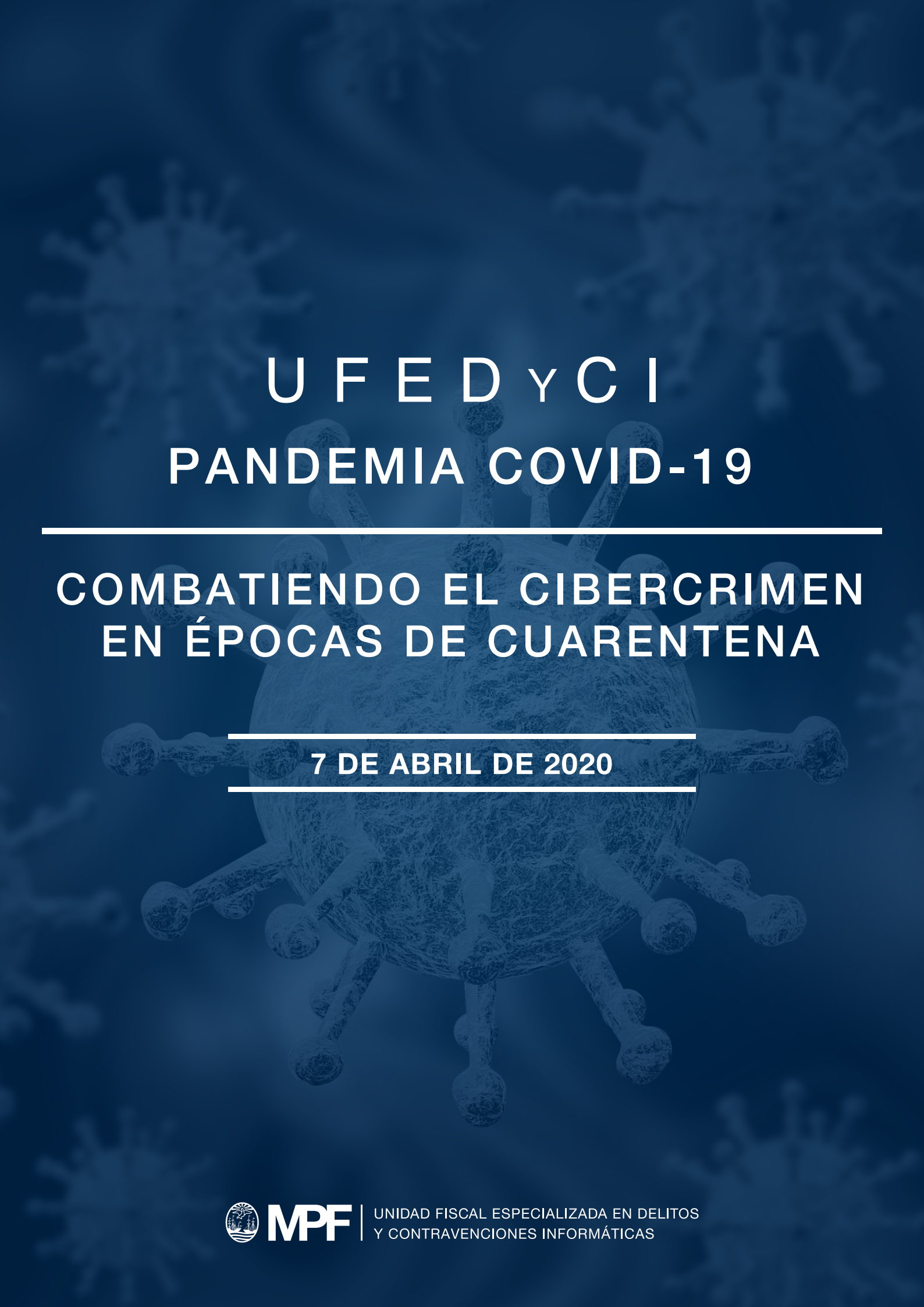

UFEDyCI

PANDEMIA COVID-19

COMBATIENDO EL CIBERCRIMEN EN ÉPOCAS DE CUARENTENA

7 DE ABRIL DE 2020

MPF | UNIDAD FISCAL ESPECIALIZADA EN DELITOS Y CONTRAVENCIONES INFORMÁTICAS

INTRODUCCIÓN

La Pandemia COVID-19 no sólo representa un desafío para los gobiernos y sistemas de salud mundiales, sino también para la prestación del servicio de justicia.

La Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas - UFEDyCI -, creada recientemente a través de la Resolución 20/2020 por el Fiscal General de la Ciudad Autónoma de Buenos Aires, Dr. Juan Bautista Mahiques, a cargo de la Fiscal Daniela Dupuy; ha adoptado diferentes medidas para enfrentar la crisis y continuar en su lucha contra el Cibercrimen.

DR. JUAN BAUTISTA MAHIQUES
FISCAL GENERAL - MPF CABA

DANIELA DUPUY
FISCAL UFEDyCI

PROLIFERACIÓN DE DELITOS INFORMÁTICOS DURANTE LA PANDEMIA COVID-19

EXPLOTACIÓN SEXUAL INFANTIL A TRAVÉS DE LA WEB

A lo largo de la última década, internet ha facilitado la producción, distribución y facilitación de material de explotación sexual infantil en línea. Las razones que han contribuido a este fenómeno son numerosas: la abundancia y facilidad para descargar y compartir archivos a cero costo; el anonimato que provee la red; la posibilidad de acceder a los niños con mayor facilidad; la creación de comunidades en donde los depredadores sexuales comparten no sólo material sino también información; son algunas de las tantas ventajas que proveen los ambientes digitales. Este fenómeno ha llevado a la comunidad internacional a realizar grandes esfuerzos para combatir la nueva modalidad delictiva, como así también cada país ha adoptado en sus legislaciones internas diferentes previsiones que intentan frenar el flagelo que afecta a tantos niños, niñas y adolescentes a nivel mundial.

LEGISLACIÓN NACIONAL

Es así que la Argentina ha efectuado dos modificaciones a su Legislación Nacional. La primera de ellas, a través de la Ley 26.388 del año 2008 y otra más reciente por Ley 27.436 del año 2018, modificando el actual art. 128 del Código Penal de la Nación que ha quedado redactado del siguiente modo.

> *"Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a un (1) año, el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años".*

En consecuencia, Argentina se ha comprometido a atacar todo el ciclo de explotación sexual infantil, abarcando la producción del material prohibido hasta su eventual distribución, comercialización e inclusive la mera tenencia.

GROOMING

El Grooming tiene como exclusivas víctimas a los niños, niñas y adolescentes. No se trata de un nuevo delito sino de una forma evolucionada de cometer un delito preexistente. Es una técnica mediante la cual los pedófilos contactan a sus potenciales víctimas y consiste en el acoso o seducción a un niño, niña o adolescente, por parte de una persona mayor, para obtener algún tipo de gratificación sexual o imágenes sexuales del niño, o bien, como antesala de un posible encuentro personal con la víctima.

LEGISLACIÓN NACIONAL:

El 13 de noviembre de 2013, el Senado de la Nación Argentina aprobó la Ley de Grooming, en la cual la UFEDyCI tiene competencia, quedando la norma del actual art. 131 del Código Penal Argentino redactada de la siguiente forma:

> *"Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".*

RESPUESTA DEL MINISTERIO PÚBLICO FISCAL DE LA CABA ANTE ESTE FENÓMENO

El 11 de octubre de 2013, se suscribió un acuerdo para el Acceso Remoto al CyberTipline entre el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) y el Ministerio Publico Fiscal de la CABA, mediante Resolución de Fiscalía General 435/2013, de fecha 12 de noviembre del mismo año.

El NCMEC es una organización sin fines de lucro con sede en los Estados Unidos. Esta institución, ha recibido el apoyo del Congreso de los EE.UU. con el fin de construir una respuesta internacional coordinada e intercambiar información respecto a la problemática de los niños desaparecidos y explotados sexualmente.

Asimismo, el NCMEC ha obtenido autorización para establecer la CyberTipline, que proporciona un mecanismo centralizado donde los proveedores deservicios de Internet reportan actividades sospechosas relacionadas a la explotación sexual de los niños. A partir de la celebración del Convenio, la UFEDyCI tiene acceso a todos los reportes de actividades sospechosas en los que se detecten usuarios de Internet en nuestro país.

La UFEDyCI, también recibe denuncias de ONG´s y de cualquier ciudadano que tome conocimiento de hechos de producción o distribución de material de explotación sexual infantil, a través de la página web del Ministerio Público Fiscal; línea 0800 FISCAL que recibe denuncias 24 horas, los 7 días de la semana; on-line a través de la página del MPF como así también aquéllos reportes iniciados a través de las denuncias puestas en conocimiento de diversas fuerzas policiales (Policía de la Ciudad, Policía Federal, Gendarmeria Nacional, entre otros).

