 20.3% a teléfonos fijos, el 4.4% a larga distancia internacional[2] y el 2.2% a números especiales. Comparado con el año 2018, las llamadas locales incrementaron en 7.4 puntos porcentuales y las llamadas a móviles y de larga distancia internacional disminuyeron en 1.8 y 4.9 puntos porcentuales, respectivamente.

Tabla 1. Resumen estadístico del tráfico analizado

Reclusorio	Tipo de Conexión	Porcentaje de Aceptación de llamadas	Llamadas Procesadas	Duración Promedio (minutos)	Destinos
D	Con IVR	43%	86	1.3	69.8% Móvil 30.2% Local
E	Con IVR	75%	142,251	2.7	67.2% Móvil 31.8% Local
F	Con IVR	76%	380	5.9	64.2% Móvil 35.8% Local
1	Con IVR	56%	70,471	2.4	79.3% Móvil 14.2% Local
2	Con IVR	80%	64,222	3.2	76.3% Móvil 23.7% Local
3	Sin IVR	---	2,271	2.5	64.3% Móvil 19.1% Local
4	Sin IVR	---	47,810	3.2	78.1% Móvil 19.9% Local

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 estadística que permitió analizar las llamadas provenientes de las casetas telefónicas en 7 centros penitenciarios del país, mismos que fueron analizados durante el estudio 2017 y 2018[3]; los identificados con letras corresponden a los mismos reclusorios presentados en el estudio de móviles.

Las llamadas analizadas se toman de la primera semana de cada uno de los primeros 8 meses (enero-agosto) del año 2019:

Mes	Inicio	Fin
Enero	Lunes 7	Domingo 13

[2] Se consideran las llamadas de larga distancia interanacional, EUA y Canadá y resto del mundo.
[3] Para el año 2018 se sustituyó el recinto "A" por el recinto "4".

Mes	Inicio	Fin
Febrero	Lunes 4	Domingo 10
Marzo	Lunes 4	Domingo 10
Abril	Lunes 1	Domingo 7
Mayo	Lunes 6	Domingo 12
Junio	Lunes 3	Domingo 9
Julio	Lunes 1	Domingo 7
Agosto	Lunes 5	Domingo 11

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, larga distancia nacional e internacional o números especiales), y;
- Duración de la llamada.

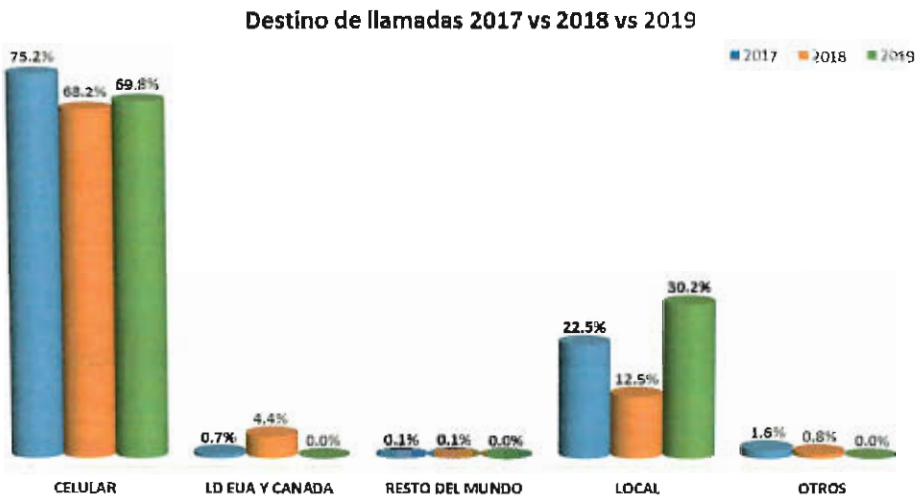
Análisis de Llamadas de Telefonía Fija por Reclusorio

Penal D

Este centro penitenciario registró muy poco tráfico en las casetas telefónicas analizadas, sin embargo, presenta resultados consistentes con los estudios de años anteriores. No se observaron llamadas al extranjero o números especiales de las casetas telefónicas, solo se registraron llamadas a telefonía fija así como a móvil; 60 llamadas pasaron por el sistema de IVR, de las cuales se registró un índice de rechazo del 57% (porcentaje más alto de rechazo en la muestra).

De las llamadas aceptadas, cuya duración promedio fue de 1.3 minutos (2.6 minutos menos que el año pasado), el 100% de las llamadas se realizaron entre las 7 y las 21 horas. Asimismo, el 5.8% de las llamadas aceptadas tuvieron una duración menor a los 10 segundos, lo cual representa una disminución de 6.2 puntos porcentuales respecto al año anterior. El 38.5% de las llamadas tuvieron una duración entre 10 y 30 segundos, lo que representa un incremento de más de 32 puntos porcentuales respecto a 2018.

De las llamadas generadas, el 69.8% se dirigió a teléfonos móviles, 1.6% más comparado contra el 2018 (68.2%). Las llamadas cursadas a números locales alcanzaron un 30.2%, es decir, un incremento de 19.7% respecto al 2018. Finalmente, no se registraron llamadas dirigidas a EUA y Canadá o resto del mundo.



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

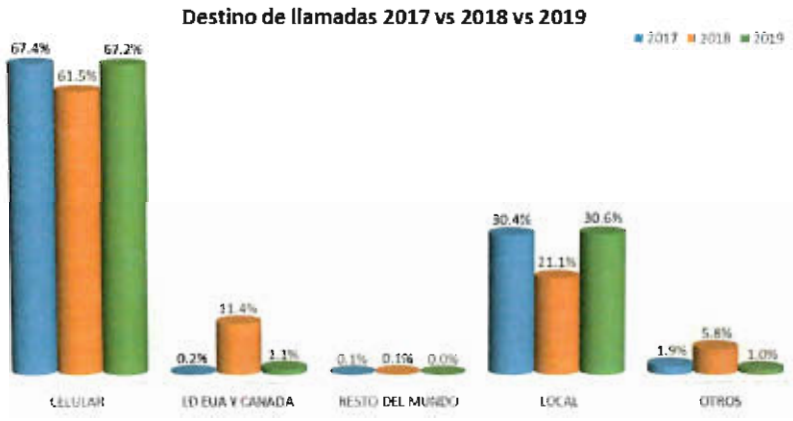
Penal E

Se analizaron 53,094 llamadas que pasaron de forma directa sin pasar por IVR; adicionalmente, 89,157 que pasaron por el sistema de IVR y el 25% de éstas fueron rechazadas.

En relación con el horario de las 66,658 llamadas aceptadas, cuya duración promedio fue de 2.7 minutos (igual al año anterior), el 97.6% se realizaron entre las 7 y las 21:00 horas; el resto (1,631) después de las 9 p.m. y antes de 7 a.m., concentrándose principalmente en los horarios de 9 p.m. a 1 a.m. Las llamadas rechazadas siguen un patrón similar a 2018 en cuanto a horarios y los mayores porcentajes de rechazo se centran después de las 9:00 p.m. y antes de las 4:00 a.m.

El 22.8% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa una variación a la baja de 8.5 puntos porcentuales respecto a 2018. Asimismo, el 9.9% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un incremento comparado con el año anterior de 3.5%.

De las llamadas generadas, el 67.2% se dirigió a teléfonos móviles, en términos generales, lo anterior representa un incremento de 5.7 puntos porcentuales comparado contra el 2018 (61.5%). Las llamadas cursadas a números locales alcanzaron un 29.6%, es decir, un incremento de 9.2% respecto al 2018. Finalmente, las llamadas de larga distancia internacional tuvieron una baja de 10 puntos porcentuales respecto al año anterior, llegando a un tráfico del 2.2% del total de las llamadas analizadas para este recinto, dicha disminución se debe principalmente a las llamadas dirigidas a EUA y Canadá (1.1% de 2019 contra el 11.4% de 2018).



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

Penal F

Se estudiaron 13 llamadas que pasaron de forma directa al ir dirigidas a números en el extranjero o números especiales; adicionalmente, 367 que pasaron por el sistema de IVR, de las cuales el 24% fueron rechazadas.

De las 291 llamadas aceptadas, cuya duración promedio fue de 5.9 minutos (3 minutos más que el año pasado), el 82.4% de las llamadas se realizó entre las 7 a.m. y las 9 p.m. y el 17.6% restante se realizó después de las 9 p.m. y las 1 a.m. Las llamadas rechazadas siguen un patrón similar en cuanto a horarios al año pasado.

Se observó que el 9.3% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa una variación a la baja de 3.8 puntos porcentuales respecto a 2018 (13.1%). Asimismo, el 4.8% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un decremento comparado con el año anterior de 1.9%.

De las llamadas generadas, el 64.2% se dirigió a teléfonos móviles, lo anterior representa una disminución de casi 20 puntos porcentuales comparado con 2018 (83.6%). Las llamadas cursadas a números locales alcanzaron un 25.8%, es decir, un aumento de 14.9% respecto al 2018. Finalmente, las llamadas de larga distancia internacional tuvieron un alza de 4.5 puntos porcentuales respecto al año anterior, llegando a un tráfico del 10% del total de las llamadas analizadas en este recinto.

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

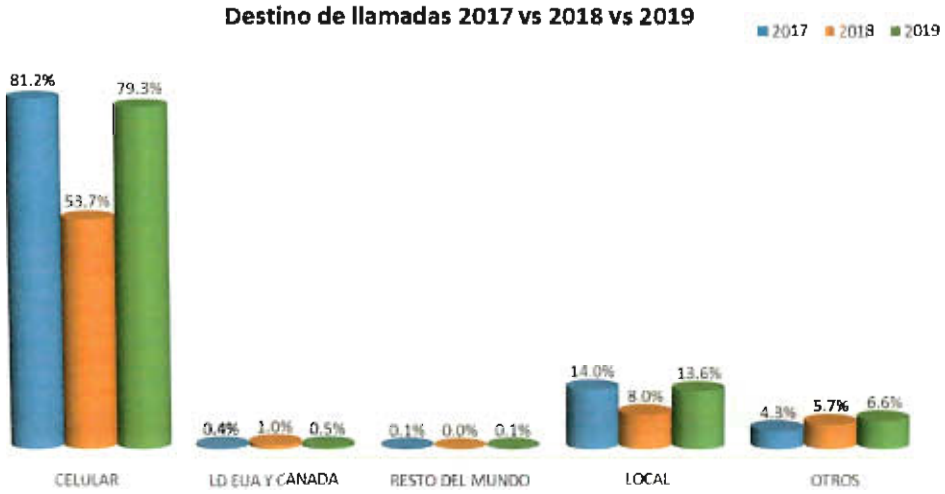
Penal 1

Se analizaron 21,561 llamadas que pasaron de forma directa sin pasar por IVR; adicionalmente, 48,910 que pasaron por el sistema de IVR, de las cuales se registró un índice de rechazo del 44%.

De las 27,275 llamadas aceptadas, cuya duración promedio fue de 2.4 minutos (18 segundos menos que el año pasado), el 95.1% de las llamadas se realizó entre las 7 a.m. y las 9 p.m. y las 1,342 llamadas restantes se registraron entre después de las 9 p.m. y antes de las 7 a.m. A diferencia de los otros centros penitenciarios este recinto muestra llamadas salientes las 24 horas del día. Las llamadas rechazadas siguen un patrón similar a 2018 en cuanto a horarios y los mayores porcentajes de rechazo (entre 51 y 64%) se encuentran entre las 12:00 a.m. y las 6:00 a.m.

El 11.5% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa un incremento de poco más de 5.7 puntos porcentuales respecto a 2018 (5.8%). Asimismo, el 12.31% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un incremento comparado con el año anterior de 7.5%.

De las llamadas generadas, el 79.3% se dirigió a teléfonos móviles, lo anterior representa un alza de 25.6 puntos porcentuales comparado contra el 2018 (53.7%). Las llamadas cursadas a números locales alcanzaron un 7.1%, es decir, un aumento de 2.3 puntos porcentuales respecto al 2018. Finalmente, las llamadas de larga distancia internacional también tuvieron un crecimiento de 2.8 puntos porcentuales en términos netos respecto al año anterior, llegando a un tráfico de 7.1% del total de las llamadas analizadas.



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

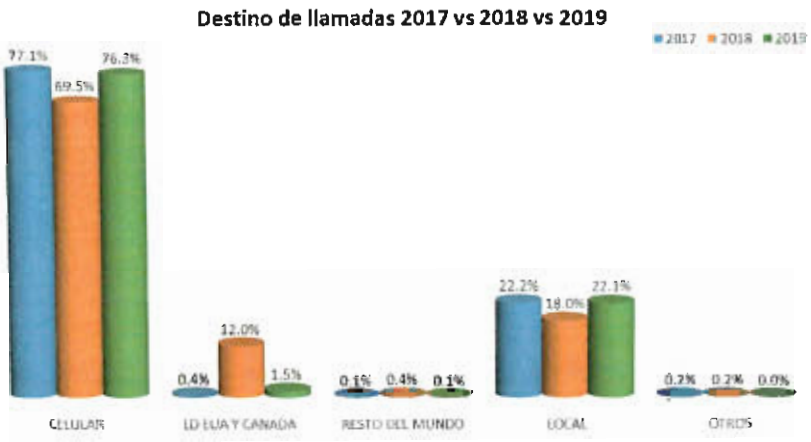
Penal 2

Se estudiaron 23,914 llamadas que pasaron de forma directa. Adicionalmente, 40,308 que pasaron por el sistema de IVR, de las cuales se registró un índice de rechazo del 20% (el porcentaje más bajos de rechazo en la muestra).

De las 32,382 llamadas aceptadas, cuya duración promedio fue de 3.2 minutos (18 segundos menos que el año anterior), el 94.2% de las llamadas se realizó entre las 7 a.m. y las 9 p.m.; las 1,876 llamadas restantes se registraron después de las 9 p.m. y las 2 a.m. Las llamadas rechazadas siguen un patrón similar a 2018 en cuanto a horarios, se observa un porcentaje de rechazo constante a lo largo del día entre el 15 y el 20%, los mayores porcentajes de rechazo se encuentran entre las 12:00 p.m. y la 1:00 p.m.

El 22.6% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa un decremento de más de 12 puntos porcentuales respecto a 2018 (35.1%). Asimismo, el 8.1% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un incremento comparado con el año anterior de 3.6%.

De las llamadas generadas, el 76.3% se dirigió a teléfonos móviles, en términos generales, lo anterior representa un aumento de 6.8 puntos porcentuales comparado contra el año 2018 (69.5%). Las llamadas cursadas a números locales alcanzaron un 21.3%, es decir, un incremento de poco más de 4 puntos porcentuales respecto al 2018. Finalmente, las llamadas de larga distancia internacional tuvieron una baja de 10.8 puntos porcentuales respecto al año anterior, llegando a un tráfico de tan solo 2.4% del total de las llamadas analizadas.



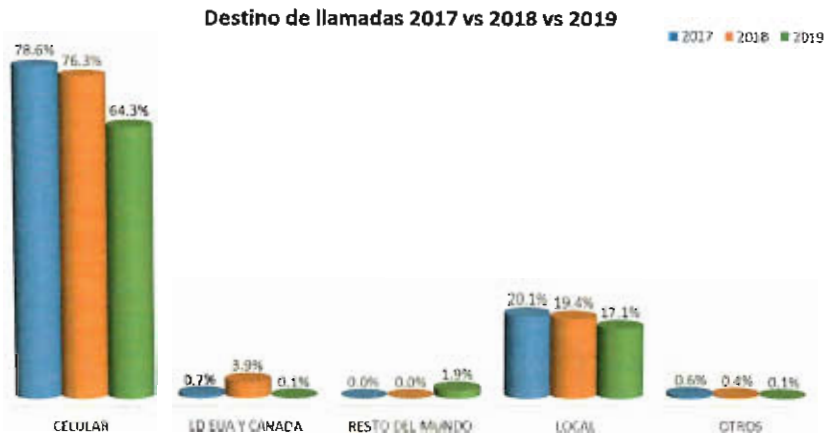
Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 2 analizado.

Penal 3

Se analizaron 2,271 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 2.5 minutos (igual que el año pasado), todas tuvieron lugar entre las 7 a.m. y las 7 p.m.

El 9.3% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa un incremento de casi 2 puntos porcentuales respecto a 2018 (7.4%). Asimismo, el 10.8% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa un incremento comparado con el año anterior de 0.5%.

De las llamadas generadas, el 64.3% se dirigió a teléfonos móviles, lo que representa una disminución de 11.9 puntos porcentuales comparado contra el año 2018 (76.3%). Las llamadas cursadas a números locales alcanzaron un 12.6%, es decir, un incremento de 0.7 puntos porcentuales respecto al 2018. Finalmente, las llamadas de larga distancia internacional decrecieron 4.9 puntos porcentuales respecto al año anterior, llegando a un tráfico de 6.5% del total de las llamadas analizadas.



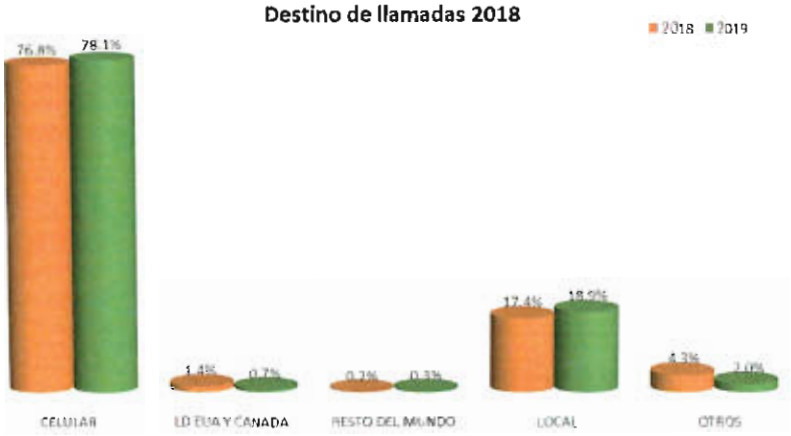
Fuente: Elaborado con datos del tráfico cursado desde las casetas telefónicas públicas localizadas al interior del Penal 3 analizado.

Penal 4

Se estudiaron 47,810 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 3.2 minutos (10 segundos más que el año pasado), el 98% tuvieron lugar entre las 6 a.m. y las 7 p.m. y el 2% restante se observa, en términos generales, entre las 4 a.m. y las 6 a.m.

El 4.7% de las llamadas aceptadas tuvieron una duración menor a 10 segundos, lo cual representa un incremento 0.7 puntos porcentuales respecto a 2018 (4%). Asimismo, el 7.5% de las llamadas aceptadas tuvieron una duración entre 10 y 30 segundos, lo que representa una disminución comparada con el año anterior de 0.6%.

De las llamadas generadas, el 78.1% se dirigió a teléfonos móviles, lo que representa un incremento de 1.3% respecto al año 2018. Las llamadas cursadas a números locales alcanzaron un 10.7%, es decir, un incremento de 0.8 puntos porcentuales respecto al 2018 y las llamadas de larga distancia internacional tuvieron un comportamiento similar, llegando a 9.2% de las llamadas analizadas solo 0.1 puntos porcentuales respecto al año anterior.



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

Implicaciones

El 18.8% 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, sin embargo, también se observó que dicho porcentaje disminuyó comparado con el año anterior (26.1%).

El 17.5% de las llamadas aceptadas concluyeron en los primeros 10 segundos, lo que sugiere que la gente colgó por no gustarle lo que escuchó, cabe mencionar que esta métrica incrementó 1.2 puntos porcentuales comparado con 2018.

Otro elemento de interés es que en los 7 recintos analizados, 3 de cada 4 llamadas tuvieron como destino un equipo móvil.

También se observó que existen centros penitenciarios con un horario restringido para llamadas, a saber, entre 7 a.m. y 7 p.m., si se consideran los centros que no cuentan con esta restricción, existe un 15.1% 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, buscarán objetivos delictivos; cabe mencionar que dicha cifra incrementó ya que en 2018 se situaba en 10.8%.

En suma, la información que se desprende de este esfuerzo preliminar al que pudieran adherirse 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:

"ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE INFORMACIÓN"

Estudio propuesto por el grupo
MAXCOM, MCM, IZZI, AXTEL, AVANTEL Y MARCATEL

ESTUDIO INTITULADO **"ESTUDIO EN MATERIA DE CIBERSEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"** QUE PRESENTAN LAS EMPRESAS **MAXCOM TELECOMUNICACIONES, S.A.B. DE C.V., AXTEL, S.A.B. DE C.V., AVANTEL, S. DE R.L. 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., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., Y FTTH DE MÉXICO, S.A. DE C.V.**

Contenido

1. Introducción.

En el mundo digital en el que vivimos hoy en día, no podríamos imaginarnos una organización, sector e incluso país el cual no esté habilitado o **soportado** por tecnología. Además, el ciberespacio no está solo limitado a las instituciones privadas o a gobiernos si no que está al alcance de la mayoría de los seres humanos. Nuevas tecnologías, regulaciones, y el amplio rango de amenazas a las que está expuesta la tecnología hace que los gobiernos y sectores privados volteen a desarrollar y establecer una cultura de seguridad para proteger la información de la cual son responsables.

La tecnología continúa revolucionado el mundo en el que vivimos brindándonos una infinidad de oportunidades para que las organizaciones entreguen sus servicios de una forma más eficiente. El sector de telecomunicaciones es comúnmente más abierto a la adopción de nuevas tecnologías, computación en la nube, dispositivos móviles. El internet incrementa el mercado de subscriptores y oportunidades para el sector de telecomunicaciones. Esto demanda a los operadores de comunicaciones un mayor grado de sofisticación en sus operaciones e infraestructura con el objetivo de guardar la privacidad de la información.