Sin perjuicio de los reportes del NCMEC y de las denuncias detalladas anteriormente, la UFEDyCI también interviene en operaciones y reportes remitidos por Fuerzas de Aplicación de la Ley con sede en el extranjero, como las sedes de Interpol en diferentes países, Homeland Security –entre otras-, coordinando de esta forma investigaciones a nivel global, para atacar con eficacia las comunidades de pedófilos en la web.

La UFEDyCI ha creado protocolos de actuación para los casos que involucran material de explotación sexual infantil, a través de una actuación coordinada con fuerzas policiales, el Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal y los requerimientos al sector privado –lo que resulta fundamental ya que éste cuenta con los datos informáticos necesarios para identificar a los autores de estas conductas aberrantes.

PANORAMA ACTUAL EN ÉPOCA DE COVID-19

Gran cantidad de los casos que la Unidad se encuentra abocada a investigar, tratan sobre explotación sexual infantil, los que se ven incrementados con la cuarentena absoluta decretada por orden Presidencial.

En este sentido, la modalidad de acoso a niños en línea; producción, facilitación y distribución de imágenes y videos a través de la web por parte de depredadores sexuales que hoy en día se encuentran en sus casas con acceso a internet en forma constante, ha originado un aumento de los reportes que llegan a la UFEDyCI.

Según el informe presentado por Europol[1] el día 3 de abril de este año, sobre la situación actual de la Unión Europea en relación a delitos informáticos durante la Panademia de COVID-19, resulta probable que los delincuentes intenten aprovechar la vulnerabilidad de niños aislados a raíz de la cuarentena, a través del acicalamiento y coerción sexual y extorsión. Ello, debido a que a raíz de la pandemia, se permite a los niños un mayor acceso a Internet sin adecuada supervisión, lo que los hace cada vez más vulnerables a la exposición a delincuentes a través de actividades en línea como juegos, el uso de grupos de chats, aplicaciones, intentos de phishing por correo electrónico, contacto en las redes sociales u otros medios. Indica el reporte que los adultos, que hoy en día trabajan de forma remota, no pueden supervisar las actividades en Internet de los niños o interactuar activamente con ellos fuera de línea para efectivamente vigilar los signos de estrés, aislamiento y soledad que traen aparejados estas conductas cometidas en el ciberespacio. Asimismo, advierte que los niños podrían estar más expuestos, debido a la utilización de aplicaciones en línea no tan seguras sobre educación; la atención no deseada de adultos o identificación de su información personal a través de diferentes maniobras en la web. Por otra parte, los niños pueden estar más inclinados a la autoproducción de material de carácter sexual para el intercambio con sus pares o para enviar a otros, incluidos adultos, dependiendo de varios factores.

[1]Europol, “Catching the Virus. Cybercrime, desinformation and the COVID-19 pandemic”. 3 april 2020.

ESTRATEGIAS ACTUALES IMPLEMENTADAS POR LA UFEDYCI EN EL MARCO DE LA CUARENTENA DECRETADA

LA FISCALÍA GENERAL, A TRAVÉS DE REDES SOCIALES FOMENTA LA REALIZACIÓN DE DENUNCIAS DE MODO ONLINE PARA LA INTERVENCIÓN INMEDIATA DE LA UFEDYCI, A TRAVÉS DEL CORREO ELECTRÓNICO DEL MINISTERIO PÚBLICO FISCAL - DENUNCIAS@FISCALIAS.GOB.AR - TAMBIÉN POR LA WEB DEL MPF, COMO ASÍ TAMBIÉN DENUNCIAS TELEFÓNICAS A TRAVÉS DEL SERVICIO BRINDADO 24/7 A LA COMUNIDAD CON LA LÍNEA 080033FISCAL.

ASIMISMO, LAS FUERZAS POLICIALES DE LA CIUDAD Y DE LA POLICÍA FEDERAL, CONTINÚAN RECIBIENDO DENUNCIAS DE DELITOS INFORMÁTICOS, ESTABLECIENDO COMUNICACIÓN INMEDIATA CON LA UNIDAD QUE ADOPTA LAS MEDIDAS URGENTES DEL CASO PARA COMENZAR CON LA INVESTIGACIÓN

TAMBIÉN, EL NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN –NCMEC- CONTINÚA REMITIENDO REPORTES DE EXPLOTACIÓN SEXUAL INFANTIL DETECTADOS EN LA ARGENTINA, LOS QUE SON DIRECTAMENTE RECIBIDOS Y EVALUADOS POR LA UFEDYCI EN FORMA DIGITAL.