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 MAXCOM TELECOMUNICACIONES, S.A.B. DE C.V., AXTEL, S.A.B. DE C.V., AVANTEL, S. DE R.L. 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., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., Y FTTH DE MÉXICO, 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.

En atención MAXCOM TELECOMUNICACIONES, S.A.B. DE C.V., AXTEL, S.A.B. DE C.V., AVANTEL, S. DE R.L. 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., TELEVISIÓN INTERNACIONAL, S.A. DE C.V., OPERBES, S.A. DE C.V., MÉXICO RED DE TELECOMUNICACIONES, S.A. DE C.V., Y FTTH DE MÉXICO, S.A. DE C.V., se presenta el proyecto para la elaboración el estudio de seguridad y colaboración con la justicia.

4. Objetivo general.

La presentación de un documento que tiene 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, identificando los riesgos potenciales y la vulnerabilidad de las redes de acceso a internet en México, a efecto de proponer soluciones y medidas correctivas y preventivas – desde puntos de vista técnicos y jurídicos – orientadas a reducir dichos riesgos.

5. Objetivos del proyecto.

a) Identificar los delitos o actos ilícitos más recurrentes que se cometen a través de internet, en perjuicio de los usuarios y de los operadores, así como sus elementos.

b) Identificar los elementos esenciales y genéricos que se requieren para la prestación del servicio.

c) De conformidad con los elementos que se identificaron, determinar los elementos que pueden ser requeridos como controles tecnológicos de seguridad de información y ciberseguridad

d) Determinar objetivamente la dimensión y el alcance de la responsabilidad de los concesionarios y autorizados que prestan el servicio de acceso a internet, respecto al resguardo de la privacidad de los usuarios y de la seguridad de la red.

6. Metodología del estudio.

Para el estudio en materia de ciberseguridad y privacidad de la información se realizó la investigación de delitos de seguridad de información y ciberseguridad, la identificación de regulaciones aplicables, identificación del panorama de la privacidad de la información, para la generación de recomendaciones en controles tecnológicos adecuados para preservar la seguridad de los usuarios y de su información.

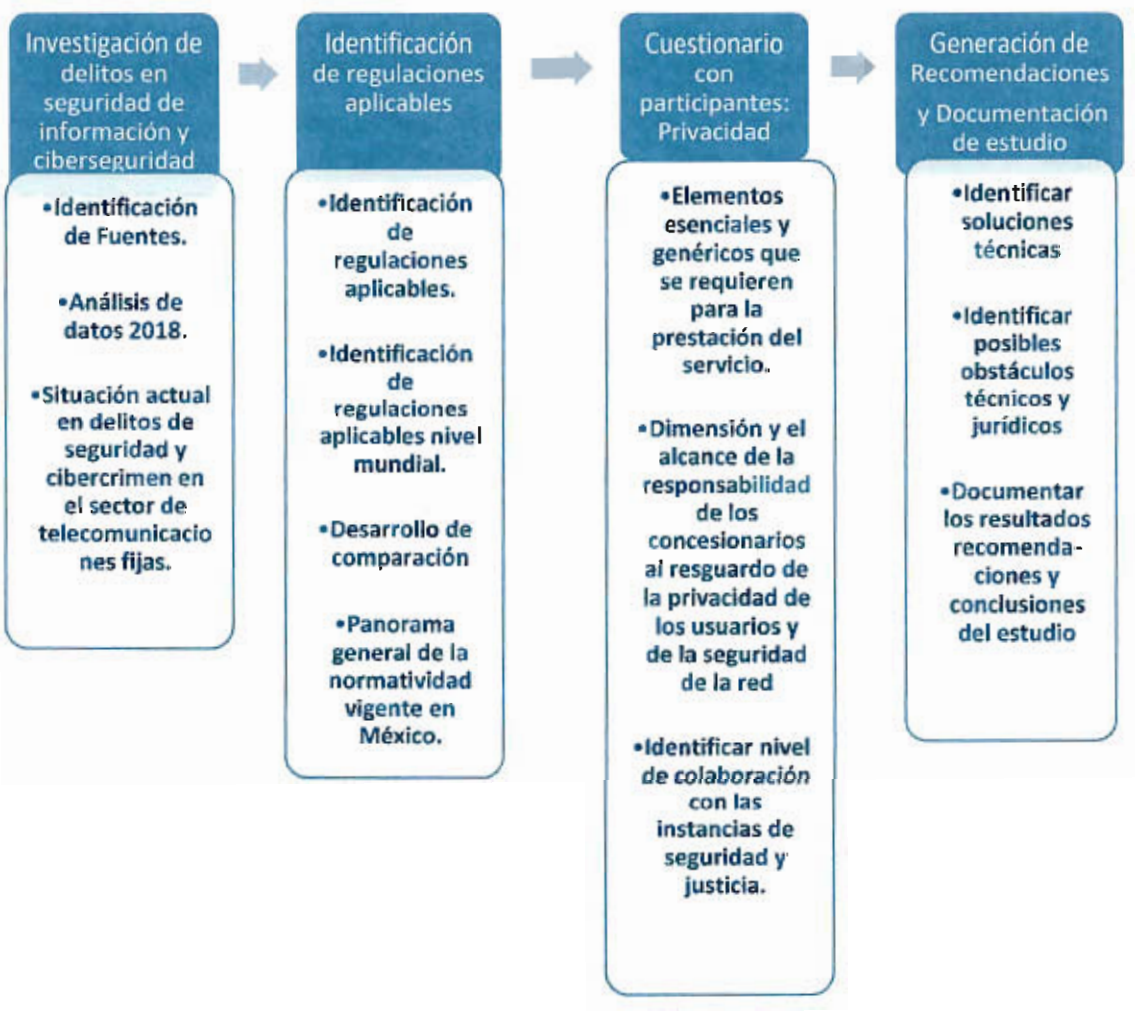


Fig. 1. Metodología del estudio en materia de ciberseguridad y privacidad de información.

7. Panorama actual en ciberseguridad.

El crimen informático o cibercrimen se está convirtiendo cada vez más en algo completamente sofisticado, con tal grado de complejidad y profesionalismo, así como extremadamente redituable para los cibercriminales los cuales buscan causar disrupción en la forma que operamos y vivimos, con el objetivo de causar daño a las empresas privadas y gobiernos a nivel mundial.

Las empresas y gobiernos reconocen hoy en día que el costo de los incidentes de seguridad puede causar un gran impacto negativo, es por esto por lo que se busca robustecer los marcos regulatorios y contractuales para facilitar la impartición de justicia y se reconoce que la tecnología de información y comunicación son parte fundamental de la infraestructura critica de los países.

Del año 2017 al 2019 el Cibercrimen y los Ciberataques a nivel mundial se han incrementado en un 89.06 % debido a que la tecnología está al alcance de todos, así mismo por el alto nivel de remuneración que representa para los cibercriminales y por el bajo nivel de aprehensión de estos. (HACKMAGEDDON , 2019)

En las siguiente Ilustración se representa algunos de los ciberataques que se tienen registrados a nivel mundial de manera general en diferentes sectores.

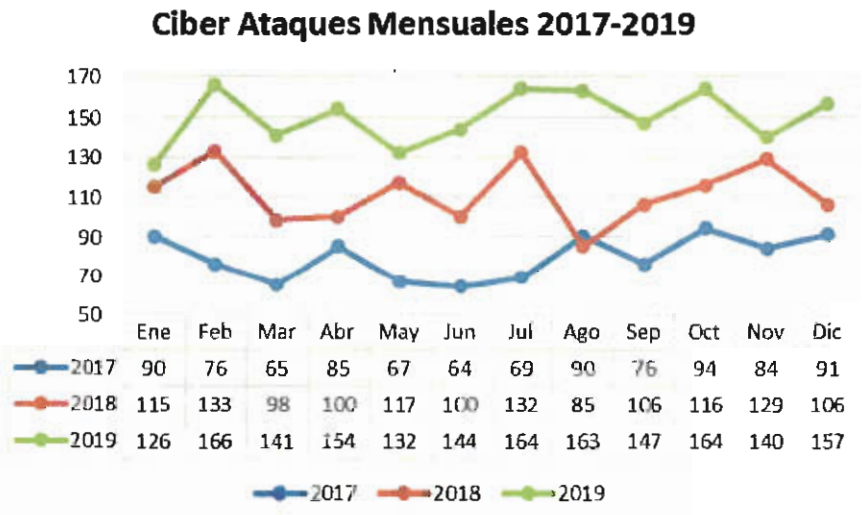


Fig. 2 Ciberataques 2017-2019 (HACKMAGEDDON , 2019)

Entre los principales incidentes de seguridad de información los cuales afectan la Confidencialidad, Integridad y Disponibilidad de la información encontramos:

1. **Cibercrimen.**

Se entiende cualquier delito cometido a través de internet por medio del uso de un equipo de computación o dispositivo móvil (ej. Computadora, teléfono, Tablet, tarjetas de memoria, etc.). (Ara, 2017)

2. **Ciber espionaje.**

Nos referimos al acto o practica de obtener secretos sin el permiso del poseedor de la información, de individuos, competidores, gobiernos, usualmente relacionada con información sensible, personal, propietaria o de naturaleza clasificada. A través del uso de equipos de computación y técnicas avanzadas. (Universidad Pompeu Fabra, 2016)

3. **Ciberguerra.**

Hace referencia al desplazamiento de un conflicto que ocurre en el ciber espacio utilizando las tecnologías de comunicación e información para atacar a una nación. Es decir las acciones de un estado o nación para tener acceso no autorizado a los equipos informáticos de otro país con el propósito de causar daños o interrupciones. (Sain, Gustavo, 2016)

4. **Hacktivismo.**

Nos referimos al acto de tener acceso no autorizado a equipos informáticos por motivaciones sociales o políticas. Cometido por un individuo o grupos de individuos motivados por un sentido de justicia de mostrar lo que consideran está mal o es incorrecto. (Rochina, 2016)

En las siguientes Ilustraciones se representan algunos de los incidentes en ciberseguridad que se tienen registrados a nivel mundial con base a las motivaciones anteriormente mencionadas.

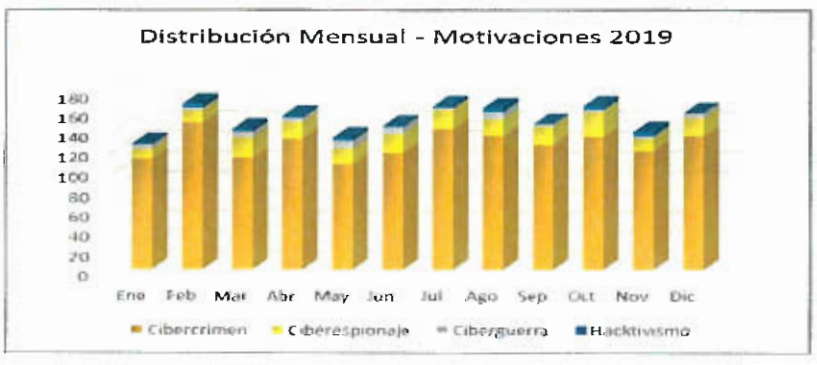


Fig. 3 Incidentes de seguridad en 2019 (HACKMAGEDDON , 2019)

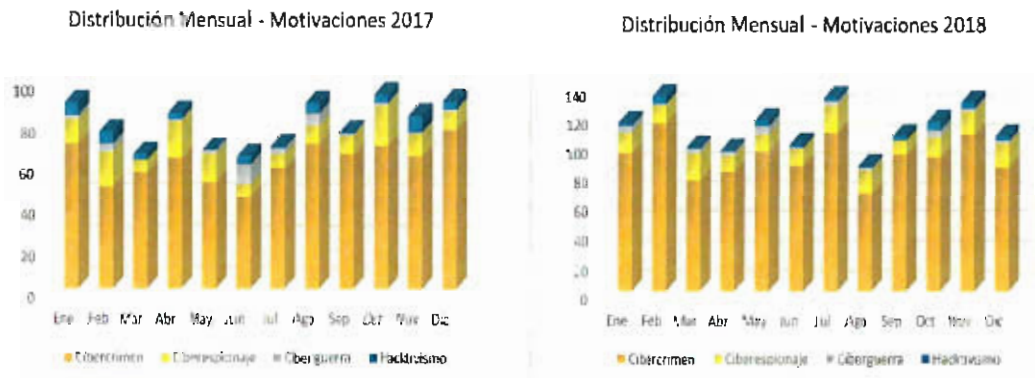


Fig. 4 y 5. Incidentes de seguridad en 2017 y 2018 (HACKMAGEDDON, 2019)

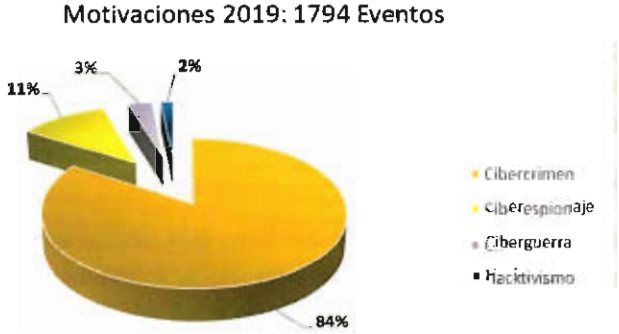


Fig. 6. Total de eventos registrados en el 2019 (HACKMAGEDDON , 2019)

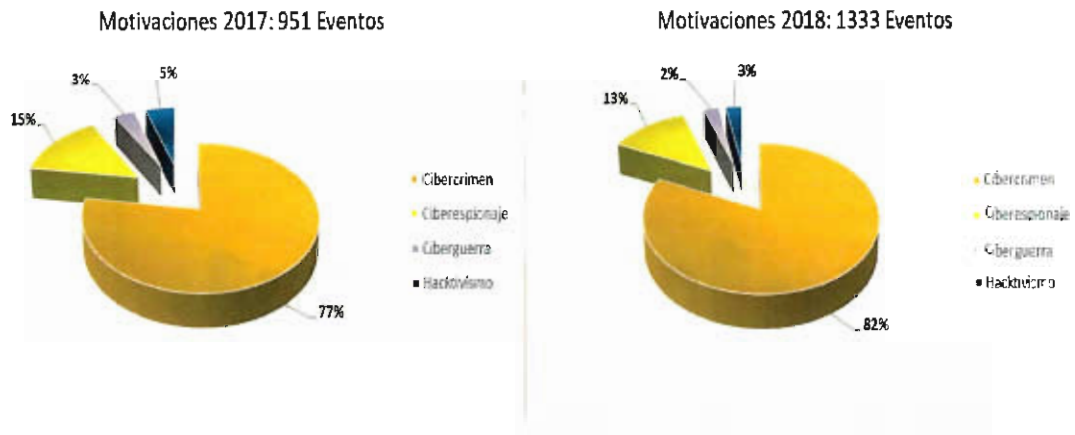


Fig. 7 y 8. Total de eventos registrados en el 2017-2018 (HACKMAGEDDON, 2019)

8. Delitos cometidos a través de internet contra los operadores.

El sector de telecomunicaciones no está fuera del alcance o la vista de los cibercriminales, desde el 2017 al 2019 se tiene evidencia de que múltiples compañías de telecomunicaciones han sido vulneradas por cibercriminales los cuales buscan extraer los datos sensibles de las compañías para logar algún tipo de lucro o beneficio. Dentro de los casos documentados se tiene como ejemplos los incidentes de:

Junio 2019: Los datos personales de clientes de la compañía SPRINT fueron vulnerados, se desconoce el número total de clientes afectados. (Mathews, Forbes, 2019)

Noviembre 2018: Configuraciones inadecuadas en los servidores informáticos revelan los datos de clientes, así como métodos de pagos de clientes de SKY Brasil. (Abel, 2018)

Agosto 2018: Robo de información Hackers roban más de 2 millones de datos personales de clientes de T-Mobile. (Mathews, Forbes, 2018)

Diciembre 2018: Proveedor de servicios de hosting en la nube pierde acceso a sus sistemas por el Ransomware Ryuk. (krebsonsecurity, 2018)

Enero 2018: Robo de información Bell Canadá un ISP informa a sus clientes que cierta información ha sido comprometida por hackers y más de 100,000 clientes se vieron afectados. (Infosecurity Group, 2018)

Octubre 2017: Un incidente masivo revela los datos personales de más de 46 millones de subscriptores telefónicos de al menos 12 operadores telefónicos. (BBC NEWS, 2017)

9. Panorama de la privacidad.

A nivel global la protección de la información sensible de los ciudadanos se ha vuelto un tema y necesidad primordial para los países y entidades regulatorias. La facilidad que el entorno tecnológico brinda al acceso de la información de los ciudadanos trae consigo actividades de protección para los Gobiernos, así como para la Industria privada.

10. Regulaciones de privacidad mundiales relevantes.

En las siguientes secciones se pretende dar un panorama general de la normatividad vigente en México y el resto del Mundo en materia de privacidad de los usuarios de Internet y de seguridad en la red.

1. **Reglamento General de Protección de Datos (GDPR).**

En materia de privacidad de Información la Unión Europea cuenta con una de las más completas regulaciones de protección de datos de los usuarios. En el 2016 se aprobó el Reglamento General de Protección de Datos (GDPR) con fecha de aplicación del 25 de mayo del 2018. El cual tiene como objetivo establecer con claridad mecanismos para proteger la privacidad de los ciudadanos europeos.

GDPR brinda a los usuarios de la Unión Europea el Derecho de Acceso, Derecho al Olvido y Rectificación, así como al Derecho a la Portabilidad de los Datos. A su vez establece sanciones económicas en el cumplimiento del reglamento GDRP. (Intersoft Consulting , 2018)

2. Regulaciones de Privacidad en Estados Unidos.

En Estados Unidos de América existen múltiples regulaciones de privacidad de información especificas por Estado y por Sector de la Industria, las cuales aplican a sectores como el de Telecomunicaciones, Financiero, de Salud, Instituciones Crediticias, Telemarketing e Información de menores.

El Estado de California cuenta con una de las regulaciones de privacidad de información más completa la cual tiene como título Ley de Privacidad del Consumidor de California (CCPA). Esta ley tiene como objetivo informar a los usuarios de que datos personales están siendo recolectados, notificar a los usuarios si sus datos son vendidos a compañías. Contar con el derecho a decir NO a la venta de datos personales. Brindar acceso a la información y solicitar a las compañías el borrado de la información de datos personales. (State of California, 2020)

A continuación, se enlistan algunas de las Leyes de Privacidad de datos a nivel mundial.

Fig. 9 Principales legislaciones de privacidad en el mundo. (Deloitte, 2018)

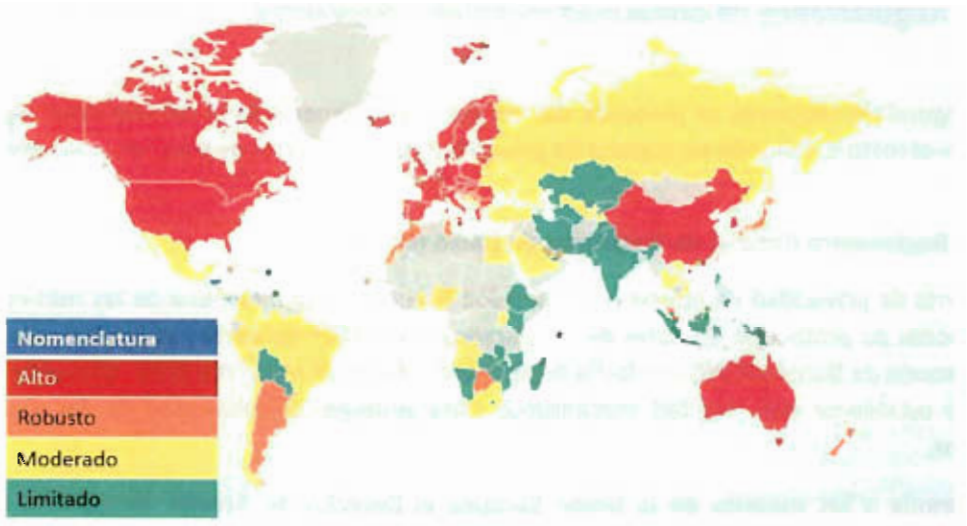


Fig.10 países con mayor grado de regulaciones de privacidad en el mundo. (DLA Piper, 2020)

La siguiente tabla contiene las principales regulaciones de privacidad de información a nivel mundial. No pretende ser una descripción a detalle del contenido, objetivo y aplicabilidad de cada regulación si no el brindar una guía de referencia sobre las regulaciones principales de cada país o nación.

PAIS / NACIÓN	REGULACIÓN
Afganistán	No cuenta con ley vigente en Privacidad de Datos.
Albania	Ley N°. 9887 en protección de datos personales.
África del Sur	Constitución de la Republica de África del Sur, protección de Información personal Ley 4 del 2013.
Andorra	Ley 15/2013 protección de Datos Personales.
Angola	Ley de protección de datos N°. 22/11.
Antigua y Barbuda	Ley de protección de datos 2013
Arabia Saudita	No cuenta con ley vigente en Privacidad de Datos. Se basa en la Ley y principios de Arabia Saudita.
Armenia	Ley de protección de datos de la Republica de Armenia.
Argentina	Ley de protección de datos personales 25, 326
Australia	Ley de Privacidad Federal 1988 y Principios de Privacidad de Australia.
Alemania, Austria, Bélgica, Bulgaria, Croacia, Chipre, Chequia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, países Bajos, Noruega, Polonia, Portugal, Reino Unido, Rumanía, Suecia, Suiza,	Reglamento General de Protección de Datos (GDPR)
Azerbaiyán	Ley de protección de datos 2010.
Bahamas	Ley de protección de datos Personales 2013.
Bangladés	No cuenta con ley vigente en Privacidad de Datos.
Barbados	Ley de protección de datos 2005.
Baréin	Ley de Baréin 30 del 2018
Belice	No cuenta con ley vigente en Privacidad de Datos. La regulación relevante es "Ley de Libertad de Información 2013"
Benín	Ley de protección de datos 2009
Bielorrusia	Ley de protección de Información N°. 455-z
Bermudas	Ley de protección de Información Personal 2019.
Bolivia	Constitución Política del Estado de Bolivia.
Bosnia y Herzegovina	Ley de protección de datos Personales N°. 49/06, 76/11 y 98/11.
Botsuana	Ley de protección de datos N°. 32 de 2018.
Brasil	Ley de Protección de Datos Personales (LGPD)

PAIS / NACIÓN	REGULACIÓN
Brunéi	Ley de protección de datos 2014
Burkina Faso	Ley N°010-2004/AN del 20 de abril del 2004
Burundi	No cuenta con ley vigente en Privacidad de Datos
Bután	No cuenta con ley vigente en Privacidad de Datos. La regulación relevante es "Ley de Información y Comunicación del 2006"
Cabo Verde	Ley de protección de datos I33/V/2001, 132/V/2001.
Camboya	No cuenta con ley vigente en Privacidad de Datos. La regulación relevante es el Artículo 10 del Código Civil de Camboya.
Camerún	No cuenta con ley vigente en Privacidad de Datos. La regulación relevante es: "Constitución política de la Republica de Camerún N°. 2008/001, 98/014"
Canadá	Ley de protección de información personal y documentos electrónicos.
Catar	Ley N°. 13, Regulación No. 6.
Chad	Ley de protección de datos personales 007/PR/2015
Chile	Ley N°. 19,628/199.
China	No cuenta con ley de privacidad de datos, se hace referencia a la Ley de Seguridad cibernética (CSL) de China vigente a partir del 1ro. De junio de 2017.
Chipre	Ley de procesamiento de datos personales.
Ciudad del Vaticano	No cuenta con ley de privacidad de datos, se hace referencia a el Código de Derecho Canónico 220.
Colombia	Ley Estatutaria 1266 de 2008 y Ley Estatutaria 1581 de 2012
Comoras	No se identificó ley de privacidad de datos vigente.
Corea del Norte	Ley de protección de datos personales 2011.
Corea del Sur	Ley de protección de datos personales 2011.
Costa de Marfil	Ley N°. 2013-450.
Costa Rica	Ley de Protección de la Persona Frente al Tratamiento De 5us Datos Personales N° 8968 y N° 7975
Cuba	No cuenta con ley de privacidad de datos.
Dominica	Ley de protección de datos 2007.
Ecuador	Ley Orgánica de Protección de Datos 15/1999 del 2016
Egipto	No cuenta con ley vigente en Privacidad de Datos
El Salvador	Ley de Protección de Datos
Eritrea	No cuenta con ley de privacidad de datos.
Estados Unidos	Cuenta con regulaciones estatales para la privacidad de datos siendo entre las más comunes: "Health Insurance Portability and Accountability Act (HIPAA), Ley de privacidad del consumidor de California 2018, Ley de privacidad de TV por Cable de 1984, Ley de privacidad y protección a menores 1988.
Etiopía	Constitución de la república Federal democrática de Etiopía de 1995.
Filipinas	Ley de protección de datos 2012 N°. 10173
Fiyi	No cuenta con ley de privacidad de datos, se hace referencia a: "Ley de Información del 2018".

PAIS / NACIÓN	REGULACIÓN
Gabón	Ley de protección de datos personales N°. 001/2011.
Gambia	Ley de Comunicaciones e Información N°. 2 del 2009.
Georgia	Ley de protección de datos personales de Georgia.
Ghana	Ley de protección de datos 2012 N°. 843.
Gibraltar	Ley de protección de datos 2004 y la directiva de la Unión Europea N°. 95/46.
Granada	No cuenta con ley de privacidad de datos.
Guernsey	Ley de protección de datos 2017.
Guatemala	No cuenta con ley de privacidad de datos. Se guía por la Constitución Política de la República de Guatemala 1985 Art. 23, 24.
Guyana	No se identificó ley vigente en Privacidad de Datos
Guinea	Ley de protección de datos 2019
Guinea Ecuatorial	Ley de protección de datos 2019
Haití	No cuenta con ley de privacidad de datos
Honduras	Constitución Política De La República de Honduras de 1982 Artículo 182.
Hong Kong	Ley de protección de datos Cap. 486.
India	Se rige por las guías de privacidad del 2011.
Indonesia	No cuenta con ley vigente en Privacidad de Datos
Irak	Ley de protección de datos en proceso de creación
Irán	No cuenta con ley vigente en Privacidad de Datos, se rige por la Constitución política de la República islámica de Irán
Islas Caimán	Ley de protección de datos 2017
Islas Vírgenes Británicas	No cuenta con ley vigente en Privacidad de Datos
Israel	Ley de protección de datos 5741 1981, Ley de privacidad de los seres humanos 5752 1992.
Jamaica	La constitución Política de Jamaica.
Japón	Ley de protección de datos personales.
Jordania	Ley de protección de datos.
Jersey "bailía de Jersey"	Ley de protección de datos 2018.
Kazajistán	Ley de la República de Kazajistán N°. 94-V 2013
Kenia	Ley de protección de datos 2019.
Kuwait	No cuenta con ley vigente en Privacidad de Datos, algunas regulaciones incluyen protección de información como lo son: Ley de Comercio Electrónico N°. 20 del 2014.
Kirguistán	Ley de protección de datos personales N°. 58 2008.
Laos	No cuenta con ley vigente en Privacidad de Datos.
Lesoto	Ley de protección de datos.
Líbano	Ley de protección de datos N°. 81/2018.
Liberia	Ley nacional de transferencia de datos 2011.
Libia	No cuenta con ley vigente en Privacidad de Datos.
Liechtenstein	Ley de protección de datos 2002.
Macao	Ley de protección de datos N°. 8/2005.
Madagascar	Ley de protección de datos N°. 2014-038.

PAIS / NACIÓN	REGULACIÓN
Malasia	Ley de protección de datos personales 2010.
Marruecos	Ley de privacidad de datos personales N°. 09-08 y su decreto N°. 2-09-165.
Mauricio	Ley de privacidad de datos 2017.
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ley federal de protección de datos personales en posesión de sujetos obligados.
Moldavia	Artículo 28 de la Constitución política de la republica de Moldavia Ley de privacidad de datos N°. 133 2011.
Mónaco	Ley de privacidad de datos N°. 1.165, N°. 1.462 2018
Mongolia	Ley de secretos personales 1995.
Montenegro	Ley de privacidad de datos N°. 79/2008, 70/2009, 44/2012, y 22/2017.
Mozambique	No cuenta con ley vigente en Privacidad de Datos, algunas regulaciones incluyen protección de información como lo son: "Ley No. 47344 del código civil, Ley de Transacciones Electrónicas N°. 3/2017".
Namibia	No cuenta con ley vigente en Privacidad de Datos, algunas regulaciones incluyen protección de información como lo son: "Constitución Política de Namibia Articulo 13".
Nauru	No cuenta con ley vigente en Privacidad de Datos
Nepal	Ley de Privacidad del 2018.
Nicaragua	Ley N°. 787 ley de Protección de Datos Personales
Nigeria	No cuenta con ley vigente en Privacidad de Datos, algunas regulaciones incluyen protección de información como lo son: Constitución política de la República Federal de Nigeria 1999, Ley de prohibición de delitos informáticos.
Nueva Zelanda	Ley de Privacidad de 1993.
Omán	Decreto Real N°. 9 2018.
Palaos	No se identificó Ley de Privacidad vigente
Pakistán	No cuenta con ley vigente en Privacidad de Datos.
Panamá	Ley 81 de Protección de Datos Personales.
Paraguay	Constitución Nacional de Paraguay Art. 135, Ley N° 1682/2001, Ley N° 4868/2013.
Perú	Ley de Protección de Datos Personales N° 29733.
República Del Congo	No se identificó Ley de Privacidad vigente.
República Dominicana	Ley N° 172-13.
República de Macedonia	Ley de protección de Datos N°. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015.
Ruanda	No se identificó Ley de Privacidad vigente.
Rusia	"Russian Constitution Art. 23 and 24, Data Protection Act N°. 152 FZ, Information Technologies and Information Protection Act. N°. 149 FZ".
Samoa	No se identificó Ley de Privacidad vigente.
San Cristóbal y Nieves	No se identificó Ley de Privacidad vigente.

PAIS / NACIÓN	REGULACIÓN
San Marino	Ley Reguladora de recolección de datos personales a través de computadoras 1983.
Santa Lucia	Constitución política de Santa Lucia.
Senegal	Ley N°. 2008-12, protección de datos personales 2019.
Serbia	Ley de protección de datos N°. 87/2018.
Seychelles	Ley de protección de datos 2003.
Singapur	Ley de protección de datos personales N°. 26 2016.
Siria	No se identificó Ley de Privacidad vigente.
Somalia	No se identificó Ley de Privacidad vigente.
Sri Lanka	Ley de protección de datos en desarrollo.
Sudán	No se identificó Ley de Privacidad vigente.
Surinam	Ley de protección de datos de Surinam.
Taiwán	Ley de protección de datos procesados por computadora.
Tanzania	Ley de protección de datos 2013.
Tayikistán	Ley de protección de datos N°. 1537, N°. 631, Ley de Información N°. 609.
Tailandia	Entrará en Vigor en mayo 2020 Ley de protección de datos.
Trinidad y Tobago	Ley de protección de datos 2011.
Túnez	Ley N°. 2004-63.
Turquía	Ley de protección de datos personales N°.6698
Turkmenistán	Ley de Turkmenistán N°. 519-V.
UAE – Abu Dhabi	Regulación de protección de datos 2015.
Uganda	Ley de privacidad de datos 2019.
Ucrania	Ley de Ucrania N°.2297, N°. 5491-VI.
Uruguay	Ley de protección de datos N°. 18.331; Decreto N°. 414/009.
Uzbekistán	Ley de protección de datos N°. ZRU-547
Venezuela	No se identificó Ley de Privacidad vigente. En la Constitución Política de Venezuela se hace referencia al Artículo 60
Vietnam	No cuenta con ley vigente en Privacidad de Datos, algunas regulaciones incluyen protección de información como lo son: La constitución del 2013 y el código civil 2015
Yemen	No cuenta con ley vigente en Privacidad de Datos.
Yibuti	No se identificó ley de privacidad de datos.
Zambia	Ley de Comunicaciones y transacciones electrónicas.
Zimbabue	Constitución política de Zimbabue y en la Ley de Privacidad y protección de información capitulo 10:27

Tabla N° 1 Principales regulaciones de privacidad a nivel mundial. Fuente (DLA Piper, 2020)

11. Regulaciones de privacidad en México.

En México, en abril del 2010 el Honorable Congreso de la Unión aprobó la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**. La cual vela por el correcto tratamiento de la información personal en posesión de terceros. (SEGOB, 2010)

Esta regulación busca que la información sensible de las personas sea tratada a lo dispuesto por las Leyes Mexicanas. Que las personas consientan el tratamiento de su información y que se les notifique cuándo, cómo y para qué será utilizada su información. A su vez pretende que la información se mantenga integra conforme a lo establecido por la ley y que solo se obtengan los datos estrictamente necesarios. Con esto las entidades están obligadas a velar y responder por el tratamiento de la información recabada.

Adicional a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México algunas de las leyes relevantes a nivel federal son:

1. **Ley general de transparencia y acceso a la información pública.**

Esta Ley tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativos, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las entidades Federativas y los municipios. (SEGOB, 2017)

2. **Ley general de protección de datos personales en posesión de Sujetos obligados.**

Esta Ley tiene por objeto establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento licito de los datos personales, garantizar que el tratamiento de datos personales sea licito, así como la protección de los datos de personas físicas en el debido cumplimiento de sus funciones y facultades por a aquellos Sujetos o Entes obligadas de informar de sus acciones y justificarlas en público con forme a la Ley de Transparencia. (SEGOB, 2017)

12. Panorama del cibercrimen mundial.

En el mundo digital en el que vivimos la infraestructura que lo soporta es naturalmente vulnerable a ataques informáticos. Los cuales pueden tomar múltiples magnitudes y formas. Desde el robo de datos personales hasta el secuestro de información y equipos. Estos ataques pueden tener la capacidad de interrumpir el curso normal de las organizaciones como afectar la infraestructura critica de países.

El Foro Económico Mundial ha categorizado por varios años consecutivos a los ciberataques como un riesgo latente y en constante crecimiento a nivel mundial llegándolos a categorizar en el top cinco (5) de los riesgos con mayor probabilidad de ocurrir. Así como en las listas de los 5 riesgos con mayor capacidad de Impacto a nivel mundial. (World Economic Forum, 2019)

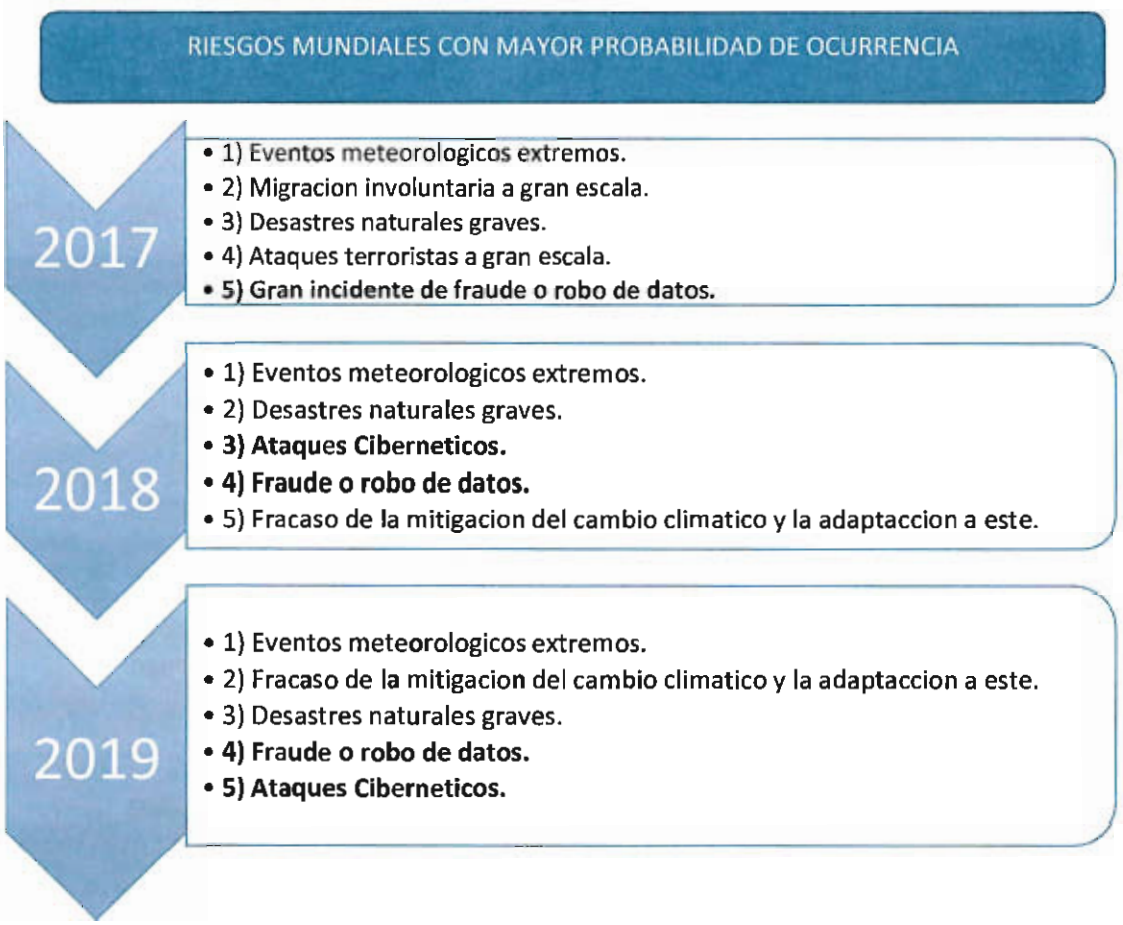


Fig. 11. Riesgos Mundiales Foro económico Mundial (World Economic Forum, 2019)

13. Regulaciones en cibercrimen a nivel mundial.

Con el objetivo de fomentar la impartición de justicia, salvaguardar la seguridad de información de los usuarios de telecomunicaciones, así como la seguridad de los prestadores de servicios de telecomunicaciones fijos, se identificaron las principales regulaciones en materia de cibercrimen a nivel mundial.

Fig. 12 Legislaciones sobre cibercrimen a nivel mundial. (United Nations, 2020)

La siguiente tabla contiene las principales regulaciones de cibercrimen de información a nivel mundial.

PAIS / NACION	REGULACIÓN
Afganistán	Sección 12 del código penal civil
África del Sur	Ley de Transacciones y Comunicaciones N°. 25 del 2002
Albania	Ley N°. 8888 articulo 22
Alemania	Código Penal de Alemania Sección 202, 303ª, 303b.
Andorra	Código Penal de Andorra Capitulo III
Angola	No cuenta con Ley vigente especifica en Cibercrimen
Antigua y Barbuda	Ley de crímenes electrónicos del 2018
Arabia Saudita	"Anti-Cyber Crime Law" Royal Decree N°. M/17
Argentina	No cuenta con Ley vigente especifica en Cibercrimen
Armenia	No cuenta con Ley vigente especifica en Cibercrimen
Australia	Ley de Cibercrimen del 2012
Austria	Austria Código Criminal (118ª, 126ª, 148ª)
Azerbaiyán	Ley Criminal de Azerbaiyán
Bahamas	Acta de Uso Indebido de Computadoras ('CMA') 2003
Bangladés	No cuenta con Ley vigente especifica en Cibercrimen. Se basa en la Ley de Comunicación e Información del 2006
Barbados	Acta de Uso Indebido de Computadoras 2005
Baréin	Legislación sobre Cibercrimen 2002
Bélgica	Código Penal (Artículo 210 bis).
Belice	No cuenta con Ley vigente especifica en Cibercrimen.
Benín	El Código Digital o Ley N°. 2017-20
Bermudas	No cuenta con Ley vigente especifica en Cibercrimen.
Bielorrusia	No cuenta con Ley vigente especifica en Cibercrimen.
Bolivia	No cuenta con Ley vigente especifica en Cibercrimen.
Bosnia y Herzegovina	No cuenta con Ley vigente especifica en Cibercrimen.
Botsuana	Ley Sobre Cibercrimen y Crímenes Relacionados con Computadoras 2007
Brasil	Ley N°. 12.737/2012 Del Código Criminal de Brasil.
Brunéi	No cuenta con Ley vigente especifica en Cibercrimen.
Bulgaria	Código Penal (Artículo 319ª).
Burkina Faso	No cuenta con Ley vigente especifica en Cibercrimen.
Burundi	No cuenta con Ley vigente especifica en Cibercrimen
Bután	No cuenta con Ley vigente especifica en Cibercrimen
Cabo Verde	"Lei N° 8/IX/2017"
Camboya	Ley de Cibercrimen de Camboya
Camerún	Ley N°. 2010/012 del 21 de diciembre del 2010
Canadá	Código Criminal de Canadá Sección 184 (RSC 1985, c C-46)
Catar	Ley No. 14 del 2014 Prevención de Cibercrimen
Chad	Ley de Cibercrimen N°. 009/PR/2015
Chequia	Ley de Seguridad cibernética (181/2014 Julio 23 2014)

PAIS / NACION	REGULACIÓN
Chile	Ley de Cibercrimen N°. 19.223
China	Ley Criminal de la República de China (Art. 285, 286, 287)
Chipre	Ley L.22(III)/2004
Chipre	Ley N°. 4411 del 2016
Ciudad del Vaticano	No cuenta con Ley vigente especifica en Cibercrimen.
Colombia	No cuenta con Ley vigente especifica en Cibercrimen. Los crímenes relacionados con el Cibercrimen se rigen por el Código Criminal (Art. 269 A al 269 H), (Art. 270 al 272) entre otros.
Comoras	No cuenta con Ley vigente especifica en Cibercrimen.
Corea del Norte	Ley de Redes de Corea del Norte
Corea del Sur	Ley de Redes de Corea del Sur
Costa de Marfil	Ley N°. 2013-451
Costa Rica	No cuenta con Ley vigente especifica en Cibercrimen. Se basa en la Ley de Intervención de Telecomunicaciones
Croacia	Código Criminal (OG 125/11, 144/12, 56/15, 61/15)
Cuba	No cuenta con Ley vigente especifica en Cibercrimen.
Dinamarca	No cuenta con Ley vigente especifica en Cibercrimen
Dominica	Ley de crímenes Relacionados con el Uso de Computadoras del 2005
Ecuador	Artículo 59, Ley de Comercio Electrónico (Ley N°. 2002-67)
Egipto	Ley N°. 175 del 2018
El Salvador	Ley Contra Delitos Informáticos de El Salvador publicada el 26/02/2016
Eritrea	No cuenta con Ley vigente especifica en Cibercrimen.
Eslovaquia	No cuenta con Ley vigente especifica en Cibercrimen
Eslovenia	No cuenta con Ley vigente especifica en Cibercrimen – Los delitos cibernéticos se apegan al código criminal de Eslovenia.
España	Código Penal de España Artículos (197, 248, 256, 270, 273)
Estados Unidos	Ley Federal de Fraude y Abuso informático
Estonia	No cuenta con Ley vigente especifica en Cibercrimen
Etiopía	Proclamación de Delitos Informáticos N°. 958/2016
Filipinas	Ley de Prevención de Cibercrimen del 2012
Finlandia,	No cuenta con Ley vigente especifica en Cibercrimen – Los delitos cibernéticos se apegan al código criminal de Finlandia.
Fiyi	Decreto de Crimen 2009 sección 336 a la 351
Francia,	Ley N°. 88-19 en Fraude informático
Gabón	Ley de Cibercrimen
Gambia	Parte III del Capítulo III de la Ley de TIC del 2019
Georgia	Código Criminal de Georgia
Ghana	Ley de Transición Electrónica 2018. N°. 772
Gibraltar	No cuenta con Ley vigente especifica en Cibercrimen.
Granada	Ley de Crímenes electrónicos del 2013
Grecia	No cuenta con Ley vigente especifica en Cibercrimen – Los delitos cibernéticos se apegan al código criminal de Grecia.
Guatemala	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Guatemala.