LA FISCALÍA GENERAL, HA BRINDADO A LA UFEDYCI UN ACCESO REMOTO AL SISTEMA DE GESTIÓN DE CASOS - DENOMINADO KIWI -, TOMANDO DE ESTA FORMA CONOCIMIENTO INMEDIATO DE LAS DENUNCIAS RECIBIDAS COMO ASÍ TAMBIÉN PERMITIENDO LA GESTIÓN DE LOS CASOS QUE YA SE ENCONTRABAN EN INVESTIGACIÓN PREVIO A LA CUARENTENA.

ASIMISMO, SE GESTIONÓ EL ACCESO REMOTO AL SISTEMA SIP.AR –EN DONDE SE ENCUENTRAN TODOS LOS REPORTES REMITIDOS POR MISSING CHILDREN-.

LA UNIDAD CUENTA CON DIFERENTES GRUPOS DE TRABAJO QUE INTERVIENEN EN LOS CASOS, QUIENES ESTABLECEN –BAJO LA MODALIDAD “HOME OFFICE”- INMEDIATA COMUNICACIÓN CON LAS VÍCTIMAS A FIN DE RECABAR INFORMACIÓN FUNDAMENTAL PARA LA INVESTIGACIÓN Y ADOPTA LAS MEDIDAS URGENTES NECESARIAS PARA LA IDENTIFICACIÓN DE SUS AUTORES.

EN ESTE SENTIDO, Y DEBIDO A QUE RESULTA FUNDAMENTAL EN LA MAYORÍA DE LOS CASOS CONTAR CON INFORMACIÓN QUE POSEEN LAS EMPRESAS PRESTATARIAS DE SERVICIOS DE INTERNET COMO FACEBOOK, GOOGLE, HOTMAIL, INSTAGRAM –ENTRE MUCHAS OTRAS-, LAS CUALES REQUIEREN AUTORIZACIÓN Y/O FIRMA DE UN JUEZ EN LAS SOLICITUDES EFECTUADAS POR LA JUSTICIA, SE HA COORDINADO CON LOS MAGISTRADOS LA REMISIÓN DE LOS PEDIDOS VÍA SISTEMA INFORMÁTICO, Y, UNA VEZ AUTORIZADOS, SE CONFECCIONAN LOS REQUERIMIENTOS CON FIRMA DIGITAL DEL FISCAL O DEL JUEZ. DE ESTA FORMA, LAS SOLICITUDES SON ENVIADAS DE MANERA VIRTUAL, A TRAVÉS DE LOS PORTALES PARA FUERZAS DE LA LEY QUE POSEEN LAS DIFERENTES EMPRESAS. ESTO NOS PERMITE ASEGURAR LA EVIDENCIA DIGITAL Y CONTAR CON LOS DATOS INFORMÁTICOS NECESARIOS PARA UNA PRONTA IDENTIFICACIÓN DE LOS AUTORES DE ESTAS MANIOBRAS.

EN CUANTO A LAS INVESTIGACIONES EN CURSO, PREVIO A LA PANDEMIA, EL ACCESO REMOTO AL SISTEMA DE GESTIÓN DE CASOS PERMITE A LA UNIDAD CONTINUAR TRABAJANDO SOBRE LOS MISMOS, JUNTO CON EL CUERPO DE INVESTIGACIONES JUDICIALES DEL MINISTERIO PÚBLICO FISCAL, Y ADOPTAR DECISIONES ESTRATÉGICAS, CON FIRMA DIGITAL DE LA FISCAL COORDINADORA, DANIELA DUPUY.

POR OTRA PARTE, LA UNIDAD CONTINÚA BRINDANDO A TRAVÉS DE LAS REDES SOCIALES DEL MINISTERIO PÚBLICO FISCAL DE LA CABA, INFORMACIÓN PARA PREVENIR CONDUCTAS DE ACOSO DE NIÑOS EN LÍNEA, BRINDANDO LOS PASOS NECESARIOS PARA PRESERVAR LA PRUEBA QUE PERMITE COMENZAR LA INVESTIGACIÓN.