PAIS / NACION	REGULACIÓN
Guernsey	Medidas Restrictivas contra el Cibercrimen del 2019
Guinea	Ley Nº. L/2016/037/AN
Guinea Ecuatorial	No cuenta con Ley vigente especifica en Cibercrimen.
Guyana	Ley Contra Cibercrimen Nº. 17 del 2016
Haití	No cuenta con Ley vigente especifica en Cibercrimen.
Honduras	No cuenta con Ley vigente especifica en Cibercrimen.
Hong Kong	Ordenanza Sobre Delitos informáticos
Hungría,	Acta LXXIX del 2004
India	Ley de Información y Telecomunicaciones del 2000
Indonesia	Ley de la República de Indonesia Nº 11 de 2008 sobre información y transacciones electrónicas
Irak	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Irak.
Irán	Ley de crímenes electrónicos del 2013
Irlanda	Acta del 2017 – Delitos relacionados con los sistemas de información.
Islandia	Legislación sobre cibercrimen del 2007 así como el código penal 228 sección 1
Islas Caimán	Ley Nº. 4 del 2012
Islas Vírgenes Británicas	Uso Indebido de Computadoras y Cibercrimen del 2019
Israel	Ley de Computadoras de 1995
Italia	Código criminal Artículos (224, 247)
Jamaica	Ley de Cibercrimen del 2010
Japón	Código Penal de Japón
Jersey "Bailía de Jersey"	Ley de Uso Indebido de Computadoras de 1995.
Jordania	Ley de Delitos de Sistemas de Información Nº. 30 del 2010
Kazajistán	Código Penal de Kazajistán del 2014 Capitulo 7
Kenia	Ley de Información y Comunicaciones de 1998
Kirguistán	Código Criminal de Kirguistán Nº. 68
Kuwait	Ley de Cibercrimen Nº. 63
Laos	No cuenta con Ley vigente especifica en Cibercrimen.
Lesoto	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Lesoto.
Letonia	Ley Criminal de 1998 Capitulo XX
Líbano	No cuenta con Ley vigente especifica en Cibercrimen.
Liberia	Ley de Transacciones electrónicas del 2007
Libia	No cuenta con Ley vigente especifica en Cibercrimen.
Liechtenstein	Código Criminal de 1987
Lituania	Código criminal de Lituania Nº. XII-1428
Luxemburgo	Acta de Julio 15, 1993 sección VI
Macao	Ley Nº. 11/2009
Madagascar	Ley Nº. 2014-006
Malasia	Ley de Delitos Informáticos de 1997
Malta	Código Criminal 2001 Nº. 337 © (1)
Marruecos	No cuenta con Ley vigente especifica en Cibercrimen.

PAIS / NACION	REGULACIÓN
Mauricio	No cuenta con Ley vigente especifica en Cibercrimen.
México	No cuenta con Ley vigente especifica en Cibercrimen. Se basa en el Código Penal Federal (Ultima Reforma publicada en el DOF 24-01-2020) Titulo Noveno.
Moldavia	Ley N°. 20-XVI, 03.02.2009
Mónaco	Ley N°. 1.383 de 02/08/2011
Mongolia	No cuenta con Ley vigente especifica en Cibercrimen.
Montenegro	Código Criminal del 2003
Mozambique	No cuenta con Ley vigente especifica en Cibercrimen.
Namibia	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Namibia.
Nauru	No cuenta con Ley vigente especifica en Cibercrimen.
Nepal	Ley de Transacciones electrónicas 2063-2008
Nicaragua	Ley 842, Ley de Protección de Derechos de las Personas Consumidoras y Usuarias y su Reglamento Decreto 26-2013
Nigeria	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Nigeria.
Noruega,	No cuenta con Ley vigente especifica en Cibercrimen
Nueva Zelanda	Ley de Delitos 1961
Omán	Ley para Combatir el Cibercrimen del 2011
países Bajos	Ley sobre crímenes informáticos (CC-II), (CC-III)
Pakistán	Ley de Prevención de Delitos informáticos del 2016
Palaos	No cuenta con Ley vigente especifica en Cibercrimen.
Panamá	Ley (45, 24, 51, 81)
Paraguay	Código Penal 1160/1997 y la Ley que lo modifica y amplia Ley 4439/2011
Perú	Ley 295–1 - Código de Protección y Defensa del Consumidor
Polonia,	No cuenta con Ley vigente especifica en Cibercrimen. Algunos delitos cibernéticos se apegan al código criminal de Polonia.
Portugal	Ley de Información Penal de 1991 Capitulo 1 Articulo 7.
Reino Unido	Ley de Uso Indebido de Computadoras 1990 ('CMA').
República de Macedonia	Código Criminal 1996
República Del Congo	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para la República del Congo.
República Dominicana	Ley General N°. 358-05 sobre la Protección de los Derechos al Consumidor O Usuario
Ruanda	Ley de Tecnologías de Información y la Comunicación N°. 24/2016
Rumanía	Ley Anti-Corrupción para Prevenir y Combatir el Cibercrimen Capitulo III sección I
Rusia	Código Criminal 1996
Samoa	Ley de Telecomunicaciones N°. 20/2005
San Cristóbal y Nieves	Ley de crímenes electrónicos del 2009
San Marino	No cuenta con Ley vigente especifica en Cibercrimen.
Santa Lucia	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Santa Lucia.

PAIS / NACION	REGULACIÓN
Senegal	Ley sobre Cibercrimen N°. 2008-11
Serbia	Código Criminal del 2005
Seychelles	Ley de Uso Indebido de Computadoras N°. 17 de 1998
Singapur	Ley de Uso Indebido de Computadoras Capítulo 50 del 2007
Siria	Libertad en la Red del 2018
Somalia	No cuenta con Ley vigente especifica en Cibercrimen.
Sri Lanka	Ley de crímenes por Computadora N°. 24 del 2007
Sudán	Ley de Tecnologías de Información No.14 / Ley de Cibercrímenes del 2007
Suecia	No cuenta con Ley vigente especifica en Cibercrimen. Los delitos de Cibercrimen se apegan al código criminal de Suecia.
Suiza	No cuenta con Ley vigente especifica en Cibercrimen. Los delitos de Cibercrimen se apegan a varias Actas publicadas por Suiza.
Surinam	No cuenta con Ley vigente especifica en Cibercrimen.
Tailandia	Ley de crímenes por Computadora del 2007
Taiwán	Ley de Ciberseguridad Articulo 358
Tanzania	Ley de Cibercrímenes del 2015
Tayikistán	Código Criminal Articulo 277, 298
Trinidad y Tobago	Ley de Uso Indebido de Computadoras Nº. 86, Ley de Cibercrimen del 2015
Túnez	Ley de Cibercrimen del 2014
Turkmenistán	Código Criminal del 2013
Turquía	Código Criminal de Turquía del 2004
UAE – Abu Dhabi	Ley Federal N°. 2 para Combatir el Cibercrimen
Ucrania	Código Criminal del 2001
Uganda	Ley de Uso Indebido del 2011
Uruguay	Ley N°. 16763
Uzbekistán	Código Criminal de la Republica de Uzbekistán Artículo 174 crímenes Relacionados con el Uso de Computadoras.
Venezuela	Ley Especial Contra Delitos informáticos N°. 37.313
Vietnam	Decreto No. 55/2001/ND-CP del 2001
Yemen	La Ley de Cibercrimen se encuentra actualmente en Desarrollo para Yemen.
Yibuti	No cuenta con Ley vigente especifica en Cibercrimen.
Zambia	Ley de Transacciones y Telecomunicaciones 2009
Zimbabue	Ley sobre Delitos informáticos y Cibercrimen capitulo 9:23

Tabla N° 2 Principales regulaciones de cibercrimen a nivel mundial. Fuente (United Nations, 2020)

14. Regulaciones sobre el cibercrimen en México.

México reconoce las ciber amenazas como riesgos reales a la seguridad nacional del país. Algunas de las regulaciones relacionadas con el cibercrimen en México son:

Código Penal Federal

Tiene por objetivo establecer las sanciones para los delitos de orden federal en toda la República relacionados con la revelación de secretos y acceso ilícito a sistemas y equipos de informática. El cual establece sanciones que van desde treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto. (SEGOB, 2020)

Ley de Seguridad Nacional

Tiene por objeto establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la Seguridad Nacional, en sus respectivos ámbitos de competencia; así como, la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea; regular los instrumentos legítimos para fortalecer los controles aplicables a la materia. (SEGOB, 2019)

15. Panorama de telecomunicaciones a nivel mundial.

Alrededor del 80% de la infraestructura critica desarrollada de las naciones se encuentra bajo control del sector privado. Esto establece la necesidad de una protección adecuada de los recursos de telecomunicaciones y otras infraestructuras críticas la cual debido a su complejidad, relevancia y criticidad debe ser un esfuerzo en conjunto entre los gobiernos e instituciones privadas para lograr una mejora significativa en la protección de la infraestructura e información. Ya que la dependencia que tenemos como seres humanos de la información es cada vez más crítica para el día a día de las actividades cotidianas.

El establecer una cultura de seguridad de información en el sector de telecomunicaciones y de los operadores fijos representa que las organizaciones puedan alinear sus procesos a una estrategia nacional, gestionar los riesgos a los que se encuentra expuestos de manera más eficiente, generar valor tanto hacia adentro de la organización como a sus suscriptores y puedan optimizar de una mejor manera sus recursos integrando procesos de aseguramiento de información sin perder de vista las metas y objetivos de cada organización.

16. Principales regulaciones de telecomunicaciones mundiales.

Las telecomunicaciones fijas representan una parte de la infraestructura medular y critica de la sociedad moderna. Al establecer marcos regulatorios y legales en el sector de Telecomunicaciones se pretende asegurar que no existan monopolios y/o prácticas ilícitas o desleales asegurando que los usuarios reciban un servicio uniforme.

El sector de telecomunicaciones a nivel mundial es un área con mayor desarrollo en temas regulatorios comparados con las regulaciones de Privacidad de Información y/o Cibercrimen. En esta sección se pretende comparar el marco regulatorio en el sector de Telecomunicaciones a nivel

mundial contra el marco regulatorio de Telecomunicaciones en México al identificar las principales leyes o directivas en los principales países a nivel mundial.

Normatividad Telecom en la Unión Europea

La UE cuenta con el llamado Marco Regulatorio para Comunicaciones Electrónicas el cual se compone de una serie de Directivas y Regulaciones que todos los Estados Miembros deben acatar y detallar en sus legislaciones locales.

La directiva establece un marco armonizado para la regulación de las redes de las comunicaciones electrónicas, es decir, los sistemas de transmisión que permiten el transporte de señales mediante cables, medios ópticos u otros medios electromagnéticos, incluidas las redes por satélite, las redes terrestres de fijas y móviles, los sistemas de cables eléctricos, las redes utilizadas para la radiodifusión sonora y televisiva y las redes de televisión por cable, con independencia del tipo de información transportada.

Asimismo, incluye los servicios de las comunicaciones electrónicas, que están formados por la transmisión de señales por estas redes, y los **recursos y servicios asociados** a las redes o a los servicios de las comunicaciones electrónicas, que permiten o apoyan la prestación de servicios mediante esa red o servicio.

Entre las principales regulaciones de la Unión Europea se identifican la:

- Directiva 2002/20/CE o Directiva de autorización.
- Directiva 2002/19/CE o Directiva de acceso.
- Directiva 2002/22/CE o Directiva de servicio universal.
- Directiva 2002/58/CE o Directiva sobre la privacidad y las comunicaciones electrónicas.
- Reglamento (CE) Nº 1211/2009 por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE).
- Reglamento (UE) Nº 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles.

Fuente: (EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, 2002)

A continuación, se enlistan algunas de las regulaciones de Telecomunicaciones a nivel mundial, con la finalidad de representar el esfuerzo que los países toman para establecer controles regulatorios hacia el sector de telecomunicaciones.

PAIS / NACIÓN	REGULACIÓN
Afganistán	Ley para Regular Servicios de Telecomunicaciones del 2005.
África del Sur	Ley de Comunicaciones electrónicas Nº. 13 del 2000.
Albania	Ley de Comunicaciones electrónicas del 2008.

PAIS / NACIÓN	REGULACIÓN
Alemania	Ley de Telecomunicaciones de Alemania.
Andorra	Decreto del Reglamento de la Infraestructura de Telecomunicaciones de Andorra.
Angola	Instituto Nacional de Telecomunicaciones de Angola.
Antigua y Barbuda	Ley de Telecomunicaciones 2018.
Arabia Saudita	Ley de Telecomunicaciones 2001.
Argentina	Ley de Telecomunicaciones 27.078.
Armenia	Ley de la Republica de Armenia sobre Telecomunicaciones.
Australia	Ley de Telecomunicaciones 1997.
Austria	Ley de Telecomunicaciones 2003.
Azerbaiyán	Ley de Telecomunicaciones del 2005.
Bahamas	Ley de Telecomunicaciones del 2006.
Bangladés	Ley de Telecomunicaciones del 2001.
Barbados	Ley de Telecomunicaciones del 2001.
Baréin	Ley de Telecomunicaciones del 2002.
Bélgica	Ley Federal de Comunicaciones electrónicas 2005.
Belice	Ley de Telecomunicaciones del 2002.
Benín	Ley de Telecomunicaciones del 2014.
Bermudas	Ley de Telecomunicaciones del 1986.
Bielorrusia	Radio/Telecom Regulación técnica TR 2018/024/BY.
Bolivia	Ley General de Telecomunicaciones N°. 164, 2011.
Bosnia y Herzegovina	Ley en Comunicaciones de Bosnia y Herzegovina.
Botsuana	Ley de Transacciones y Comunicaciones electrónicas 2014.
Brasil	Ley General de Telecomunicaciones N°. 9,472 de 1997.
Brunéi	Ley de Brunéi Capitulo 54 Telecomunicaciones.
Bulgaria	Ley de Comunicaciones electrónica 2007.
Burundi	Decreto de Ley N°. 1/011 de 1997.
Bután	Ley de Telecomunicaciones del 1999.
Cabo Verde	Ley Básica para el Sector de Comunicaciones (5/94).
Camboya	Ley de Telecomunicaciones del 2015.
Canadá	Ley de Telecomunicaciones de Canadá.
Catar	Ley de Telecomunicaciones de Catar.
Chequia	Ley No. 127/2005 sobre las Comunicaciones electrónicas.
Chile	Ley General de Telecomunicaciones.
China	Regulación de Telecomunicaciones 2016.
Chipre	Ley de Regulación de las Comunicaciones electrónicas y los Servicios Postales N°. 112 2004.
Colombia	Ley de Telecomunicaciones N°. 1341 del 2009.
Corea	Ley de Negocio de Telecomunicaciones.
Costa Rica	Ley General de Telecomunicaciones.
Croacia	Ley de Telecomunicaciones 1999.
Dinamarca	Ley sobre las comunicaciones y servicios electrónicos.
Dominica	Ley de Telecomunicaciones N°. 18.
Ecuador	Ley Orgánica de Comunicaciones 2013.
Egipto	Ley de Telecomunicaciones 10/2003.

PAIS / NACIÓN	REGULACIÓN
El Salvador	Ley de Telecomunicaciones de 1997.
Eslovaquia	Ley N°. 139/2017.
Eslovenia	Ley de Telecomunicaciones.
España	Ley de Telecomunicaciones 1987.
Estados Unidos	Ley de Comunicaciones de 1934.
Estonia	No cuenta con Ley vigente especifica en Telecomunicaciones.
Filipinas	Ley de Política de Telecomunicaciones Públicas de Filipinas.
Finlandia	Ley de Comunicaciones electrónicas.
Francia	Ley N°. 2004-669 Comunicaciones Electrónicas y Servicios de Comunicación Audiovisuales.
Ghana	Ley de Comunicaciones electrónicas del 2008.
Grecia	Ley N°. 4070/2012 Regulación de Comunicaciones electrónicas.
Guatemala	Ley de Telecomunicaciones de Guatemala.
Hong Kong	Ordenanza en Telecomunicaciones Cap. 616.
Hungría	Ley C del 2003 de Comunicaciones electrónicas.
India	Ley de Telecomunicaciones 1997.
Indonesia	Ley de la Republica de Indonesia No. 36.
Irak	La Ley de Telecomunicaciones de Irak se encuentra en desarrollo.
Irán	Ley de Telecomunicaciones de 1982.
Irlanda	Ley de Regulación de Comunicaciones del 2002.
Islandia	Ley de Comunicaciones electrónicas del 2002.
Israel	Ley de Comunicaciones 1982.
Italia	Código de Comunicaciones electrónicas N°. 259/2003.
Jamaica	Ley de Telecomunicaciones del 2000.
Japón	Ley de Negocios en Telecomunicaciones N°. 86 de 1984.
Kenia	Regulación para la Comunicación e Información 2010.
Kuwait	Ley de Telecomunicaciones (Decretos N°. 8, 77, 108,266).
Letonia	Ley de Telecomunicaciones del 2003.
Lituania	Ley de Comunicaciones electrónicas del 2004.
Luxemburgo	Ley de Comunicaciones electrónicas del 1997.
Malta	Ley de Comunicaciones electrónicas y Ley de Redes y Servicios de 1998.
Mauricio	Ley de Telecomunicaciones 1998.
México	Ley Federal de Telecomunicaciones y radiodifusión.
Nepal	Ley de Telecomunicaciones de 1997.
Nicaragua	Ley General de Telecomunicaciones y Servicios Postales 2005.
Nigeria	Ley de Comunicaciones.
Noruega	Ley de Comunicaciones electrónicas del 2003.
Nueva Zelanda	Ley de Telecomunicaciones del 2001.
países Bajos	Ley de Telecomunicaciones Holandesa 1998.
Paraguay	Ley General de Telecomunicaciones N°. 642/1995.
Perú	Ley N°. 28278.
Polonia	Ley de Telecomunicaciones del 2004.
Portugal	Ley de Comunicaciones electrónicas del 2004.
Qatar	Ley de Telecomunicaciones N°. 34.

PAIS / NACIÓN	REGULACIÓN
Reino Unido	Ley de Comunicaciones 2003.
República Del Congo	Ley N°. 013-2002.
República Dominicana	Ley de Telecomunicaciones N°. 118.
Rumanía	Ley Marco General de Telecomunicaciones N°. 239/2005.
Rusia	Ley de Telecomunicaciones.
Serbia	Ley de Comunicaciones electrónicas del 2010.
Singapur	Ley de Medios de Comunicación e Información N°. 22 2016.
Siria	Ley de Telecomunicaciones.
Sudán	Ley de Telecomunicaciones 2001.
Suecia	Ley de Comunicaciones electrónicas del 2003.
Suiza	Ley Federal de Telecomunicaciones 2007.
Tailandia	Ley de Telecomunicaciones N°. 2498, 2544, 2551, 2553.
Taiwán	Ley de Telecomunicaciones 2013.
Trinidad y Tobago	Ley de Telecomunicaciones 2001.
Túnez	Ley Federal de Telecomunicaciones.
Turquía	Ley de Comunicaciones electrónicas N°. 5809.
Ucrania	Ley de Telecomunicaciones electrónicas.
Venezuela	Ley de Telecomunicaciones N°. 39.610.
Vietnam	Decreto No. 121/CP de 1987.
Zambia	Ley de Telecomunicaciones electrónicas 2009.
Zimbabue	Ley de Telecomunicaciones Capitulo 12:05.

Tabla N° 3 Regulaciones de telecomunicaciones. Fuente: (The Telecommunication Development Sector, 2020)

17. Regulaciones telecomunicaciones en México.

México se ha preocupado por establecer reglas para garantizar el correcto funcionamiento en los diferentes sectores de la industria como el de Telecomunicaciones con el fin de brindar a los ciudadanos la certeza jurídica, preservar los derechos de propiedad, así como evitar daños y brindar bienestar a la población.

Las principales leyes relevantes a nivel federal para la impartición de justicia en materia de telecomunicaciones para prestadores de servicio fijo en México son:

Ley Federal de Telecomunicaciones y Radiodifusión.

Esta Ley tiene como objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes públicas de telecomunicaciones, el acceso a la infraestructura activa y pasiva, los recursos orbitales, la comunicación vía satélite, la prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión y la convergencia entre estos. los derechos de los usuarios y las audiencias, y el proceso de competencia y libre concurrencia en estos sectores,

para que contribuyan a los fines y al ejercicio de los derechos establecidos en los artículos 6o., 7o., 27 y 28 de la Constitución Política de los Estados Unidos Mexicanos. (SEGOB, 2020)

Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de Información (MAAGTICSI).

El objetivo de MAAGTICSI es definir los procesos con los que las empresas en materia de Tecnologías de Información las Comunicaciones y de Seguridad de Información las Instituciones deberán regular su operación, independientemente de su estructura organizacional y las metodologías de operación con las que cuenten. (SEGOB, 2018)

Ley de la Policía Federal.

La policía Federal es un órgano administrativo desconcentrado de la Secretaria de Seguridad Publica la cual tiene como objetivo salvaguardar la vida, la integridad, la seguridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos. Aplicar y operar la política de seguridad pública en materia de prevención y combate de delitos.

La Policía Federal cuenta con atribuciones y obligaciones en el sector de Telecomunicaciones para prevenir la comisión de delitos, así como solicitar por escrito, previa autorización del juez de control en los términos del artículo 16 Constitucional, a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones, de sistemas de comunicación vía satélite, la información con que cuenten, así como georreferenciación de los equipos de comunicación móvil en tiempo real, para el cumplimiento de sus fines de prevención de los delitos. La autoridad judicial competente, deberá acordar la solicitud en un plazo no mayor de doce horas a partir de su presentación. (SEGOB, 2011)

Directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.

Garantizar un Sistema de Justicia Penal eficaz, expedito, imparcial y transparente y prevé entre sus líneas de acción lo referente a diseñar y ejecutar las adecuaciones normativas y orgánicas en el área de competencia de la Fiscalía General de la república, para investigar y perseguir el delito con mayor eficacia.

Son las guías para establecer un sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión. (SEGOB, 2015)

18. Amenazas para la industria de telecomunicaciones.

El sector de Telecomunicaciones en México se encuentra y enfrenta a una cantidad creciente de desafíos complejos. Vivimos en una era de adelantos tecnológicos sin precedentes por lo que

asegurar la Confidencialidad, Integridad y Disponibilidad de la información y de la infraestructura de telecomunicaciones representa un reto para el sector público y privado.

Las amenazas a las que se enfrentan los operadores de telecomunicaciones fijas obligan a que se redoblen los esfuerzos para brindar los servicios a la población.

En esta sección se enlistan las principales amenazas a los que la Industria de Telecomunicaciones se enfrenta constantemente, en las secciones posteriores se encuentran las recomendaciones tecnológicas para minimizar el impacto de que una amenaza se materialice entre los distintos operadores de telecomunicaciones fijas.

Denegación de Servicios Distribuidos (DDOS).

Los ataques de red distribuidos o ataques de denegación de servicios son un tipo de amenaza a los que los proveedores de telecomunicaciones fijas se encuentran expuestos. Este tipo de ataques aprovecha los límites de capacidad de cualquier recurso de red, así como la infraestructura que lo habilita.

Los recursos de red y telecomunicaciones cuentan con un número finito de solicitudes que pueden atender al mismo tiempo, los cibercriminales aprovechan que los canales de comunicación tienen un ancho de banda o canales limitados y cuando la capacidad de peticiones sobrepasa los límites de capacidad de cualquiera de los componentes de la infraestructura, el nivel de servicio se ve afectado haciéndolo usualmente más lento o al ignorarse las solicitudes validas de los usuarios. (ISO27001 ES, 2005)

¿Por qué el sector de telecomunicaciones se ve afectado por ataques de denegación de servicios distribuidos?

Las motivaciones que incitan a las personas a lanzar ataques de denegación de servicios contra la infraestructura de telecomunicaciones son múltiples. Entre las principales encontramos que pueden ser por:

1. Cibercrimen
    - Obtener algún beneficio económico.
2. Razones políticas.
    - Regulaciones restrictivas
    - Descontento contra líderes políticos.
3. Razones Sociales.
    - Regulaciones de privacidad y de acceso a la información impuestas a los ciudadanos.
    - Hacktivismo. Es decir, la utilización no violenta del uso de herramientas tecnológicas
4. Competición.
    - Prestigio personal o grupal entre grupos de hackers o ciberdelincuentes.
5. Guerra cibernética.

- Es un área entre las agencias militares de los países que tiene como objetivo encontrar vulnerabilidades en la infraestructura del enemigo para penetrarlas y atacarlas.

6. Usuarios enojados.
    - Representan una amenaza latente con el fin de generar una mala reputación de las organizaciones hacia el público en general.
7. Motivación desconocida.
    - Múltiples factores que pueden hacer que una persona o grupo de personas lleven a cabo un ataque distribuido de denegación de servicios.

Las siguientes ilustraciones representan la tendencia de los casos registrados de denegación de servicio distribuido (DDOS) a nivel mundial.

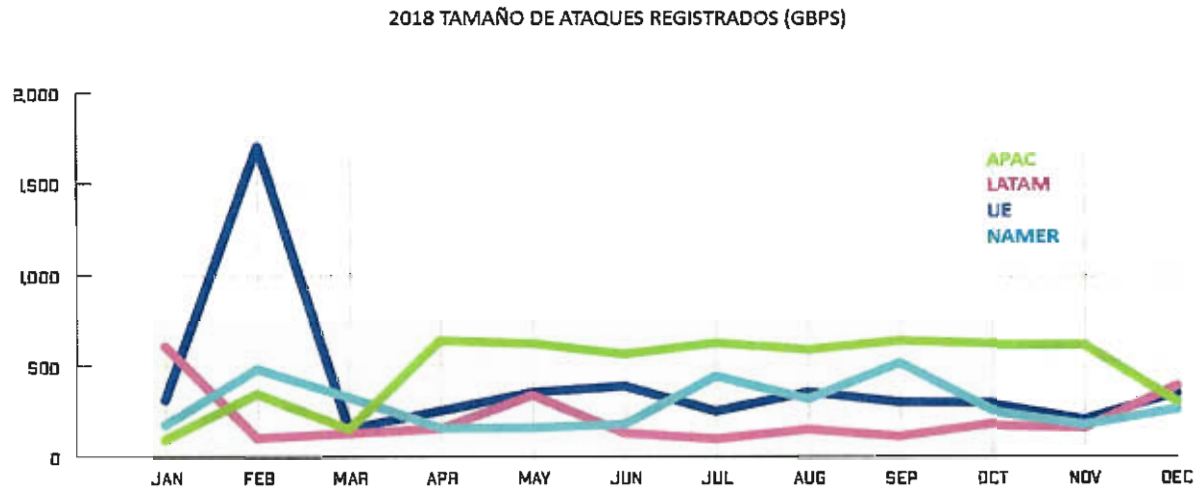


Fig. 13 Número de Incidentes de Denegación de Servicios 2018 (Netscout, 2019)

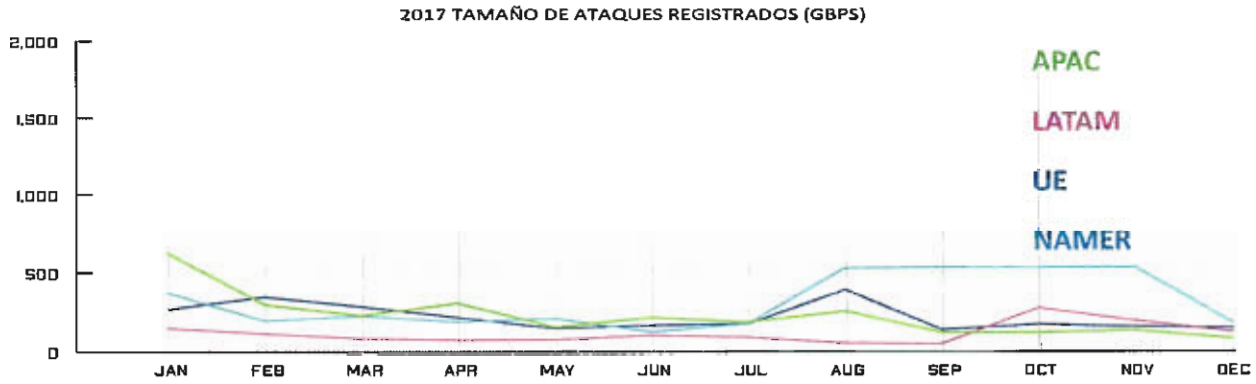


Fig. 14 Número de Incidentes de Denegación de Servicios 2017 (Netscout, 2019)

Ataques Dirigidos

Los ataques dirigidos son causados principalmente cuando se cumplen tres condiciones:

1. Los atacantes tienen un objetivo específico. Ya sea un usuario o una organización, los ataques de este tipo normalmente requieren tiempo, esfuerzo y recursos para llevar a cabo este tipo de ataques.
2. El principal objetivo de los ciberdelincuentes es tener acceso no autorizado a la infraestructura de la organización para el robo de información.
3. El ataque es persistente y normalmente el acceso en la infraestructura se mantiene sin ser detectado durante tiempos prologados.

La característica de un ataque dirigido es que usualmente se lleva acabo de forma sigilosa para evitar el ser detectado Y este es enfocado hacia una sola organización. (SOPHOS, 2018)

¿Por qué el sector de telecomunicaciones se ve afectado por ataques dirigidos?

El sector de telecomunicaciones se encuentra dentro de los primeros 10 sectores comúnmente atacados por parte de los ciberdelincuentes, pues operan la mayor parte de las redes y canales de comunicación de voz y datos. A su vez este sector usualmente almacena la mayor cantidad de información personal sensible de los ciudadanos haciéndolo un blanco de los cibercriminales.

Vulnerabilidades en Software.

El software inseguro a medida que se convierte un elemento de la infraestructura critica de una organización, sector o país aumenta su complejidad y la dificultad para lograr la seguridad en las aplicaciones.

Las vulnerabilidades en el software son un fallo de seguridad dentro de una aplicación a través de la cual los cibercriminales pueden llegan a comprometer la seguridad de toda la organización violando la confidencialidad, integridad y disponibilidad de la infraestructura y/o de la información. Las vulnerabilidades permiten a los atacantes obtener acceso no autorizado a la infraestructura para dar pie a un ataque dirigido.

Las principales diez (10) vulnerabilidades más comunes a las que se encontró expuesto el software en el 2019 son:

1. Inyección SQL "Lenguaje de Consulta Estructurada"

Se refiere a la colocación de código malicioso en declaraciones SQL a través de la entrada de información por medio de una página web. Esta es una de las técnicas más utilizadas por los cibercriminales, la cual puede destruir una base de datos completa o parcial de una organización. (OWASP, 2019)

2. Perdida o falta de Autenticación.

Las funciones del software o de aplicaciones relacionadas con la autenticación y la administración de sesiones son una vulnerabilidad latente para el sector de telecomunicaciones, debido a que a menudo se implementan de forma incorrecta, lo que permite a los atacantes comprometer las contraseñas, claves o tokens de sesiones, explotar otros defectos de implementación para asumir las entidades de otros usuarios de forma temporal o permanente durante todo el tiempo que dura el ataque. (OWASP, 2019)

3. Exposición de datos sensibles.

El software utilizado en las organizaciones frecuentemente se encuentra publicado a través de la Internet, estas aplicaciones usualmente no suelen proteger de manera correcta o adecuada la información que manejan. Los atacantes pueden llegar a robar o modificar dicha información para posteriormente realizar fraudes a través del uso de equipo de cómputo, ya sea por medio de fraude con tarjetas de crédito, robo de identidad u otros delitos. La información dentro de las aplicaciones puede verse comprometida sin protección adicional, como el cifrado de información en reposo o en tránsito, a su vez se requieren precauciones especiales cuando se intercambian entre el cliente y el servidor. (OWASP, 2019)

4. Entidades Externas (XLM/XXE).

XML por sus siglas en inglés significa Lenguaje de Marcado Extensible Y XXE se refiere a un ataque de falsificación de solicitud de un servidor. Esto quiere decir que los atacantes pueden explotar procesadores de lenguaje de marcado extensible si inyectan o cargan código vulnerable. Las entidades externas se pueden utilizar para revelar archivos internos utilizando un controlador de archivos, recursos compartidos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicios. (OWASP, 2019)

5. Pérdida de Control de Acceso

Las restricciones sobre a qué recursos los usuarios autenticados pueden hacer o acceder frecuentemente no se aplican de manera adecuada. Los atacantes pueden explotar estos defectos para acceder a la funcionalidad y/o datos no autorizados, como acceder a las cuentas de otros usuarios, visualizar archivos o información clasificada como sensible o confidencial, modificar los datos de otros usuarios, cambiar los permisos de acceso entre otras cosas. (OWASP, 2019)

6. Configuración Incorrecta de Seguridad.

Los errores de configuración de seguridad ocurren cuando algún componente es susceptible de ataque debido a una configuración incorrecta o una opción de configuración insegura. Los errores de configuración se convierten en vulnerabilidades tanto en los equipos fisicos de la infraestructura como en los aplicativos que residen en ella. (OWASP, 2019)

La configuración incorrecta de seguridad es una de las causas más comunes que representan una vulnerabilidad en el Software. Esto se debe a configuraciones predeterminadas e inseguras, configuraciones incompletas, almacenamiento de información interna en repositorios de acceso libre, mensajes de errores que contienen información específica y detallada de uso confidencial.

El impacto que la configuración incorrecta de seguridad representa para los operadores de comunicaciones fijas es que un atacante puede tener acceso no autorizado a la infraestructura o a

la información contenida en las aplicaciones, el resultado del ataque dependerá del grado de información contenida en la infraestructura o la aplicación comprometida.

7. Secuencia de Comandos de Sitios Cruzados ("Cross Site Scripting").

La secuencia de comandos de sitios cruzados es un tipo de vulnerabilidad contenida en el software usualmente asociado a las aplicaciones expuestas en internet. Esta vulnerabilidad permite a un usuario malicioso o mal intencionado a introducir código o instrucciones en una aplicación desde un lugar remoto.

El impacto que esta vulnerabilidad representa para el sector de telecomunicaciones es que si un sitio de internet de un operador es susceptible a esta vulnerabilidad, un atacante puede realizar diversos tipos de ataque basándose en la confianza que la pagina o aplicación inspira en el usuario, es decir desde redirigir a otro sitio para robar información mediante técnicas de ingeniería social, hasta lograr que un usuario autorizado descargue software que contiene una amenaza y lograr que este ejecute dicho programa. (OWASP, 2019)

8. Deserialización insegura.

La deserialización insegura es una vulnerabilidad que ocurre cuando los datos confiables se usan para abusar la lógica de una aplicación, infligir un ataque de denegación de servicio o incluso ejecutar código aleatorio para obtener acceso a la información o la infraestructura de una manera no autorizada. La deserialización consiste en transformar datos serializados provenientes de un archivo en un objeto. Es a qui donde se materializa la vulnerabilidad.

Es importante entender que esta vulnerabilidad afecta al sector de telecomunicaciones debido a que al materializarse puede causar graves consecuencias al permitir la denegación de servicios a usuarios válidos. (OWASP, 2019)

9. Utilización de componentes con vulnerabilidades conocidas.

Los componentes, como bibliotecas, marcos y otros módulos de software se ejecutan con los mismos privilegios de aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida grave de datos. Las aplicaciones que utilizan vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir varios tipos de ataques e impactos. (OWASP, 2019)

10. Registros y Monitoreo Insuficientes.

El registro y monitoreo de eventos insuficientes, junto con una mala gestión de incidentes de seguridad da pie a que los atacantes intenten atacar más de una vez a la infraestructura de telecomunicaciones sin ser detectados. En promedio una organización puede llegar hasta 200 días hasta detectar un incidente o brecha de seguridad en su infraestructura.

El mantener registros insuficientes también representa una amenaza al sector de telecomunicaciones debido a que en caso de materializarse un incidente y este requiera un proceso o denuncia legal, se podría ver afectado el proceso de cadena de custodia para la correcta gestión de incidentes de seguridad. (OWASP, 2019)

Vulnerabilidades en elementos de red e infraestructura critica.

Como infraestructura crítica nos referimos a cualquier componente, sistema, red, activo tanto físicos como virtuales, el cual es de suma importancia para las organizaciones tanto públicas como privadas y que al verse afectados puede causar un gran impacto en la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de estos.

Los riesgos a los que puede verse expuesta la infraestructura son múltiples desde condiciones climatológicas adversas, accidentes o fallas técnicas, ciberataques, terrorismo e incluso pandemias. De igual manera existen vulnerabilidades en la infraestructura al retirar o remover de sus funciones a personal altamente calificado para la operación cotidiana de la infraestructura. (NIST, 2018)

¿Por qué el sector de telecomunicaciones se ve afectado por las vulnerabilidades en los elementos de red?

Como hemos mencionado los riesgos a los que la infraestructura se ve expuesta son múltiples, en el caso de los eventos naturales las tormentas y fuertes vientos pueden causar interrupciones en el servicio de los usuarios. Existe la amenaza de que la infraestructura del sector de telecomunicaciones se vea afectada por actividad criminal, debido a que los delincuentes buscan obtener algún beneficio manipulando los recursos de los operadores.

Algunos grupos especializados de terrorismo cuentan con recursos suficientes para llevar acabo espionaje en las redes de los operadores, buscando obtener información sensible para beneficio de algún grupo.

Atacantes Internos.

Las amenazas pueden servir a múltiples factores como lo hemos mencionado (ej. fraude, extorsión, robo de información, venganza o simplemente por ganar reconocimiento entre grupos de cibercriminales). Los atacantes internos son personas que trabajan o han trabajado dentro de las organizaciones siguiendo los procesos establecidos de reclutamiento y en algunos casos sin motivación maliciosa.

Un atacante interno se resume en una persona con acceso autorizado y con cierto grado de confianza para acceder a la infraestructura y los sistemas que la soportan. (FBI, 2019)

¿Por qué el sector de telecomunicaciones se ve afectado por atacantes internos?

Existen múltiples factores que pueden hacer a una persona volverse una amenaza para las organizaciones:

Beneficio económico es decir la creencia de que el dinero resuelve todo o deudas excesivas. Enojo o venganza que son múltiples factores que llevan a las personas hasta el grado de tomar represalias en contra de la organización, la falta de reconocimiento, desacuerdos con otros empleados, insatisfacción con las funciones de trabajo.

La ideología de las personas es otra de las amenazas que un atacante interno usualmente suele verse afectado o influenciado al querer apoyar a una causa en particular o el querer pertenecer a algún grupo social. La habilidad de tener acceso información confidencial o sensible y el no recibir una adecuada capacitación en cómo manejar y clasificar la información termina siendo una amenaza a la que comúnmente se enfrentan las organizaciones.

La falta de políticas y procedimientos establecidos para el correcto desarrollo de sus actividades o la falta de tiempo y la presión de formalizar algún entregable usualmente hace que los empleados busquen formas alternativas para lograr sus metas aun cuando estas van en contra de los lineamientos establecidos.

Amenazas dirigidas a los suscriptores de proveedores de contenido y servicios.

Actualmente en el mundo de la tecnología y seguridad de información se considera a el factor humano como el eslabón más débil de la cadena. Es decir, los suscriptores de proveedores de telecomunicaciones tanto de contenido como de servicios de internet. Las organizaciones realizan un gran esfuerzo en establecer controles tecnológicos y administrativos para proteger la confidencialidad, integridad y disponibilidad de la información es por esto por lo que los cibercriminales usualmente enfocan sus esfuerzos en engañar y manipular a los usuarios finales para lograr sus objetivos.

El papel del usuario final es fundamental para prevenir incidentes de seguridad, es por esto por lo que los operadores de telecomunicaciones deben de estar constantemente generando campañas de concientización sobre el correcto manejo de contenido por parte del usuario final ya que son estos los que utilizan la información o los servicios, estos deben estar conscientes de sus responsabilidades al utilizar contenido o servicios.

¿Por qué el sector de telecomunicaciones se ve afectado por amenazas dirigidas a los suscriptores?

Los cibercriminales siempre se enfocarán sus esfuerzos en vulnerar al eslabón más débil, como ya mencionamos son las personas. Entre las técnicas comúnmente utilizadas para vulnerar al ser humano en el sector de telecomunicaciones encontramos:

1) **Manipulación de suscriptores.**

Se produce cuando un individuo o grupo de individuos ejercen una forma de control sobre el comportamiento de otro con el fin de obtener algún beneficio. Este tipo de amenaza afecta a los operadores puesto que usuarios validos con algún tipo de confianza brindada por la compañía pueden llevar a cabo acciones de manera consciente o inconsciente la cual pudiese afectar de manera negativa el curso normal de las operaciones. (FBI, 2019)

2) **Ingeniería social**

Este tipo de amenaza es el ataque más peligro al que se encuentran expuestos tanto los operadores de servicio como los suscriptores debido a que este tipo de ataques consiste en manipular la confianza e ingenuidad o desconocimiento de los usuarios con el objetivo de que proporcionen

información que pueda ser utilizada por los cibercriminales en ataques posteriores. La ingeniería social pretende abarcar la mayor cantidad de usuarios y el nivel de exposición para los ciberdelincuentes es muy bajo y con una tasa muy baja de detección.