CONSEJOS ÚTILES

- NO PROHIBIR EL USO DE INTERNET A LOS NIÑOS, DEBE REALIZARSE UNA SUPERVISIÓN POR PARTE DE LOS PADRES DE LA UTILIZACIÓN DE LOS SISTEMAS INFORMÁTICOS, PROGRAMAS Y APLICACIONES UTILIZADAS POR LOS NIÑOS Y NIÑAS.
- CONVERSAR CON LOS NIÑOS PARA QUE EVITEN EL CONTACTO O ACERCAMIENTO CON EL CIBER-ACOSADOR.
- CONTROL POR PARTE DE LOS PADRES RESPECTO DE LA SEGURIDAD DE LOS EQUIPOS UTILIZADOS, APLICANDO FILTROS QUE IMPIDAN ACCEDER A CONTENIDOS INADECUADOS.
- ESTAR ALERTA ANTE CUALQUIER CAMBIO REPENTINO E INEXPLICABLE EN EL COMPORTAMIENTO DEL NIÑO.
- TENER ESPECIAL CUIDADO EN EL USO DE LAS REDES SOCIALES, YA QUE LOS CIBER- ACOSADORES FRENCUENTAN ESTE TIPO DE SERVICIOS EN BÚSQUEDA DE POTENCIALES VÍCTIMAS.
- HABLAR CON LOS NIÑOS SOBRE LA INFORMACIÓN PUBLICADA EN LAS REDES, EVITANDO SUMINISTRAR DATOS PERSONALES COMO DOMICILIO, COLEGIO, INFORMACIÓN FAMILIAR, ETC.
- UTILIZAR LA WEBCAM ÚNICAMENTE CON PERSONAS DE MÁXIMA CONFIANZA.
- EN CASO DE SER VÍCTIMA DE “GROOMING” O ADVERTIR LA DISTRIBUCIÓN Y/O FACILITACIÓN DE MATERIAL DE
- EXPLOTACIÓN SEXUAL INFANTIL, DAR INMEDIATA INTERVENCIÓN A LA JUSTICIA A TRAVÉS DE LOS CANALES DE DENUNCIA QUE CONTINÚAN FUNCIONANDO DURANTE ESTA CRISIS SANITARIA.
- PRESERVACIÓN DE LA EVIDENCIA: NO BORRAR CONVERSACIONES, MENSAJES NI IMÁGENES O VIDEOS ENVIADOS/RECIBIDOS/DETECTADOS.
- NO INTERACTUAR CON EL GROOMER Y/O AUTOR DE LA DISTRIBUCIÓN DE MATERIAL DE EXPLOTACIÓN SEXUAL INFANTIL.
- ES INDISPENSABLE EFECTUAR UN CONTACTO INMEDIATO CON LOS PADRES Y EVENTUALMENTE EL/LA NIÑA/O PARA QUE RELATE LA FORMA EN QUE OCURRIERON LOS HECHOS.

ATAQUES A LA INTEGRIDAD Y CONFIDENCIALIDAD DE LOS SISTEMAS INFORMÁTICOS

A lo largo de estos años, se ha advertido otro incesante crecimiento de amenazas en la red: los atentados contra la integridad y confidencialidad de datos y sistemas informáticos. La mayoría de las instituciones gubernamentales como así también ciudadanos en sus dispositivos y sistemas informáticos, han experimentado intentos de ingreso y/o manipulación de sus equipos. Asimismo, estas maniobras se han multiplicado o se han vuelto más sofisticadas. La proliferación de estos ataques puede explicarse a partir de los beneficios que reportan. En primer lugar, la tecnología y la experiencia necesarias para llevar a cabo una maniobra de este tipo implican bajos costos. Las herramientas utilizadas y las instrucciones de uso se encuentran muchas veces disponibles en la red. Por otra parte, se destaca el gran alcance e impacto que puede tener una misma maniobra, al cumplir con una multiplicidad de propósitos y causar diversas consecuencias. Otra variable es la ventaja que reportan en cuanto al anonimato de sus autores, ya que la complejidad de las maniobras efectuadas, junto con las características propias de Internet y de la evidencia digital, muchas veces torna difícil la identificación de los responsables.

LEGISLACIÓN NACIONAL

Argentina también hizo frente a estas amenazas a través de la incorporación de diferentes figuras en el Código Penal de la Nación, a través de la Ley 26.388 y respecto de las cuales la UFEDyCI resulta competente:

Artículo 153 bis del CP: "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

Artículo 183, 2do párrafo del CP: "Será reprimido con prisión de quince (15) días a un (1) año … el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".