La ingeniería social no siempre utiliza herramientas tecnológicas para materializarse, es decir que una personal mal intencionada puede llegar a utilizar cartas, llamadas telefónicas, conversaciones presenciales o noticias falsas publicadas por medios impresos para lograr su objetivo. (UNAM, 2011)

3) Phishing.

El phishing es un tipo de ataque que busca a través de diferentes medios recolectar información personal, sensible o confidencial tanto como de los proveedores de servicio como de los usuarios finales. Es básicamente un fraude en el que el estafador se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa formalmente establecida. El phishing usualmente llega a los usuarios por medio de correo electrónico, mensajes electrónicos, conversaciones telefónicas o presenciales.

Cuando un usuario cae en el engaño, este puede llegar revelar información sensible y confidencial, habilitar puertas traseras a la infraestructura de los operadores sin conocimiento de que lo hizo y los cuales posteriormente los cibercriminales utilizaran para tener accesos no autorizados, realizar ataques persistentes y lograr el robo o secuestro tanto de la información como la infraestructura de la persona o compañía. (CSO Online, 2020)

4) Kits o módems vulnerables.

Los módems son dispositivos que los suscriptores utilizan para tener acceso a los servicios e infraestructura de los operadores el cual permite la comunicación entre los equipos.

Las vulnerabilidades existentes en los kits o módems pueden ser utilizadas por ciberdelincuentes infectando equipos con código malicioso de forma remota, permitiendo que el tráfico o información generada por el modem y enviada al proveedor sea susceptible de intercepción o robo, revelando la ubicación física del suscriptor, así como permitiendo la capacidad de los delincuentes acceder y modificar las configuraciones de seguridad por defecto de manera no autorizada.

Las siguientes figuras representan al sector de telecomunicaciones en el séptimo y octavo lugar de sectores con más amenazas dirigidas durante el 2018 y 2019:

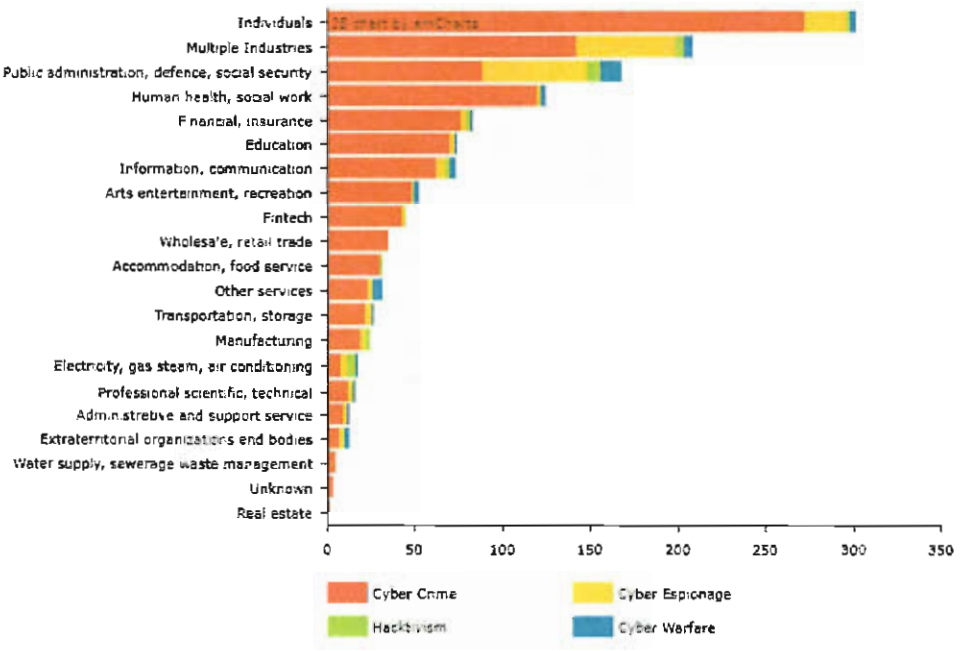


Fig. 15 sectores de la Industria con más Amenazas. (HACKMAGEDDON, 2018)

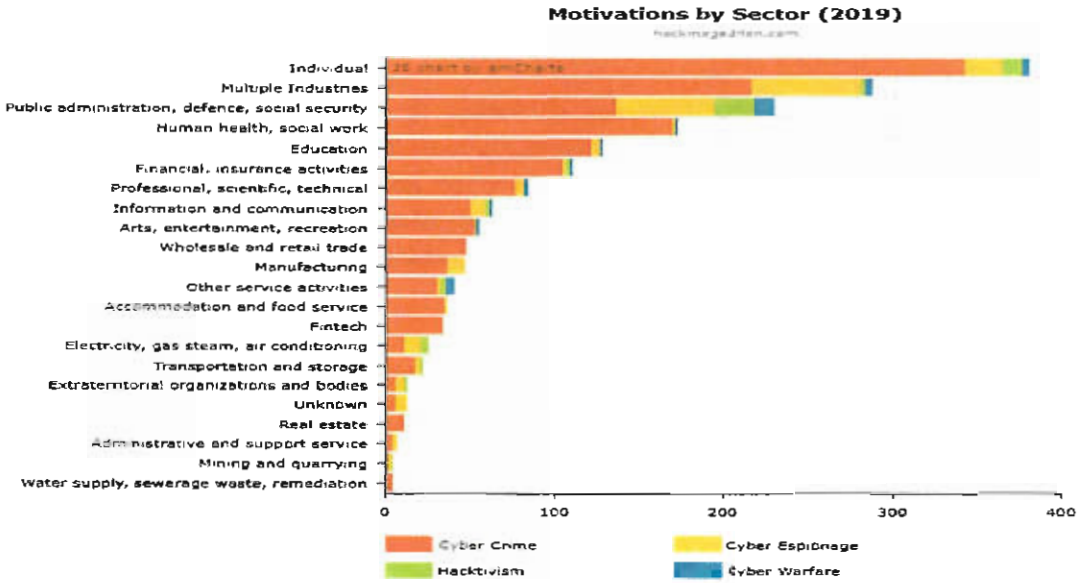


Fig. 16 sectores de la Industria con más Amenazas. (HACKMAGEDDON, 2019)

19. Conclusión sobre las amenazas en la industria de telecomunicaciones.

Las telecomunicaciones son parte critica de la infraestructura de las naciones y debe ser protegida de manera correcta, el panorama de amenazas aquí expuesto muestras múltiples vectores de ataque que los cibercriminales pueden utilizar para llevar acabo sus ataques o acciones mal intencionadas. Es por esto por lo que los operadores de telecomunicaciones fijas cuenten con controles administrativos y tecnológicos para reducir el impacto que los riesgos representan en la infraestructura.

En las siguientes secciones del presente documento se encontrarán las recomendaciones básicas de controles de seguridad para mitigar las amenazas aquí expuestas.

20. Medidas para la mitigación de amenazas.

La seguridad de información nos ayuda a proteger los activos que valoramos, una vez identificadas las amenazas comunes a las que se encuentran expuestos los concesionarios de telecomunicaciones procederemos a proponer las soluciones técnicas, físicas y administrativas adecuadas para que los concesionarios autorizados que presenten los servicios cumplan con mayor grado de eficacia el objetivo de preservar la privacidad, confidencialidad, integridad y disponibilidad de la infraestructura y la información de los suscriptores.

Para establecer las medidas necesarias con el objetivo de mitigar las amenazas necesitamos establecer que la mitigación propuesta será representada en forma de controles o contramedidas. Por control nos referimos el medio de gestionar el riesgo, que incluye políticas, procedimientos, lineamientos que pueden ser de naturaleza administrativa, técnica, gerencia o legal y por contramedidas, es decir cualquier proceso que reduce directamente una amenaza o vulnerabilidad.

Los controles pueden llegar a ser del tipo:

1) **Preventivo:** Controles necesarios para bloquear un ataque o al cerrar las posibles vulnerabilidades que pueden ser utilizadas previo a un ataque.

2) **Contención:** Controles necesarios para que el llevar acabo un ataque sea más difícil más sin embargo no imposible.

3) **Detección:** Controles que permiten detectar un ataque cuando ocurre o poco tiempo después de ocurrido.

4) **Reactivo:** Controles necesarios para investigar, analizar y registrar los fallos en el sistema o infraestructura.

5) **Correctivo:** Son controles o medidas que aseguran tomar acciones para revertir un evento no deseado.

Las medidas para mitigar las amenazas pueden ser agrupados en tres principales clases o grupos los cuales son independientes uno del otro.

Fuente: (F5 Labs, 2019)

1) **Medidas Físicas:** Son medidas que consisten en la aplicación de barreras físicas y procedimientos de control como medidas de prevención, contención, detección contra las amenazas a la infraestructura e información de los operadores y suscriptores. Es decir, los procesos, normas y mecanismos de implementación que controlan el acceso a los sistemas de información, a los recursos y al acceso físico a las instalaciones.

2) **Medidas Procedurales o Administrativas:** Son las reglas, procedimientos y prácticas que están relacionados con la efectividad operativa, la eficiencia y el cumplimiento con las regulaciones y políticas gerenciales.

3) **Controles Técnicos o de aplicación:** Las políticas, procedimientos y actividades diseñadas para proporcionar una seguridad razonable de que se alcancen los objetivos relevantes para una determinada solución automatizada (software o hardware).

Fuente: (F5 Labs, 2019)

21. Recomendaciones administrativas para la mitigación de amenazas.

Las siguientes recomendaciones son medidas preventivas para la mitigación de amenazas en el sector de telecomunicaciones:

1. Establecer una estrategia de seguridad de información.

Establecer y/o mantener una estrategia de seguridad de la información alineada con las metas y los objetivos de la organización para orientar el establecimiento y/o la administración continua del programa de seguridad de información. Una estrategia debe tener presente que la seguridad de la información nunca es estática. Las amenazas, las vulnerabilidades y las exposiciones cambian permanentemente debido a factores internos y externos. Para que esta sea efectiva debe ser un documento vivo con objetivos, enfoques y métodos que cambien para cumplir con nuevas condiciones.

2. Implementación y operación de Sistemas de Gestión de Seguridad de Información.

Una vez establecida una estrategia en materia de seguridad de información para mitigar las amenazas a las que se encuentran expuestos los operadores de telecomunicaciones se debe buscar un "estado deseado" el cual utilizaremos para denotar un panorama completo de todas las

condiciones relevantes en un punto particular en el futuro. Para lograr un estado deseado sólido se deben incluir principios, políticas y marcos de referencia, procesos, estructuras, cultura y ética para la información, servicios, infraestructura, aplicaciones para las habilidades y competencias de las personas.

La implementación y operación de un sistema de gestión de seguridad de información en términos puramente cuantitativos puede llegar a ser imposible. En consecuencia, la implementación debe establecerse en términos cualitativos. Ejemplo, proteger los intereses de aquellos que dependen de la información y a los procesos, los sistemas y las comunicaciones que manejan almacenan y entregan, de sufrir algún daño que sea de consecuencia de fallas en la disponibilidad, confidencialidad e integridad de la información.

Para la implementación y operación de sistemas de gestión se cuentan con múltiples enfoques actualmente aceptados a nivel mundial. Se recomienda se sigan estas buenas prácticas de la industria sin ser requisito indispensable llevar su cumplimiento obligatorio a un nivel de certificación en cada una de estas prácticas. A fin de garantizar que todos los elementos relevantes de la seguridad estén cubiertos en una estrategia de seguridad organizacional considerando el:

1) Asegurar los activos críticos.
2) Administrar los riesgos de manera efectiva.
3) Mejorar y mantener la confianza de los subscriptores.
4) Demostrar conformidad con las mejores prácticas internacionales.
5) Evitar daños de marca, pérdida de ganancias o posibles multas regulatorias.

Objetivos y Principios de Control para la Información y Tecnología

El estado deseado para la seguridad de la información puede ser basado considerando de manera cualitativa mas no limitativa seis (6) principios para el sistema de gobierno y gestión de la tecnología y seguridad de información.

a) Principio 1 Proporcionar valor a las necesidades de las partes interesadas:

Las organizaciones existen para crear valor para sus grupos de intereses, manteniendo un equilibrio entre la realización de beneficios, la optimización del riesgo y el uso de recursos. Cada empresa necesita un sistema de gobierno para satisfacer las necesidades de las partes interesadas y generar valor del uso de la Tecnología de Información. El valor refleja un equilibrio entre el beneficio, el riesgo y los recursos, y las empresas necesitan una estrategia y un sistema de gobierno práctico para materializar este valor.

b) Principio 2 Enfoque Holístico:

Un sistema de gobierno para la Tecnología de Información de la empresa se crea a partir de una serie de componentes que pueden ser de distinto tipo y que funcionan conjuntamente de forma holística.

c) Principio 3 Sistema de Gobierno Dinámico:

Un sistema de gobierno debería ser dinámico. Esto significa que cada vez que se cambian uno o más factores del diseño (p. ej. un cambio de estrategia o tecnología), debe considerarse el impacto de estos cambios en el sistema de Gestión de Seguridad de Información y Tecnología. Una visión dinámica llevará a un sistema de Gestión correctamente preparado para el futuro.

d) Principio 4 Separar Gobierno de la Gestión:

El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas y la gestión planifica, construye, ejecuta y controla actividades. Esto permite a las empresas optimizar la inversión y la rentabilidad en beneficio de las partes interesadas.

e) Principio 5 Adaptar las necesidades de la empresa:

Un sistema de gobierno debería personalizarse de acuerdo con las necesidades de la empresa, utilizando una serie de factores de diseño como parámetros para personalizar y priorizar los componentes del sistema de gobierno.

f) Principio 6 Sistema de Gobierno Integro:

Un sistema de gobierno debería cubrir la empresa de principio a fin, centrándose no solo en la función de TI, sino en todo el procesamiento de tecnología e información que la empresa pone en funcionamiento para lograr sus objetivos, independientemente de dónde se realice el procesamiento en la empresa.

Los principios generales a considerar para un Marco de Gobierno adecuado de manera cualitativa mas no limitativa dependiendo de cada empresa deberán ser:

1) Basados en el modelo conceptual:

Un marco de gobierno se debería basar en un modelo conceptual que identifique los componentes principales y las relaciones entre componentes para maximizar la uniformidad y permitir la automatización.

2) Abierto y flexible:

Un marco de gobierno debería ser abierto y flexible. Debería permitir la incorporación de nuevo contenido y la capacidad para abordar nuevos asuntos de la forma más flexible, mientras mantiene la integridad y uniformidad.

3) Alineado con las principales normativas:

Un marco de gobierno debería alinearse con los principales estándares, marcos y regulaciones relacionados.

Fuente: (ISACA, 2020)

I. Modelo de Madurez de Capacidad

La integración de un modelo de madurez es una estructura de mejora de la capacidad que ofrece orientación a las organizaciones para elevar el desempeño. Este modelo ayuda a comparar las actividades contra buenas prácticas identificando brechas de desempeño. Las organizaciones que deciden operar en niveles de madurez más elevados fomentan capacidades y promueven procesos

más efectivos logrando una mayor calidad, satisfacción del cliente, mejor retención de empleados y mejor rentabilidad. Los niveles de madurez dependen de la cantidad de recursos disponibles de cada organización, las regulaciones aplicables y la estrategia establecida por la alta dirección en materia de seguridad de información.

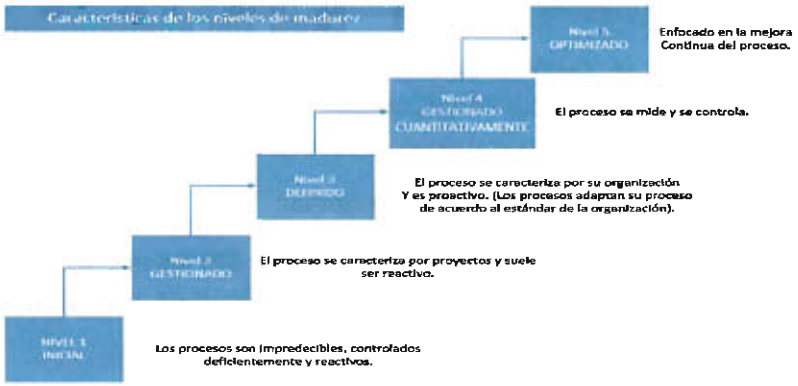


Fig. 17 características de los Niveles de madurez (CMMI Institute, 2020)

II. Sistemas de gestión de Seguridad para Protección de Datos Personales. (SEGOB, 2013)

En las recomendaciones en materia de seguridad de datos personales publicadas en el Diario Oficial de la Federación el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se recomienda la implementación y operación de un Sistema de Gestión de Seguridad de Datos Personales (SGDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), para la protección de datos personales alineado a estándares internacionales.

III. Guía de cumplimiento para LFPDPPP. (INAI, 2016)

El sistema de gestión propuesto para el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares se basa en el modelo (PHVA). Los operadores de telecomunicaciones podrán optar por este sistema con base a las Guías para implementar un Sistema de Gestión de Seguridad de Datos Personales junio 2015 las cuales establecen:

Fase	Actividades
Planificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado por la organización (Meta).
Hacer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
Verificar	Evaluar y medir los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
Actuar	Adoptar medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras informaciones relevantes, para lograr la mejora continua

Fig. 18 ciclo General del Sistema de Gestión de Seguridad en Datos Personales

Las acciones que los operadores de telecomunicaciones se les recomiendan llevar a cabo para la seguridad de los datos personales, basadas en el ciclo PHVA, considerando que cada uno de los pasos del SGSDP debe mantener un adecuado registro documental, el cual se resume en el siguiente gráfico.

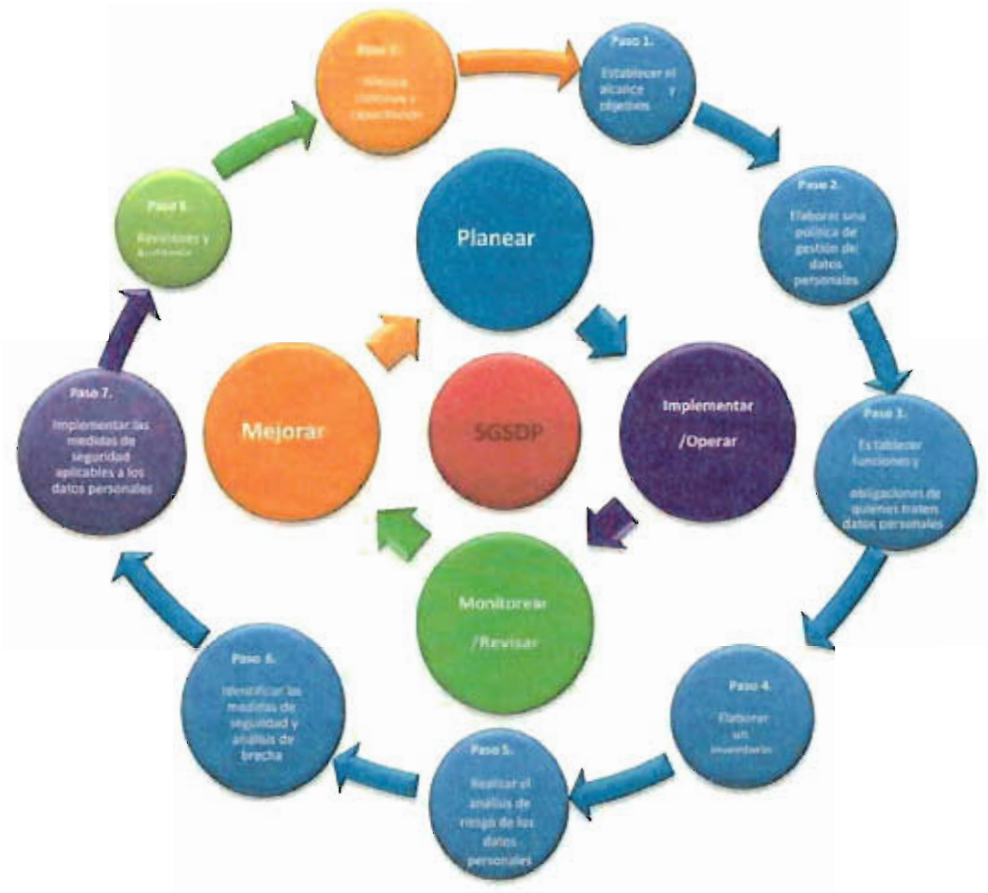


Fig. 19 acciones para la seguridad de los datos personales.

De manera simplificada el INAI recomienda una síntesis de pasos para la implementación de un SGSDP que incluye:

1. Presentación
2. Descripción del Sistema de Gestión de Seguridad de Datos Personales.
    I. Planear
        i. Alcance y Objetivos.
        ii. Definición de política de Gestión de Datos Personales.
        iii. Funciones y Obligaciones de quienes traten los datos.
        iv. Inventario de Datos Personales.
        v. Análisis de Riesgo de los Datos Personales.

vi. Identificación de las medidas de seguridad y Análisis de Brecha.

II. Implementar y Operar el SGSDP.
   i. Implementación de las medidas de seguridad aplicables a los datos personales.
   ii. Plan de tratamiento para la implementación de las medidas de seguridad.

III. Monitorear y Revisar el SGSDP.
   i. Revisiones y Auditoria.

IV. Mejorar el SGSP.
   i. Mejora continua.
   ii. Capacitación.

Puede ser de utilidad emplear una combinación de métodos para describir el estado deseado a fin de contribuir a la protección de la privacidad de información de los operadores de telecomunicaciones y los subscriptores. Se recomienda se sigan estos enfoques y metodologías de la industria sin ser requisito indispensable llevar su cumplimiento obligatorio a un nivel de certificación en cada una de estas prácticas.

3. **Sistema de Gestión de Incidentes de Seguridad.** (BSI, 2016)

La gestión y respuesta a incidentes es el componente operativo de la gestión de riesgos. Están incluidas las actividades que tienen que lograrse como resultado de amenazas no anticipadas, perdidas, robo, accidentes o cualquier evento adverso inesperado que ocurra como resultado de controles fallidos o inexistentes.

No existe un único enfoque que cumpla con los requerimientos de gestión de incidentes de seguridad para cada organización; más bien es responsabilidad de los operadores de telecomunicaciones establecer un enfoque que incluya de manera enunciativa mas no limitativa:

1) La comunidad de usuarios a prestar servicios.
2) Misión, metas y objetivos de la organización.
3) Servicios provistos.
4) Modelos de negocio de la organización.
5) Financiamiento para los costos de puesta en funcionamiento y las operaciones en curso.
6) Recursos necesarios por el equipo de respuesta a incidentes.

Estos enfoques pretender mitigar el impacto de un incidente al materializarse teniendo en cuenta:

1) Proporcionar un medio efectivo de abordar la situación de manera tal que minimice el impacto a la empresa.
2) Brindar a la Gerencia suficiente información para decidir los cursos de acción apropiados.
3) Mantener o restaurar la continuidad de los servicios de la empresa.
4) Proporcionar una defensa contra ataques posteriores.
5) Proveer disuasión adicional mediante el uso de tecnología, investigación y acusación para la correcta impartición de justicia.

El alcance de la gestión de incidentes y la capacidad de respuesta deben estar en equilibrio con la seguridad básica, la continuidad de negocio y la recuperación ante desastres.

Las empresas que implementan un sistema de gestión de respuesta a incidentes pueden llegar a:

1) Detectar incidentes rápidamente.
2) Diagnosticar incidentes con exactitud.
3) Reducir y minimizar los daños.
4) Restaurar los servicios afectados.
5) Determinar la causa raíz.
6) Implementar mejoras para evitar que se repitan.
7) Documentar e informar.
8) Seguimiento adecuado de procesos de impartición de justicia.

Fig. 20 flujo de proceso recomendado del plan de respuesta a incidentes.

Cuando se desarrolla un Sistema de Gestión de Incidentes pueden existir retos inesperados como la falta de participación de la gerencia, Incompatibilidad entre empresas, rotación excesiva de personal, falta de comunicación por lo que las empresas de telecomunicaciones deberán considerar múltiples desafíos para la correcta implementación de un efectivo Sistema de Gestión de Incidentes de Seguridad.

4. Capacitación a los usuarios

Como última media administrativa para mitigación de amenazas se recomienda la capacitación, la formación y la concientización como elemento fundamental para que la estrategia de seguridad de información desarrollada por los operadores de telecomunicaciones sea efectiva. Como hemos mencionado el eslabón más débil en la cadena de seguridad es el ser humano como operador y como usuario final. Se debe considerar la necesidad de desarrollar métodos y procesos que permitan que las políticas, estándares y procedimientos sean más fáciles de seguir, implementar y monitorear.

Un programa recurrente de concientización sobre seguridad de información y amenazas que afectan al sector de telecomunicaciones dirigido a usuarios finales refuerza la importancia de mantener la confidencialidad, integridad y disponibilidad de información y a su vez varias regulaciones como la Ley Federal de Protección de Datos Personales en Posesión de Particulares lo han establecido como requerimiento por ley para varios sectores.

Capacitar a personal de nuevo ingreso o personal ya existentes para dotarlos de habilidades necesarias para proteger la infraestructura e información de forma adecuada es una opción más rentable como medida de prevención previo a una amenaza explotar vulnerabilidades y causar incidentes de seguridad de información.

Es importante resaltar que los operadores de telecomunicaciones que enfoquen las campañas de concientización dirigidas a sistemas, procesos y políticas específicas aprovecharán de manera eficiente la asignación de recursos debido a que este enfoque puede integrarse perfectamente a los programas e iniciativas existentes de la organización, apoyar áreas deficientes y alinear los procesos de seguridad con los procesos de negocio. Fuente: (INAI, 2015)

Como marco de referencia para desarrollar un programa de capacitación y concientización de tecnología y seguridad de información se recomienda:

Fig. 21 Pasos necesarios para la implementación de un programa de capacitación. (SANS, 2020)

22. Medidas tecnológicas para la mitigación de amenazas en el sector de telecomunicaciones.

Las medidas tecnológicas nos permiten establecer las reglas, procedimientos, y prácticas que están relacionadas con la efectividad operativa, la eficiencia y el cumplimiento con las políticas definidas por la alta dirección, así como los marcos regulatorios aplicables.

La siguiente lista de controles tecnológicos se sugiere considerar de manera enunciativa mas no limitativa para mantener la confidencialidad, integridad y disponibilidad de la información.

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
Actualizaciones de Seguridad	Son acciones que giran en torno a los problemas que se descubren en las	Permite evitar problemas de vulnerabilidades y de funcionamiento para	Preventivo Reactivo Correctivo	• Vulnerabilidades en Software. • Vulnerabilidades en elementos de

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
	aplicaciones y sistemas operativos.	reducir las amenazas que pueden ser utilizadas en ataques informáticos.		red e infraestructura critica. • Kits o módems vulnerables.
Antivirus	Herramienta Tecnológica para análisis de amenazas en servidores y estaciones de trabajo en red corporativa. Revisiones y actualizaciónes periódicas de seguridad sobre elementos de la red de servicios.	Detecta la presencia de virus informáticos y brinda la capacidad de eliminarlos.	Preventivo Contención Detección Reactivo Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica (donde aplique). • Infecciones por código malicioso.
Anti-DDOS DNS	Sistemas contra la denegación de ataques de servicios contra los sistemas de nombres de dominio.	Previene a los atacantes el saturar los sistemas de nombres de dominio los cuales proporcionan las rutas para acceder recursos y contenidos disponibles en Internet.	Preventivo Contención Detección Reactivo	• Denegación de Servicios Distribuidos (DDOS) (donde aplique). • Ataques Dirigidos
Anti-DDOS Perimetral	Sistemas contra ataques de servicios en los FW perimetrales, para las redes que aplique.	Previene y proteger de los atacantes la saturación de los servicios de infraestructura de los operadores de telecomunicaciones.	Preventivo Contención Detección Reactivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos
Anti DDOS Web	Sistemas contra la denegación de ataques de servicios contra los aplicativos expuestos en Internet.	Previene a los atacantes el saturar los aplicativos expuestos en Internet logrando la disponibilidad de los recursos se encuentre disponible en todo momento para los suscriptores de contenido.	Preventivo Contención Detección Reactivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos
Anti-Phishing	Herramienta que previene el robo de datos e información sensible	Permite identificar, analizar y bloquear el contenido malicioso proveniente de	Preventivo Contención Detección	• Ataques Dirigidos • Manipulación de suscriptores.

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
		correos electrónicos, sitios web y generalmente proporciona una alerta al usuario		• Ingeniería social • Phishing
Balanceadores de Carga	Herramienta que permite distribuir de forma eficiente el tráfico proveniente de Internet.	De manera automatizada permite compartir la carga de trabajo entre varios procesos, ordenadores, discos u otros componentes.	Contención Reactivo Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Kits o módems vulnerables.
Borrado Seguro de Información	Software para la eliminación efectiva de información.	Permite el borrado seguro de información almacenada en medios digitales que vayan a ser dados de baja o eliminados por parte de alguna dependencia.	Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos.
Certificados de Autenticación	Herramienta que permite realizar comunicaciones, comercio electrónico e interacciones de forma segura en Internet.	Herramienta para evitar el acceso de equipos no autorizados o con identificadas falsas.	Preventivo Contención	• Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica.
Cifrado de Archivos, Bases de Datos, Sesiones.	Conversión de datos de un formato legible a un formato codificado.	Preserva la confidencialidad de la información contenida en diversos medios ante robo o perdida.	Preventivo	• Ataques Dirigidos • Atacantes Internos. • Manipulación de suscriptores.
Configuración Segura en Equipos de Información	Especificaciones de configuraciones para los equipos de cómputo.	Establecer e implementar configuraciones automatizadas para todos los sistemas en la infraestructura.	Preventivo Correctivo	• Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Control de acceso a nivel de puerto	Control de acceso tecnológico que permite la gestión de autenticación de dispositivos en la red.	Permite la implementación de control de acceso a nivel de puertos de red según el estándar 802.1x para asegurar que solo equipos	Preventivo detección Reactivo Correctivo	• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica.

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
		autorizados se pueden conectar a la red.		• Atacantes Internos.
Firewall de Aplicaciones Web	Es un dispositivo cuya función es gestionar la seguridad entre redes.	Permite verificar y validar el tráfico que va al servidor de una aplicación. Cualquier tráfico no autorizado es registrado y bloqueado.	Preventivo Contención Detección	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP.
Firewall Siguiente Generación	Es un dispositivo cuya función es gestionar la seguridad entre redes.	A diferencia de un Firewall tradicional contiene funcionalidades de detección de intrusos (IPS), prevención de intrusos (IDS), control de aplicaciones, prevención de perdida de datos (DLP), autenticación de usuarios, antivirus y filtrado de trafico de internet.	Preventivo Contención Detección	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Firewall Tradicional	Es un dispositivo cuya función es gestionar la seguridad entre redes.	Dispositivo diseñado para bloquear solo el acceso no autorizado, permitiendo solo las comunicaciones autorizadas.	Preventivo Contención Detección	• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Fuentes de Tiempo Sincronizadas	Sincronización de relojes de los sistemas informáticos de una sola fuente	Debido a que las aplicaciones y los dispositivos sean capaces de sincronizar los tiempos en los relojes para mantener una sola configuración y permitir la gestión de incidentes.	Correctivo Reactivo	• Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica.
Gestión de Cuentas Privilegiadas	Tecnología para ejercer control sobre el acceso elevado o privilegiado y los permisos para usuarios.	Permite identificar y gestionar de manera automatizada las cuentas administrativas tanto de domino como locales para	Preventivo Contención Reactivo Correctivo	• Ataques Dirigidos • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
		garantizar que solo usuarios autorizados tengan privilegios elevados.		• Phishing
Gestión de Identidades y Acceso	Un sistema integrado de políticas y procesos organizacionales.	Permite controlar el acceso a los sistemas de información y a las instalaciones con el objetivo de proteger la información e infraestructura.	Preventivo Contención	• Ataques Dirigidos • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing
GRC	Gobernanza, gestión de Riesgos y Cumplimiento.	Permite la toma de decisiones, coordinación de políticas y controles de manera automatizada para su correcto seguimiento y vigilancia.	Preventivo	• Manipulación de suscriptores.
Herramienta de Descubrimiento de Activos	Herramienta para descubrir todos los dispositivos en la infraestructura administrada por los proveedores.	Permite la Identificación de todos los dispositivos conectados a la infraestructura para actualizar el inventario de activos.	Prevención Detección	• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos. • Manipulación de suscriptores. • Kits o módems vulnerables.
Herramienta de Gestión de configuración	Especificaciones de configuraciones para los equipos de cómputo.	Permite la gestión de configuración de sistema que automáticamente fuerzan y vuelven a implementar los parámetros de configuración en los sistemas en intervalos programados.	Detección Reactivo Correctivo	• Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables
Herramienta de Respaldo de Información	Copias de seguridad de información.	Genera la capacidad de llevar un historial de respaldos, realiza copias de información que permiten volver a un punto del tiempo posterior a un incidente.	Preventivo Reactivo Correctivo	• Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
				infraestructura critica. • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing
IDMS	Sistemas Inteligentes para Mitigación de denegación de servicios.	Proporciona la capacidad de detectar ataques incluso con tráfico cifrado, protección contra amenazas saliente.	Preventivo Contención Detección Reactivo Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos
IDS	Sistemas de detección de Intrusos.	Sistemas basados en red para buscar mecanismos de ataques inusuales y detectar el compromiso de estos sistemas en cada uno de los elementos de red de la organización.	Detección	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos.
IPS	Sistemas de prevención de Intrusos.	Sistemas basados en red para bloquear mecanismos de ataques inusuales y detectar el compromiso de estos sistemas en cada uno de los elementos de red de la organización.	Preventivo Contención Detección Reactivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos.
Listas blancas de aplicaciones	Inventario de aplicaciones permitidas en la infraestructura.	Permite asegurar que solo aplicaciones permitidas se encuentran en los equipos de cómputo de la organización y prevenir la ejecución de software no autorizado en dichos activos.	Detección Preventivo	• Ataques Dirigidos • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing
Múltiple Factor de Autenticación	Método de control de acceso para sistemas y aplicaciones.	Permite el acceso autorizado a los recursos solo después de haber presentado dos o	Preventivo	• Denegación de Servicios Distribuidos (DDOS).

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
		más pruebas de quien es quien dice ser.		• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing • Kits o módems vulnerables.
Programa electrónico de capacitación	Herramienta tecnológica para concientización sobre amenas de denegación de servicios distribuidos.	Concientizar al usuario para identificar la amenaza y reportar incidentes de manera efectiva.	Preventivo	• Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing
Proxy server	Programa o dispositivo que actúa como intermediario entre un cliente y un servidor.	Permite asegúrese de que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación autenticado que esté configurado para filtrar conexiones no autorizadas.	Detección Contención Reactivo Correctivo	• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica.
Pruebas de Penetración	Es un ataque a un sistema en la infraestructura con la intención de encontrar debilidades de seguridad.	Permite encontrar de manera proactiva las vulnerabilidades a las que se encuentran expuestos todos los elementos de la infraestructura para su correcta mitigación previo a que un ataque se materialice.	Preventivo Detección Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Pruebas de Vulnerabilidades	Pruebas que identifican vulnerabilidades conocidas en la infraestructura.	Permite escanear todos los dispositivos en la red de forma automatizada con el fin de identificar vulnerabilidades en los equipos e	Preventivo Detección Reactivo Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
		infraestructura de los operadores de telecomunicaciones.		• Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Registro de DHCP	Herramienta para actualizar el registro de activos.	Permite identificar todos los dispositivos conectados a la infraestructura para actualizar el inventario de activos.	Preventivo detección	• Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos.
Sandbox	Aislamiento de procesos o entorno aislado.	Permite ejecutar programas con seguridad y de manera separada para revisar la confiabilidad de código o software de terceros.	Preventivo Contención Detección	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Kits o módems vulnerables.
Seguridad en correo electrónico	Autenticar los correos electrónicos entrantes y salientes de la compañía.	Para reducir la posibilidad de correos electrónicos falsificados o modificados se debe implementar políticas basadas en la Autenticación de Mensajes Basada en Dominio, Reportes y Conformidad (DMARC).	Preventivo Detección	• Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Manipulación de suscriptores. • Ingeniería social • Phishing
SIEM	Sistema de Gestión de Eventos e	Habilita la capacidad de centralizar la información y	Preventivo	• Denegación de Servicios

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
	Información de Seguridad.	permite la correlación e interpretación de datos de seguridad identificando tendencias y patrones no deseados.		Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos. • Kits o módems vulnerables.
SOC	Centro de Operaciones de Seguridad.	Es una central de operaciones de seguridad que previene, monitorea y controla la seguridad en la organización.	Preventivo Contención Detección Reactivo Correctivo	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Vulnerabilidades en Software. • Vulnerabilidades OWASP. • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos. • Manipulación de suscriptores. • Ingeniería social • Phishing • Kits o módems vulnerables.
UEBA	Análisis de comportamiento de usuarios.	Detecta y previene amenazas de personas internas mediante el análisis de comportamiento de los usuarios.	Preventivo Detección	• Denegación de Servicios Distribuidos (DDOS). • Ataques Dirigidos • Atacantes Internos. • Kits o módems vulnerables.

Control	¿Qué es?	¿Por qué implementarse?	Tipo de control	Amenaza Atendida
VPN	Red Privada Virtual.	Es una tecnología que permite establecer canales de comunicación segura entre equipos de cómputo a través de redes públicas para mantener la confidencialidad de la información.	Preventivo	• Ataques Dirigidos • Vulnerabilidades en elementos de red e infraestructura critica. • Atacantes Internos. • Manipulación de suscriptores.

Tabla N°4 Lista de controlos tecnológicos.

23. Recomendaciones del Centro para la Seguridad de Internet.

(CIS por sus siglas en Ingles) (CIS, 2020)

Como hemos mencionado en la sección anterior, existen múltiples herramientas disponibles para la protección de la privacidad e información de los operadores de telecomunicaciones y de los suscriptores de contenido. Las organizaciones pueden optar por la implementación de algunos o todos los controles sugeridos, esto dependerá del nivel de madurez y la disponibilidad de recursos de cada organización.

El Centro para la Seguridad de Internet recomienda un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes de información. La recomendación para los operadores de telecomunicaciones en adoptar las recomendaciones y controles los cuales están enfocados con base al principio de que la ofensa es la mejor defensa, priorización, mediciones y métricas, diagnóstico y mitigación continua, así como la automatización.

24. Medidas físicas para la mitigación de amenazas en el sector de telecomunicaciones.

La siguiente lista de controles fisicos son aplicables para lograr el debido cumplimiento de protección en seguridad de información y privacidad de manera enunciativa mas no limitativa.

Control	Objetivo	Tipo de Control	Amenaza Atendida
Acceso físico	Proporcionar acceso físico a las instalaciones solo a personal autorizado.	Preventivo	• Ataques Dirigidos • Atacantes Internos.
Aire Acondicionado de Precisión	Equipo con el objetivo de mantener la temperatura adecuada en los centros de	Preventivo	• Ataques Dirigidos • Atacantes Internos.

Control	Objetivo	Tipo de Control	Amenaza Atendida
	datos para el correcto funcionamiento de los equipos de infraestructura.		• Vulnerabilidades en elementos de red e infraestructura critica.
Cableado Estructurado	Sistema de cables, conectores, canalizadores y dispositivos que permiten establecer una infraestructura de telecomunicaciones en una instalación física.	Preventivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Cámaras de Vigilancia	Monitoreo de puntos de acceso físico y mantener grabación se recomienda como mínimo 90 días en línea y 360 días fuera de línea con base a la norma PCI DSS (Payment Card Industry Data Security Standard).	Preventivo Detección Reactivo	• Ataques Dirigidos • Atacantes Internos.
Detectores de Humo	Alarma que detecta la presencia de humo en el aire y emite una señal acústica avisando el peligro de incendio.	Detección	• Vulnerabilidades en elementos de red e infraestructura critica.
Extintores	Equipo que sirve para apagar fuego el cual contiene un agente extintor de incendios a presión.	Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Gafete de Empleado	Credenciales empresariales utilizadas para identificar a las personas de una empresa.	Preventivo Detección	• Ataques Dirigidos • Atacantes Internos.
Gafete de Proveedor y Visitante	Credenciales empresariales utilizadas para identificar a las personas externas de una empresa.	Preventivo Detección	• Ataques Dirigidos • Atacantes Internos.
Generadores eléctricos	Es un equipo cuya utilización está indicada para aplicaciones que requieran mayor potencia y funcionamiento continuo capaces de convertir combustible en energía eléctrica.	Preventivo Contención Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Luces de Emergencia	Son dispositivos de iluminación respaldados por una batería que tienen por objeto asegurar, en caso de fallo en la alimentación eléctrica el alumbrado normal	Preventivo Contención	• Vulnerabilidades en elementos de red e infraestructura critica.
Personal de Seguridad	Llevar acabo funciones de vigilancia y protección de la infraestructura y los bienes de una empresa, así como la protección de las personas que puedan encontrase en los mismos.	Preventivo Contención Detección Reactivo Correctivo	• Ataques Dirigidos • Atacantes Internos.
Salidas de Emergencia	Es una estructura de salida especial utilizadas durante una emergencia, tales como incendios, temblores etc. Permite una rápida evacuación, así como una ruta alterna cuando la entrada/salida principal se encuentra indisponible.	Preventivo	• Ataques Dirigidos • Atacantes Internos.
Sensores de Humedad	Es un aparato de lectura utilizado en espacios interiores para controlar la humedad del aire y la temperatura.	Preventivo Detección Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Sensores de Temperatura	Es un aparato de lectura utilizado en espacios interiores para controlar la temperatura.	Preventivo Detección Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Sistema Contra Incendio	Permite detectar esta clase de siniestros en sus primeras fases, evitando que se vuelvan un problema mayor.	Preventivo Contención Detección Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.
Tarjetas de Acceso	Tarjeta que se utiliza para el acceso seguro a las instalaciones de infraestructura.	Preventivo Contención Detección	• Ataques Dirigidos • Atacantes Internos.

Control	Objetivo	Tipo de Control	Amenaza Atendida
Ubicación de Instalaciones Físicas fuera de zonas vulnerables	Se hace referencia a todas aquellas que se encuentran expuestas a eventos, que puedan afectar los diversos usos del lugar.	Preventivo	• Vulnerabilidades en elementos de red e infraestructura critica.
UPS	Son sistemas de alimentación interrumpida que utiliza baterías para proveer energía eléctrica a la infraestructura durante la interrupción del suministro eléctrico.	Preventivo Detección Reactivo	• Vulnerabilidades en elementos de red e infraestructura critica.

Tabla N° 5 Lista de controles fisicos.

25. Retos para la preservación e impartición de justicia.

Mientras algunos planes estratégicos pueden fracasar por motivos obvios tales como una planificación deficiente, una ejecución fallida, eventos imprevistos y falta de conducta corporativa, otras causas que previenen la correcta impartición de justicia pueden llegar a no ser del todo comprendidas. Algunas de las causas que pueden representar un reto para la preservación e impartición de justicia son:

1) El exceso de confianza:

Las personas responsables de implementación y gestión de controles para asegurar la impartición de justicia muestran una tendencia a tener un exceso de confianza en su capacidad para hacer cálculos exactos con base a el tiempo que llevan desempeñando un puesto o función. Las personas tienden a confiar demasiado en sus capacidades VS el seguimiento sistemático de planes y/o procedimientos específicos. (FBI, 2020)

2) Optimismo:

La gente tiende a ser optimista en sus pronósticos, es decir una combinación de exceso de confianza y optimismo excesivo puede derivar en un impacto desastroso en las estrategias de seguridad de información y en las estrategias para la impartición de la justicia. (Mejor con Salud, 2019)

3) Sedentarismo:

Los seres humanos podemos llegar a realizar tareas de forma rutinaria una vez se domina una actividad o proceso, el sedentarismo afecta la impartición de justicia al momento en que el responsable pierde el interés para llevar a cabo sus funciones causando retrasos en tiempos de respuesta establecidos o llevando la gestión de atención de servicio e incidentes de una forma incompleta que avanzado el proceso derive en retrabajo. (medlineplus, 2020)

4) Tendencia a la confirmación:

Buscar opiniones o hechos que respalden las propias creencias, aceptar solo hechos que respaldan la posición o perspectiva de un grupo o individuo. Así mismo, la fácil aceptación de evidencia que sustenta la hipótesis de un caso, a menudo las personas responsables de impartir la justicia se ven atacados con motivos hostiles o se pone en tela de juicio su competencia resultando en que la presión para llegar a un acuerdo que no sea no del todo apegado a las leyes. (explorable, 2010)

5) Marcos Jurídicos indefinidos:

La infraestructura de telecomunicaciones puede existir en una jurisdicción específica, pero la información, productos o servicios que la soportan pueden estar ubicados en cualquier parte del mundo, haciendo que las responsabilidades de mantenimiento, soporte y operación sean compartidas entre una o múltiples entidades con diferentes marcos jurídicos aplicables.

Como mencionamos en secciones anteriores existes muchos países y naciones los cuales aún no cuentan con leyes de privacidad, ciberseguridad y telecomunicaciones el cual puede afectar negativamente el proceso de investigación y la aplicación de justicia. (OECD, 2000)

6) Complejidad de la infraestructura:

La interconexión de los sistemas e infraestructura en el sector de telecomunicaciones es tan compleja que su administración, gestión y monitoreo se vuelve un reto. (NIST, 2018)

7) Inadecuada Gestión de Incidentes: (BSI, 2020)

En caso de investigación de incidentes de seguridad la falta de capacitación al personal responsable de la gestión de incidentes puede llegar a afectar el debido proceso de recolección de evidencia y afectar el proceso de cadena de custodia, llegando a si a afectar negativamente el proceso legal al desecharse pruebas validas por un incorrecto manejo debido a errores humanos.

8) Riesgos Globales: (World Economic Forum, 2019)

La preservación de justicia está ligada a factores internos y externos. La gestión de riesgo es un tema complejo con muchas variables conocidas y desconocidas y, a menudo, es difícil de determinar con precisión. Con base al Informe de Riesgos Globales del Foro económico Mundial algunos riesgos que pueden afectar la impartición de justicia son:

I. Inestabilidad geopolítica.
II. Preocupaciones económicas.
III. Deficiencias en la respuesta climática.
IV. Impactos de la pérdida de biodiversidad.
V. Déficit de gobernanza tecnológica.
VI. Sistemas de salud tambaleantes.

A su vez los principales riesgos que se espera aumenten en el 2020 son:

I. Confrontación económica / Fricciones entre poderes principales.
II. Polarización de políticas locales.
III. Ondas de calor extremas.
IV. Destrucción de ecosistemas naturales.
V. Ataques cibernéticos: disrupción de operaciones e infraestructura.
VI. Proteccionismo en relación con el comercio y la inversión.
VII. Agendas locales y populistas.
VIII. Ataques cibernéticos: robo de datos o dinero.
IX. Recesión en una economía grande.
X. Incendios incontrolados.

La vigilancia será critica para que los responsables de la preservación de justicia sean capaces de llevar acabo sus funciones.

26. Conclusiones sobre las medidas para la mitigación de amenazas.

La seguridad de información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la infraestructura e información de telecomunicaciones. Estos objetivos son dependientes del hardware, software e infraestructura específica a cada organización. Las situaciones de seguridad de información aparecen en las actividades cotidianas del día a día, aun cuando a veces resulta complicado el diferenciar entre un simple error humano y un incidente de seguridad. Los cibercriminales aprovechan esto para lograr que un ataque informático parezca un simple error humano o incidente aleatorio.

Los controles o contramedidas pueden ser aplicados a la información, programas, sistemas, dispositivos fisicos, redes e infraestructura. Una correcta identificación de amenazas y controles a lineada a la gestión de riesgos puede ayudar a los operadores de telecomunicaciones a que un control tanto físico, administrativo o tecnológico resuelva múltiples amenazas y/o problemas para mejorar la rentabilidad y la inversión que las empresas deben asignar para lograr la protección de la privacidad e información. Las recomendaciones aquí expuestas representan un esfuerzo para que los operadores de telecomunicaciones cumplan con el objetivo de garantizar que se mantiene la confidencialidad, integridad y disponibilidad de la información. La implementación de estos controles aquí expuestos permite minimizar el impacto de que una amenaza motivada por el cibercrimen, ciber espionaje la ciberguerra y Hacktivismo se haga presente permitiendo mantener la Seguridad Nacional así como la privacidad de la información de los suscriptores.

27. Conclusiones del estudio en materia de ciberseguridad y privacidad de información.

La efectividad de implementación de una estrategia de seguridad de información que esté alineada a prácticas internacionales de gestión de seguridad de información por parte de los operadores de telecomunicaciones fijas, la cual tenga como objetivo proteger la infraestructura que brinda servicio a los suscriptores de contenido, dependerá del grado en que sea parte de la cultura de una organización y la medida en que la gestión del riesgo sea responsabilidad de todos los involucrados.

No existe un único mejor enfoque para la seguridad de información, sin embargo, la adopción de buenas prácticas y el deseo de proteger lo que es valioso para las organizaciones puede llevar a la identificación y generación de casos de negocio que habiliten mejoras en las prácticas de privacidad y seguridad actuales en materia de seguridad de información.

La seguridad de información continuará siendo un área que este en constante evolución e innovación dependiendo del avance tecnológico. Es responsabilidad de los operadores de telecomunicaciones, gobierno y público en general en mantener un constante monitoreo en los

riesgos y eventos a nivel mundial los cuales puedan contribuir a la mejora de las estrategias de seguridad y privacidad de la información. Así mismo el panorama de amenazas seguirá variando a la par que evoluciona el crimen cibernético y se promulgan nuevas leyes y regulaciones.

Finalmente es esencial que se continúe con el trabajo colaborativo entre el sector público y privado para el estudio continuo en materia de privacidad y ciberseguridad de información.

28. Conceptos Clave

Acceso Privilegiado: El principio de permitir a los usuarios o aplicaciones la cantidad necesaria de permisos necesarios para realizar sus funciones esperadas.

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.

Almacenamiento: La locación que contiene las copias de respaldo que se van a utilizar en caso de que sea necesaria la recuperación o restablecimiento cuando ocurre un desastre.

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).

Análisis de riesgo: Los pasos iniciales de la gestión de riesgo. Análisis del valor de los activos de la empresa, identificación de las amenazas a esos activos y evaluación de la vulnerabilidad de cada activo a esas amenazas. A menudo involucra la evaluación de la probable frecuencia de un evento en particular, además del impacto probable de ese evento.

Análisis de vulnerabilidades: Proceso de identificación de vulnerabilidades.

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.

Autenticación: El acto de verificar la identidad de una entidad (por ejemplo, un usuario, un sistema o un nodo de red).

Autorización: Privilegio de acceso de un usuario, programa o proceso o el acto de otorgar dichos privilegios.

BIA (Análisis / valoración de impacto al negocio): Evaluar la criticidad y la sensibilidad de los activos de información. Es un ejercicio que determina el impacto que tendría en una organización perder el soporte de algún recurso; establece el incremento de dicha pérdida al paso del tiempo; identifica

los recursos mínimos que se requieren para recuperar y prioriza la recuperación de procesos y sistemas de soporte.

Causa raíz: Proceso de diagnóstico para establecer los orígenes de eventos, que pueden ser utilizados para el aprendizaje de las consecuencias, por lo general de errores y problemas.

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.

Control de acceso: Los procesos, normas y mecanismos de implementación que controlan el acceso a los sistemas de información, a los recursos y al acceso físico a las instalaciones.

Criticidad: Una medida del impacto que puede tener en una organización la falla de un sistema para funcionar según lo requerido.

Datos del titular de la tarjeta: Se denomina "Datos del titular de la tarjeta" a la siguiente información generada a partir de transacciones realizadas por clientes y que podrá ser almacenada, a los siguientes elementos: El nombre del titular de la tarjeta, número de cuenta principal (PAN), fecha de vencimiento, código de servicio.

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.

Disponibilidad: La información que se puede acceder cuando lo requiera el proceso de negocio ahora y en el futuro.

Dueño: Persona u organización que tiene la responsabilidad del desarrollo, obtención, integración, modificación, funcionamiento y mantenimiento y/o disposición final de un sistema de información.

Encriptación: El proceso de tomar un mensaje no cifrado (texto plano), aplicarle una función matemática (algoritmo de cifrado con una clave) y producir un mensaje encriptado (texto codificado).

Estándar: Un requisito obligatorio, un código de práctica o una especificación aprobada por una organización normalizadora externa reconocida, como ISO.

Firewall: Un sistema o una combinación de sistemas que impone una barrera entre dos o más redes que por lo regular forman una barrera entre un ambiente seguro y uno abierto, como la Internet.

Fuga de datos: Extracción o fuga de información mediante el vaciado de archivos de computadora o el robo de informes y grabaciones de computadora.

Hardware: computadoras y dispositivos de telecomunicaciones, medios magnéticos, servidores, dispositivos de almacenamiento, etc.

Impacto al negocio: 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.

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.

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

Métricas de seguridad: Un estándar de medición utilizado en la gestión de actividades relacionadas con la seguridad.

Múltiple factor de Autenticación: El uso de dos mecanismos independientes para autenticación (por ejemplo, solicitar una tarjeta inteligente y una contraseña); en general, la combinación de algo que se conoce es o se tiene.

Plan de continuidad del negocio (BCP): Plan utilizado por una organización para responder ante la interrupción de los procesos críticos de negocio. Depende del plan de contingencia para la restauración de sistemas críticos.

Plan de recuperación de desastre (DRP): Una serie de recursos humanos, físicos, técnicos y de procedimientos orientados a recuperar, dentro de tiempos y costos definidos, una actividad interrumpida por una emergencia o desastre.

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

Privacidad: Libertad contra intrusión o divulgación no autorizada de información sobre personas.

Privilegios mínimos: El principio de permitir a los usuarios o aplicaciones la mínima cantidad de permisos necesarios para realizar sus funciones esperadas.

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.

Pruebas de penetración: Una prueba en vivo de la eficacia de las defensas de la seguridad mediante la imitación de acciones que llevan a cabo atacantes en la vida real.

Red Privada Virtual (VPN): Una red privada segura que utiliza la infraestructura pública de telecomunicaciones para transmitir datos.

Responsabilidad: La capacidad de hacer corresponder una determinada actividad o incidente con la parte responsable.

Respuesta a incidentes: Respuesta de las organizaciones a un desastre u otro evento significativo que pueda afectar considerablemente a la empresa, su gente o su capacidad para funcionar de manera productiva.

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).

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

Software 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.

Software no autorizado: Aplicaciones o programas categorizados como inapropiados y que su instalación no está permitida en la organización.

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.

Fuente: (BSI, 2020)

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

Bibliografía

United States of America in Congress. (2002 , Diciembre 17). *PUBLIC LAW 107-347*. Retrieved from https://certification.comptia.org/es/por-qu%C3%A9-certificarse/gobierno/comptia-y-la-ley-federal-de-seguridad-de-la-informaci%C3%B3n-(fisma) United States of America in Congress a

¿QUÉ ES EL PHISHING? (n.d.). Retrieved from https://www.infospyware.com/articulos/que-es-el-phishing/

Abel, R. (2018, Noviembre 30). *SC Media*. Retrieved from Sky Brasil exposes data of 32M customers on ElasticSearch: https://www.scmagazine.com/home/security-news/sky-brasil-one-of-the-biggest-subscription-television-services-in-brazil-is-the-latest-elasticsearch-server-user-to-leave-its-customers-exposed-after-not-securing-the-server-with-a-password/

Ara, C. (2017). La sistemática general de los delitos cibernéticos y los delitos cibernéticos propios en el Derecho penal alemán: La necesidad de una regulación diferenciada. *Revista de Derecho Penal y Criminología (7)*, 32-64.

BBC NEWS. (2017, Octubre 31). Retrieved from Malaysian data breach sees 46 million phone numbers leaked: https://www.bbc.com/news/technology-41816953

BSI. (2016). *Information security incident managemen.* Retrieved from ISO/IEC 27035:2016: https://www.iso27001security.com/html/27035.html

BSI. (2020). *Continuidad del Negocio ISO 22301.* Retrieved from https://www.bsigroup.com/es-MX/continuidad-del-negocio-ISO-22301/

BSI. (2020). *Gestión de Seguridad de la Información ISO/IEC 27001*. Retrieved from https://www.bsigroup.com/es-MX/seguridad-dela-informacion-ISOIEC-27001/

BT. (2019, Diciembre). *DDoS attacks*. Retrieved from https://www.btplc.com/Digitalimpactandsustainability/Humanrights/Privacyandfreeexpression/cyberindex/ddos/index.htm

CIS. (2020). *Center for Internet Security Controls*. Retrieved from https://www.cisecurity.org/controls/

CMMI Institute. (2020). *What is CMMI*. Retrieved from https://cmmiinstitute.com/cmmi/intro

Crane, C. (2019, Mayo 19). *DDOS Attacks*. Retrieved from The largest DDos Attack in History: https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

CSO Online. (2020, Abril 7). *What is phishing? How this cyber attack works and how to prevent it.* Retrieved from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Deloitte. (2018). *Ley de Protección de Datos de*. Retrieved from Enfoque práctico de adecuación: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/ley_n29733_la_experiencia_implementacion.pdf

DLA Piper. (2020, Enero 14). *Data Protecciont Laws of the World*. Retrieved from https://www.dlapiperdataprotection.com/

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. (2002, Marzo 07). *Diario Oficial de las Comunidades Europeas.* Retrieved from https://www.boe.es/doue/2002/108/L00007-00020.pdf

explorable. (2010, Septiembre 4). *Sesgo de confirmación*. Retrieved from https://explorable.com/es/sesgo-de-confirmacion

F5 Labs. (2019, Agosto 22). *What Are Security Controls?* Retrieved from https://www.f5.com/labs/articles/education/what-are-security-controls

FBI. (2019). *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*.

FBI. (2020). *White-Collar Crime* . Retrieved from https://www.fbi.gov/investigate/white-collar-crime

HACKMAGEDDON . (2019, Diciembre 18). *Cyber Attacks Statistics*. Retrieved from https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

HACKMAGEDDON. (2018, Diciembre 28). *2018 Cyber Attacks Statistics*. Retrieved from https://www.hackmageddon.com/category/security/cyber-attacks-statistics/page/2/

INAI. (2015, Junio). *Guia para implementar un Sistema de Gestión de seguridad de Datos Personales.* Retrieved from http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

INAI. (2016, Junio). *Coordinación de Protección de Datos Personales*. Retrieved from Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales

en Posesión de los Particulares: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Infosecurity Group. (2018, Enero 24). *nfosecurity-mogazine*. Retrieved from bell canada suffers customer data: https://www.infosecurity-magazine.com/news/bell-canada-suffers-customer-data/

Intersoft Consulting . (2018, Mayo). *General Data Protection Regulation GDPR*. Retrieved from https://gdpr-info.eu/

ISACA. (2018). *Manual de Preparación CISM* (15 ed.). IL, USA: ISACA.

ISACA. (2020). *COBIT*. Retrieved from Effective IT Governance at Your Fingertips: https://www.isaca.org/resources/cobit

ISF. (2020). *Information Security Forum*. Retrieved from https://www.securityforum.org/

ISO27001 ES. (2005). *Glosario.* Retrieved from http://www.iso27000.es/glosario.html

krebsonsecurity. (2018, Diciembre 29). *krebsonsecurity*. Retrieved from Cloud Hosting Provider DataResolution.net Battling Christmas Eve Ransomware Attack: https://krebsonsecurity.com/2019/01/cloud-hosting-provider-dataresolution-net-battling-christmas-eve-ransomware-attack/

Mathews, L. (2018, Agosto 24). *Forbes*. Retrieved from Hackers Swipe Data On 2 Million T-Mobile Subscribers: https://www.forbes.com/sites/leemathews/2018/08/24/t-mobile-hackers-swipe-data-on-2-million-subscribers/#3cbef5577a52

Mathews, L. (2019, Julio 17). *Forbes*. Retrieved from Sprint Customer Data Exposed After A Samsung Website Gets Hacked: https://www.forbes.com/sites/leemathews/2019/07/17/sprint-customer-data-exposed-after-a-samsung-website-gets-hacked/#21c485f16ab5

MECIP. (n.d.). *Portal del MECIP*. Retrieved from 6.1.1.3. Controles: http://www.mecip.gov.py/mecip/?q=node/176

medlineplus. (2020). *Riesgos de una vida sedentaria*. Retrieved from https://medlineplus.gov/spanish/healthrisksofaninactivelifestyle.html

Mejor con Salud. (2019, Marzo 2). *5 ideas falsas sobre el optimismo*. Retrieved from https://mejorconsalud.com/5-ideas-falsas-optimismo/

Netscout. (2019, Marzo). *Global Survey Results*. Retrieved from https://www.netscout.com/report/

NIST. (2018, Abril 16). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

OECD. (2000). *CHALLENGES FOR REGULATORY COMPLIANCE*. Retrieved from https://www.oecd.org/gov/regulatory-policy/1910833.pdf

OWASP. (2019, Diciembre). *OWASP Top Ten.*

Passeri, P. (2019, Diciembre 18). *HACKMAGEDDON* . Retrieved from https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Rochina, P. (2016, Mayo 18). *revistadigital*. Retrieved from https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

Sain, Gustavo. (2016, Noviembre 20). ¿Qué es la ciberguerra? *Revista Pensamiento Penal*, 1. Retrieved from http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42952.pdf

SANS. (2020). *Security Awareness*. Retrieved from https://www.sans.org/security-awareness-training/products/end-user

SEGOB. (2001, Enero 24). *REGLAMENTO DE TELECOMUNICACIONES* . Retrieved from http://www.ift.org.mx/sites/default/files/contenidogeneral/concesiones-permisos-y-autorizaciones/78reglamentodetelecomunicaciones01.pdf

SEGOB. (2010, Julio 05). *Diaria Oficial de la Federación.* Retrieved from Leyes y Reglamentos Federales: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

SEGOB. (2011, Mayo 25). *Diario Oficial de la Federación.* Retrieved from http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf

SEGOB. (2013, Octubre 30). *Diaria Oficiol de la Federación*. Retrieved from INSTITUTO FEDERAL DE ACCESO A LA INFORMACION Y: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

SEGOB. (2015, Febrero 12). *Diario Oficial de la Federación.* Retrieved from https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015

SEGOB. (2017, Enero 27). *Diario Oficial de la Federación.* Retrieved from Leyes y Reglamentos Federales: http://www.ordenjuridico.gob.mx/leyes.php

SEGOB. (2018, Diciembre 01). *MAAGTICSI.* Retrieved from https://www.gob.mx/cni/documentos/manual-administrativo-de-aplicacion-general-en-materia-de-tecnologias-de-la-informacion

SEGOB. (2019, Noviembre 08). *Diario Oficial de la Federación.* Retrieved from http://www.ordenjuridico.gob.mx/leyes.php

SEGOB. (2020, Enero 24). *Diario Oficiol de la Federación.* Retrieved from http://www.ordenjuridico.gob.mx/leyes.php

SEGOB. (2020, Enero 24). *Diario Oficial de la Federación.* Retrieved from http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf

SOPHOS. (2018, Noviembre 15). *INFORME DE AMENAZAS 2019.*

State of California. (2020, Abril 19). *California Legislative Information*. Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

The Telecommunication Development Sector. (2020). *National Telecommunication Agencies.* Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/links/nta.aspx

UNAM. (2011, Mayo 04). *INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA.* Retrieved from https://revista.seguridad.unam.mx/category/revistas/numero-10

United Nations. (2020, Febrero 18). *Cybercrime Legislation Worldwide.* Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

Universidad Pompeu Fabra. (2016, Marzo 15). *Ciberespionaje: una nueva forma de otaque y de defensa cibernética*. Retrieved from https://www.upf.edu/web/antenas/el-neologismo-del-mes/-/asset_publisher/GhGirAynV0fp/content/ciberespionaje-una-nueva-forma-de-ataque-y-de-defensa-cibernetica#.XqBRpmhKhPY

World Economic Forum. (2019). *The Global Risks Report 2019.* Retrieved from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf