Asuntos Cibernéticos

Primera Conferencia Cumbre

Ministerio de Seguridad
Argentina

primero la gente

Autoridades

Presidente de la Nación
Dr. Alberto Ángel Fernandez

Vicepresidenta de la Nación
Dra. Cristina Fernández de Kirchner

Jefe de Gabinete de Ministro
Dr. Juan Luis Manzur

Ministro de Seguridad
Cdor. y Dr. Aníbal Domingo Fernández

Unidad Gabinete de Asesores
Cdor. José Lucas Gaincerain

Secretaría de Seguridad
Lic. Mercedes La Gioiosa

Director Nacional de Ciberdelito
Lic. Pedro Janices

INTRODUCCIÓN

Las dos jornadas de la Primera Conferencia Cumbre sobre Asuntos Cibernéticos que organizamos desde el Ministerio de Seguridad de la Nación han dejado inquietudes, ideas, certezas y, sobre todo, una agenda de trabajo de cumplimiento urgente e imprescindible si queremos ponernos a tono con los tiempos que corren. Y debemos hacerlo.

El cibercrimen "no se va a ningún lado, llegó para quedarse", fue uno de los conceptos más contundentes y, a la vez convocantes, que se escucharon en la primera jornada de la Conferencia. Porque no sólo define la situación con solidez, sino que nos advierte sobre la posibilidad cierta de que se vuelva cada vez más seria y peligrosa.

Hace más de 80 años, el filósofo y ensayista español José Ortega y Gasset nos convocaba con su célebre "Argentinos, a las cosas". No perdamos un minuto más. La responsabilidad es de todos. Pero, sobre todo de aquellos en quienes la ciudadanía ha depositado su confianza.

Tenemos que trabajar conjuntamente con el sector privado, la Justicia y los legisladores para formular normas puntuales que ayuden a proteger a los ciudadanos a la vez que nos permitan atender con eficacia el ciberdelito.

Hay que generar, además, conciencia de los riesgos en los usuarios; instruir a la ciudadanía sobre cómo proceder. Y para lograrlo, tenernos que compartir estrategias de comunicación con todas las instituciones involucradas y, así, producir saberes e información a la que puedan accedan especialistas, investigadores y toda aquella persona interesada en cuestiones de la cibercultura.

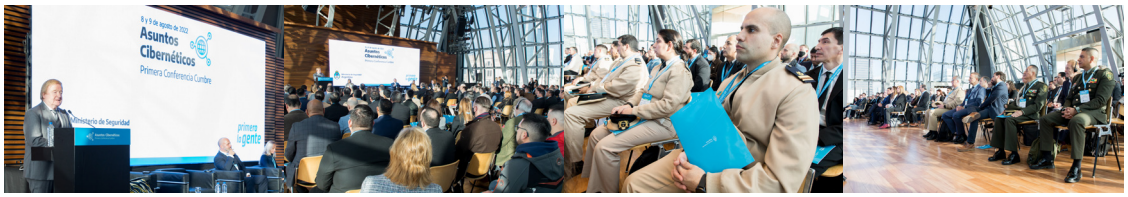
Finalmente, la cooperación internacional es una herramienta indispensable en la lucha contra el cibercrimen. Por eso, en mi rol de presidente del Consejo Latinoamericano de Seguridad Interior (CLASI) he propiciado la adhesión al segundo protocolo de cibercrimen de la Unión Europea y la participación en las Naciones Unidas en apoyo de la nueva convención sobre ciberdelitos a través de nuevas tecnologías de la información y las comunicaciones (TICs).

El delito se vuelve más y más sofisticado y los hombres y las mujeres de a pie, más indefensos frente a tanta tecnología y desarrollo desplegados. Es deber del Estado pero también de las organizaciones privadas más relevantes de la comunidad, asistir y proteger a la ciudadanía. Ahora. Ya. Sin dilación. Y sin descanso.

Aníbal Domingo Fernández
Ministro de Seguridad de la Nación

PRIMERA CONFERENCIA CUMBRE SOBRE ASUNTOS CIBERNETICOS - ARGENTINA

Los días 8 y 9 de agosto se llevó a cabo la PRIMERA CONFERENCIA CUMBRE SOBRE ASUNTOS CIBERNETICOS organizada por el MINISTERIO DE SEGURIDAD DE LA NACIÓN, en la cual se presentaron y desarrollaron temas concernientes a esta temática, tales como: la generación y sinergia en la cooperación público privada a los fines de la detección, investigación y preservación de la evidencia digital, el abordaje a los delitos de altas tecnologías, la situación nacional y provincial de los ciberdelitos, el delito financiero como fraudes, el lavado de activos y la utilización de criptoactivos por parte de la delincuencia, estrategias y herramientas para la protección de datos, cómo prevenir y detectar incidentes, el abordaje a la trata de personas considerando su prevención, detección y acompañamiento a las víctimas y la necesidad de fortalecer la legislación para hacer más efectiva la lucha contra los ciberdelitos.



A nivel internacional, se impulsó la cooperación en prevención e investigación de ciberdelitos, la construcción en capacidades cibernéticas, la elaboración de estrategias y herramientas en investigación de delitos complejos, y la importancia de la ciberdiplomacia en el contexto internacional de los ciberdelitos.

En dicho encuentro participaron 36 expositores internacionales y nacionales, de organizaciones y organismos como el Comité de la Convención sobre Cibercrimen del Consejo de Europa, el Instituto de Estudios de Seguridad de la Unión Europea, el proyecto EU-Cybernet, la Organización de Estados Americanos, INTERPOL, la embajadora para Asuntos Cibernéticos del Ministerio Federal de Relaciones Exteriores de Alemania, el Global Forum on Cyber Expertise, el Operation Underground Railroad, Fundacion Argentina de Prevención de Lavados de Activos, Asociacion de Bancos, Asociación de Fiscales y Funcionarios del Ministerio Publico Fiscal de la Nacion, y del sector privado como Microsoft, Oracle, Eset, Fortinet, Intel, Meta, Whatsapp, Chainalisys, Maltego, Voyager Labs, Grayshift.

Los y las asistentes a la conferencia fueron funcionarios y funcionarias entre quienes se encontraban Ministros y Ministras de diversas provincias, Secretarios y Secretarias, Directores y Directoras, fiscales y agentes de las fuerzas de seguridad de más de 16 provincias, así como del gobierno nacional de diferentes ministerios junto a representantes de más de 6 embajadas extranjeras.

RELATORÍA DE LAS JORNADAS

DIA 1 (08 AGOSTO 2022)

COOPERACIÓN INTERNACIONAL EN PREVENCIÓN E INVESTIGACIÓN DE CIBERDELITO

Conferencistas: Christopher PAINTER (GFCE), Cristina SCHULMAN (COE), Liina ARENG (EU- CYBERNET)

Moderador: Pedro JANICES (Ministerio de Seguridad)

Dicho bloque abordó las iniciativas y acciones que se llevan adelante desde el Global Forum on Cyber Expertise, el Consejo de Europa y la Unión Europea como las prácticas de visibilización y de cooperación internacional que incluyen acciones en varios continentes con el fin de abordar la temática en base al respeto de la privacidad y con el fin de combatir el ciberdelito.

Entre otras consideraciones al estado actual de la cooperación se destacó, transversalmente, las *asimetrías de participación* de algunas naciones en las diferentes convenciones y proyectos, así como la necesidad de mayor cooperación en materia de *evidencia transfronteriza ágil y veloz* y para lo cual el Convenio sobre el Cibercrimen (conocido como el Convenio de Budapest), en su Segundo Protocolo Adicional, puede ser una herramienta que permita afrontar el desafío, al menos, entre las naciones que participan del mismo.

Adicionalmente se expuso que la ciberseguridad y el ciberdelito son "*dos caras de la misma moneda*" dado que la primera hace a la segunda más difícil de tener éxito.

Se destacó que fuera de convenios y convenciones, algunos Estados no colaboran en la prevención e investigación al no cooperar con información y, de esta forma, permitir un accionar facilitador a la ciberdelincuencia.

Se señaló la necesidad de que los Estados puedan realizar ejercicios de ciberseguridad a nivel ministerial y de respuesta a incidentes cibernéticos de forma conjunta entre el sector público y el sector privado como también promover el intercambio internacional de saberes, pero fortaleciendo la cooperación, en términos legales, técnicos e investigativos.

Se destacó la importancia de contar con mecanismos, como acuerdos y convenios de cooperación internacional, para el abordaje de los ciberdelitos, haciendo hincapié en la necesidad de que los Estados fortalezcan sus capacidades internas, así como de realizar ejercicios de ciberseguridad a nivel ministerial y de respuesta a incidentes cibernéticos de forma conjunta entre el sector público y el sector privado.

Por último, se dejó de manifiesto que el cibercrimen "*no se va a ningún lado, llegó para quedarse*" y tiende a perdurar haciéndose cada vez más serio, amenazando los derechos humanos.

Conclusiones

Estado de la cuestión

1.- La cooperación internacional enfrente el desafío de las asimetrías de participación de algunas naciones en las diferentes convenciones y proyectos.
2.- La necesidad de mayor reciprocidad en materia de evidencia transfronteriza ágil y veloz, sigue siendo uno de los objetivos a lograr.
3.- Algunos Estados no colaboran en la prevención e investigación al no cooperar con información y, de esta forma, permitir un accionar facilitador a la ciberdelincuencia.

Propuestas

1.- Se debe fortalecer la cooperación internacional para la prevención e investigación de ciberdelitos, en términos legales, técnicos e investigativos.
2.- Se debe continuar propiciando la adhesión a convenios internacionales vigentes, así como la generación de nuevos espacios que involucren más Estados en materia de cooperación internacional.
3.- Se debe formular la realización, por parte de los Estados, de ejercicios de ciberseguridad a nivel ministerial y de respuesta a incidentes cibernéticos de forma conjunta entre el sector público y el sector privado.

CONSTRUCCION Y FORTALECIMIENTO DE CAPACIDADES CIBERNÉTICAS

Conferencistas: Brennan BAYBECK (ORACLE), Christopher PAINTER (GFCE), Gustavo MAGGI (FORTINET), Alexander SEGER (COE)

Moderadora: Mariana GALAN (Ministerio de Seguridad)

Los conferencistas coincidieron en que los Estados se encuentran afectados por la existencia de un déficit de personal técnico especializado en asuntos cibernéticos que es ocasionado, principalmente, por la falta de incentivos suficientes que posibiliten su retención. Entre los cuales se hizo especial mención a los salarios poco competitivos del sector público, en relación al sector privado, y la falta de planes de capacitación continua en la materia.

Como propuestas para poder subsanar esta situación, se manifestó la importancia de que los Estados trabajen sobre la implementación de mecanismos para facilitar la cooperación público-privada, haciendo foco sobre los ejes de capacitación, ejercicios y talleres multidisciplinarios. Se planteó que las empresas y las universidades pueden ser un socio estratégico del sector público, ya que cuentan con sus propias academias destinadas a la formación y capacitación de recursos humanos que pueden ser aprovechadas por los Estados para fortalecer el conocimiento de sus planteles, así como de lugares donde realizar estos talleres junto al descubrimiento de nuevos recursos con habilidades especiales.

Uno de los conferencistas destacó la importancia de que los funcionarios judiciales, indistintamente del fuero al que pertenezcan, reciban capacitación en materia de evidencia electrónica. En este sentido, manifestaron que parte o todo el material probatorio de un crimen tradicional puede encontrarse dentro de un sistema informático, dando cuenta de las implicancias tecnológicas que necesariamente deben ser atendidas para la prosecución de las investigaciones.

Además, se hizo referencia a que los asuntos cibernéticos no son una cuestión inminentemente técnica, sino que, por su resultado ante un ataque, puede afectar la economía, el desarrollo y los aspectos sociales de los Estados, por lo que es necesario que los mismos cuenten con políticas públicas para la construcción y el fortalecimiento de habilidades multidisciplinarias en el tema, sin las cuales se dificultaría la tarea de determinar con precisión las áreas prioritarias a las que se deban asignar recursos.

Un representante del sector privado expuso que para fortalecer la ciberseguridad y disminuir los indicadores del cibercrimen es necesario contar con plan integral de respuesta a incidentes cibernéticos, que aborde aspectos esenciales como, por ejemplo, la concientización y la capacitación del personal e involucre a todas las áreas de la organización. Sumado a esto se hizo referencia a la necesidad de modificar las responsabilidades reales establecidas en torno a las empresas privadas, entendiendo que la misma no debe ser atribuida únicamente a los jefes de seguridad de la información (CISO), sino a todos los empleados y ejecutivos involucrados para cada caso y siendo del mismo tenor para las organizaciones y organismos.

Conclusiones

Estado de la cuestión

1.- Los Estados se encuentran afectados por la existencia de un déficit de personal técnico especializado en asuntos cibernéticos que es ocasionado, principalmente, por la falta de incentivos suficientes que posibiliten su retención.

2.- Necesidad de que los funcionarios judiciales, indistintamente del fuero al que pertenezcan, reciban capacitación en materia de evidencia electrónica.

3.- Los asuntos cibernéticos deben ser abordados de forma multisectorial.

4.- Ausencia de un plan integral de respuesta a incidentes cibernéticos, que aborde aspectos esenciales.

Propuestas

1.- Los Estados deben trabajar sobre la implementación de mecanismos para facilitar la cooperación público-privada, haciendo foco sobre los ejes de capacitación, ejercicios y talleres multidisciplinarios.

2.- Se deben generar políticas públicas para la construcción y el fortalecimiento de habilidades multidisciplinarias en el tema.

3.- Se deben propiciar los planes de concientización y la capacitación del personal -público/privado-, que involucre a todas las áreas de la organización.

4.- Desde el ámbito privado modificar las responsabilidades reales establecidas en torno a las empresas, entendiendo que la misma no debe ser atribuida únicamente a los jefes de seguridad de la información sino a todos los empleados y ejecutivos involucrados para cada caso y siendo del mismo tenor para las organizaciones y organismos.

PANEL DE ESTRATEGIAS Y HERRAMIENTAS EN DELITOS COMPLEJOS

Conferencistas: Joseph COURTESIS (VOYAGERLABS), Kristopher DOUCETTE (CHAINALYSIS), Nick BURTON (GRAYSHIFT), Carlos FRAGOSO MARISCAL (MALTEGO)

Moderador: Facundo MORALES (Ministerio de Seguridad)

Durante el bloque se hizo referencia a que la motivación de los criminales no ha cambiado, sino el contexto en el cual los delitos se cometen y que, a medida que la tecnología avanza a un ritmo mucho mayor que las investigaciones, los criminales cuentan cada vez con técnicas más complejas para utilizarla y obtener beneficios ilícitos.

Por ello, coincidieron en la necesidad de empoderar a los investigadores, fortaleciéndolos con herramientas proporcionadas por distintas empresas y desarrolladas para la tarea investigativa, así como los protocolos y procedimientos necesarios para incrementar su nivel de madurez en la materia.

Por su parte, uno de los representantes de las empresas del sector privado hizo especial referencia a la necesidad de contar con la mayor cantidad de fuentes y canales de información posible para lograr un abordaje exitoso de cada investigación.

Se destacó que, por la volumetría de la información producida por los incidentes, es necesario contar con herramientas como la inteligencia artificial que ayude a discernir sobre la información realmente importante para la investigación. No obstante, el conferencista señaló la importancia de diferenciar los roles de los analistas y los investigadores, ya que no solamente es necesario extraer información sino también hay que analizarla, por lo que será necesaria la capacitación específica en esos aspectos.

Otra de las empresas destacó la creciente tendencia respecto del uso de los criptoactivos para la obtención de beneficios ilícitos y para el lavado de activos, haciendo especial hincapié en la complejidad, y en algunos casos ausencia, del régimen jurídico aplicable a los mismos, manifestando que podrían ser considerados, por ejemplo, como un bien mueble, como una moneda de curso legal o como un título valor.
Además, los conferencistas coincidieron en que los datos ya no se encuentran cen-

tralizados en un solo lugar, por lo que será necesario un mayor nivel de precisión al momento de realizar los requerimientos de información y establecer los mecanismos necesarios para un intercambio efectivo de la misma.

Los conferencistas recomendaron abordar las investigaciones complejas estableciendo responsabilidades claras para los actores intervinientes y haciendo eje no solamente en un actor malicioso individual, sino en toda la organización criminal de la cual forma parte, permitiendo un mayor impacto en la lucha contra el crimen.

Conclusiones

Estado de la cuestión

1.- Es manifiesta la necesidad de trabajar en el requerimiento de fuentes y canales de información posible para lograr un abordaje exitoso de cada investigación.
2.- La discriminación de los roles de los analistas y los investigadores para la capacitación específica en esos aspectos es insuficiente.
3.- La tendencia respecto del uso de los criptoactivos para la obtención de beneficios ilícitos y para el lavado de activos va en aumento.
4.- Se visibiliza la importancia de contar con herramientas que ayuden al análisis de grandes volúmenes de datos.

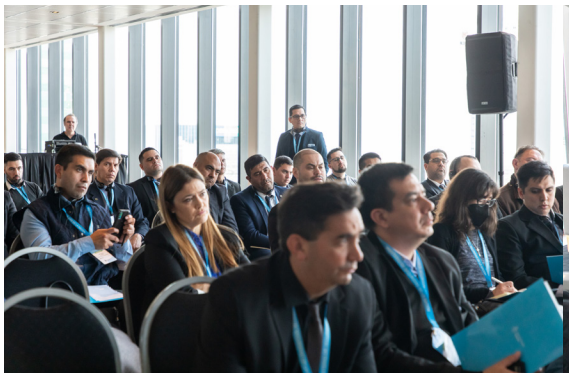
Propuestas

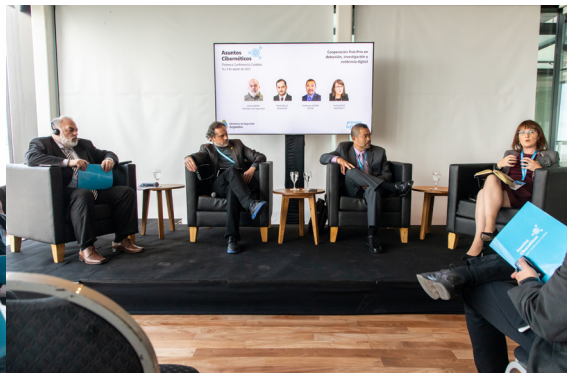
1.- Se debe lograr un mayor empoderamiento de los investigadores, fortaleciéndolos con herramientas proporcionadas por distintas empresas y desarrolladas para la tarea investigativa.
2.- Se deben generar los protocolos y procedimientos necesarios para incrementar el nivel de madurez en la materia.
3.- Se debe aumentar el nivel de precisión al momento de realizar los requerimientos de información y establecer los mecanismos necesarios para un intercambio efectivo de datos.

COOPERACIÓN PUBLICA-PRIVADA EN DETECCION, INVESTIGACIÓN Y EVIDENCIA DIGITAL

Conferencistas: Aisling KELLY (MICROSOFT), Pablo BELLO (WHATSAPP), Guillermo AUYON (TIKTOK)

Moderador: Adrián MORO (Ministerio de Seguridad)





Durante el mismo, los conferencistas acordaron que una de las mayores dificultades al momento de investigar un delito, detectar un incidente o intentar preservar evidencia digital, es la jurisdicción en la cual se encuentran los datos.

Esto lo atribuyeron a sus respectivos modelos de negocio y al carácter transnacional que tienen los asuntos cibernéticos, por lo que destacaron la importancia de crear e implementar mecanismos y políticas de cooperación nacionales e internacionales entre los sectores público y privado, haciendo foco en las solicitudes judiciales de preservación de datos transfronterizos y aquellas de información de usuarios criminales.

En este sentido, destacaron que actualmente algunas plataformas cuentan con canales de contacto -Law Enforcement Requests Channels, LERC-, a través de los cuales, las autoridades que investigan pueden requerir a las empresas la información en forma directa. No obstante, hicieron hincapié en la necesidad de implementar nuevos mecanismos de solicitud de información, más allá de los canales existentes, lo que permitirá mejorar su eficacia y agilizar la cooperación entre los sectores público y privado.

Acuerdos, como la Convención sobre Cibercrimen y su Segundo Protocolo Adicional, proponen canales más directos y ágiles entre los organismos encargados de llevar adelante las investigaciones y el sector privado, evitando pasos intermedios que obstaculizan o demoran las investigaciones, ayuda a obtener mayor cantidad de información directa formal y mantiene el respeto a los derechos humanos.

Por último, una de las empresas hizo mención al falso dilema entre la privacidad y la seguridad, afirmando que no es necesario renunciar a ciertos grados de privacidad para tener seguridad, sino que ambos aspectos pueden y debieran coexistir para evitar que uno reduzca al otro.

Conclusiones

Estado de la cuestión

1.- Persiste la complejidad en términos de la jurisdicción en la cual se encuentran los datos.
2.- Se cuenta con importantes canales de contacto, a través de los cuales, las autoridades que investigan pueden requerir a las empresas la información en forma directa, pero los mismos no son provistos por todas las plataformas y las que hay no son suficientemente ágiles y no cubren todas las necesidades de las fuerzas de ley.
3.- No es necesario renunciar a ciertos grados de privacidad para tener seguridad, sino que ambos aspectos pueden y debieran coexistir para evitar que uno reduzca al otro.

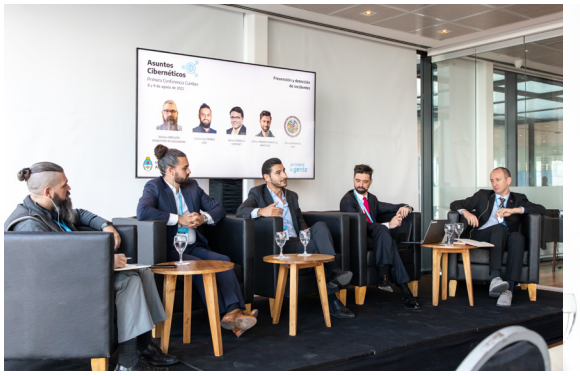
Propuestas

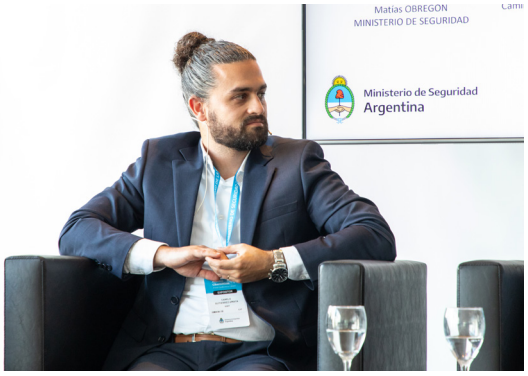
1.- Se deben promover la creación de mecanismos y políticas de cooperación nacionales e internacionales entre los sectores público y privado, haciendo foco en las solicitudes judiciales de preservación de datos transfronterizos y aquellas de información de usuarios criminales.
2.- Se deben implementar y ampliar nuevos mecanismos de solicitud de información, más allá de los canales existentes.

ABORDAJE A LOS DELITOS DE ALTA TECNOLOGÍA

Conferencistas: Camilo GUTIERREZ (ESET), Arturo TORRES (FORTINET), Adrián DE GRAZIA (INTEL)

Moderadora: Daniela LÓPEZ (Ministerio de Seguridad)





Los conferencistas estuvieron de acuerdo en que dentro del panorama actual de los asuntos cibernéticos existen distintas clases de ciberdelincuentes, entre los cuales se pueden encontrar aquellos que pertenecen organizaciones criminales complejas, generalmente asociadas a la finalidad de obtener un rédito económico, político o geopolítico. Uno de los escenarios es el caso de los grupos que utilizan amenazas persistentes avanzadas -Advanced Persistent Threats - APT-, con el objeto y la capacidad de atacar de forma sofisticada, a través de múltiples vectores de actuación y de forma constante en el tiempo, un objetivo estratégico determinado, sea éste una empresa, una infraestructura crítica o dependencias de gubernamentales.

En esta misma línea, una de las empresas mencionó que hay una creciente tendencia en la cantidad y complejidad de los ataques que se realizan, por lo que será necesario incrementar las capacidades de prevención, detección e investigación del ciberdelito, aprovechando la experiencia de trabajo de cada fuerza policial y de seguridad federal.

Por su parte, otra de las empresas destacó la importancia de comprender el verdadero funcionamiento y manejo de las tecnologías de la información y la comunicación (TICs), no solo por los técnicos sino también por los operadores de justicia.

Señaló que esto puede ser realizado a través de ejercicios que repliquen el accionar criminal, pero en ambientes contenidos, para poder optimizar la elaboración de métodos, procesos y protocolos asi como la asignación de los recursos, tanto humanos como materiales, permitiendo lograr la mejora continua del accionar policial en materia de investigación de ciberdelitos y análisis forense digital. Para ello, focalizó en la necesidad de cooperación entre los sectores público y privado, en especial sobre la importancia de brindar formación y capacitación continua a los efectivos de las fuerzas federales policiales y de seguridad asi como a los operadores de justicia.

Los delitos de altas tecnologías no solo apuntan a los organismos del Estado sino tienen un foco creciente y productivo en el sector privado, que en oportunidades son infraestructuras críticas, donde hacen foco por la falta de medidas de seguridad producto de escasa inversión por falta de regulación y auditorias.

Más allá de la información suministrada por la cooperación publico privada, la actuación y colaboración entre las universidades y las fuerzas policiales y de seguridad debe ser activa, sugiriendo que la creación de sus propios laboratorios de análisis de malware podrían ser una gran herramienta a los fines de poder investigar e informar sobre nuevas amenazas, tendencias y sus comportamientos.

Conclusiones

Estado de la cuestión

1.- Se registra la creciente tendencia en la cantidad y complejidad de los ataques que se realizan enfocados a sectores específicos, siendo el ransomware el visibilizador más conocido pero acompañado con otros comportamientos.
2.- Las organizaciones criminales complejas hacen uso del ciberespacio entendiendo las ventajas tecnológicas que les proporciona y los desafíos que presenta a la investigacion su accionar transfronterizo.
3.- Van en aumento los ataques dirigidos a sectores privados aprovechándose de aquellos que no han invertido en la seguridad de sus infraestructuras.

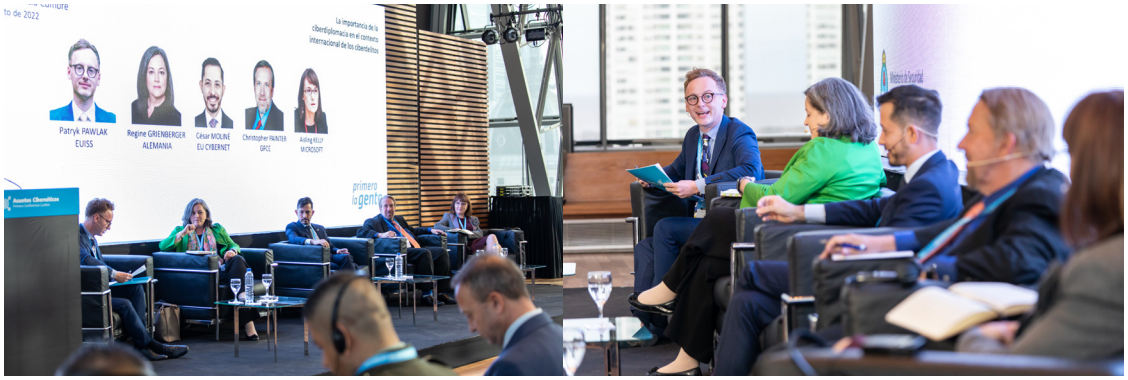
Propuestas

1.- Se deben incrementar las capacidades de prevención, detección e investigación de los ciberdelitos, aprovechando la experiencia de trabajo de cada fuerza policial y de seguridad federal.
2.- Se debe ensayar, mediante ejercicios específicos, el verdadero funcionamiento y manejo de las tecnologías de la información y la comunicación (TICs), replicando escenarios reales ya conocidos y producir documentacion respaldatoria de cómo proceder para lograr la resiliencia y un plan de respuesta.
3.- Se debe crear el mecanismo entre las universidades y de las fuerzas policiales y de seguridad para la creación de sus propios laboratorios de análisis.

IMPORTANCIA DE LA CIBERDIPLOMACIA EN EL CONTEXTO INTERNACIONAL DE LOS CIBERDELITOS

Conferencistas: Christopher PAINTER (GFCE), Regine GRIENBERGER (EMBAJADORA DE ASUNTOS CIBERNETICOS, ALEMANIA), César MOLINÉ (EU-CYBERNET), Aisling KELLY (MICROSOFT)

Moderador: Patryk PAWLAK (European Union - Institute for Security Studies)



Se puso de manifiesto que las nuevas tecnologías de la información y las comunicaciones (TICs) están teniendo una alta importancia en la diplomacia y por ello forman parte de las agendas de los formuladores de políticas internacionales, no solo para la difusión del conocimiento de las culturas, empresas, y productos de un país, sino también para evitar, prevenir y gestionar diplomáticamente los asuntos cibernéticos.

Temas como el desarrollo de nuevas tecnologías y sus implicaciones en la seguridad, la defensa y en los derechos humanos deben ser parte de la agenda diplomática, así como la cooperación y comprensión en lo referente a como las nuevas tecnologías están redefiniendo la relación en materia de ciberdelito y ciberseguridad, sumando el análisis de impacto de la dependencia y la interdependencia internacionales -según el caso del país donde se encuentre-.

Los y las conferencistas estuvieron de acuerdo en que la ciberdiplomacia es un aspecto esencial para que los Estados puedan lograr un abordaje efectivo, integral y resiliente, respecto de los asuntos cibernéticos promoviendo el derecho internacional en el ciberespacio y tratando de evitar la mala interpretación y el escalamiento en los conflictos generando, para esto, la construcción de medidas de confianza.

En este sentido, destacaron que es necesaria la estructuración de una política a nivel nacional que contemple la diplomacia cibernética y mencionaron lo fundamental que es el apoyo y acompañamiento de los Ministerios de Relaciones Exteriores de los países para la consolidación de la misma.

Uno de los conferencistas mencionó que, algunos países, carecen de las capacidades o los recursos suficientes para tener una presencia constante en debates sobre la diplomacia cibernética, lo cual puede generar que no acompañen el crecimiento y la universalidad de la temática y dependan de las definiciones de los países con más recursos.

Por ello, destacó la responsabilidad de los funcionarios políticos de visibilizar esta problemática y las ventajas que acarrea la creación de cursos de formación, con un enfoque específico en la ciberdiplomacia, por parte de las organizaciones y hasta en el ámbito académico por su carácter interdisciplinario.

Además, una conferencista manifestó que es fundamental la participación activa de mujeres y el abordaje a las cuestiones con perspectiva de género, generando y acompañando proyectos que amplíen la creación de capacidades en ciberdiplomacia.

Conclusiones

Estado de la cuestión

1.- La ciberdiplomacia es un aspecto esencial para que los Estados puedan lograr un abordaje efectivo, integral y resiliente, respecto de los asuntos cibernéticos.
2.- El desarrollo de nuevas tecnologías y sus implicaciones en la seguridad, la defensa y en los derechos humanos deben ser parte de la agenda diplomática, así como la cooperación y comprensión en lo referente a como las nuevas tecnologías están redefiniendo la relación en materia de ciberdelito y ciberseguridad, sumando el análisis de impacto de la dependencia y la interdependencia internacionales.
3.- Se manifiesta la falta de capacidades o los recursos suficientes para tener una presencia constante de algunos Estados en debates sobre la diplomacia cibernética.

Propuestas

1.- Se debe propiciar el establecimiento de una política a nivel nacional que contemple la diplomacia cibernética.
2.- Los funcionarios políticos deben comprometerse a visibilizar la problemática y propiciar las ventajas que acarrea la creación de cursos de formación, con un enfoque específico en la ciberdiplomacia.
3.- Se debe fomentar la participación activa de mujeres y el abordaje a las cuestiones con perspectiva de género, generando y acompañando proyectos que amplíen la creación de capacidades en ciberdiplomacia.

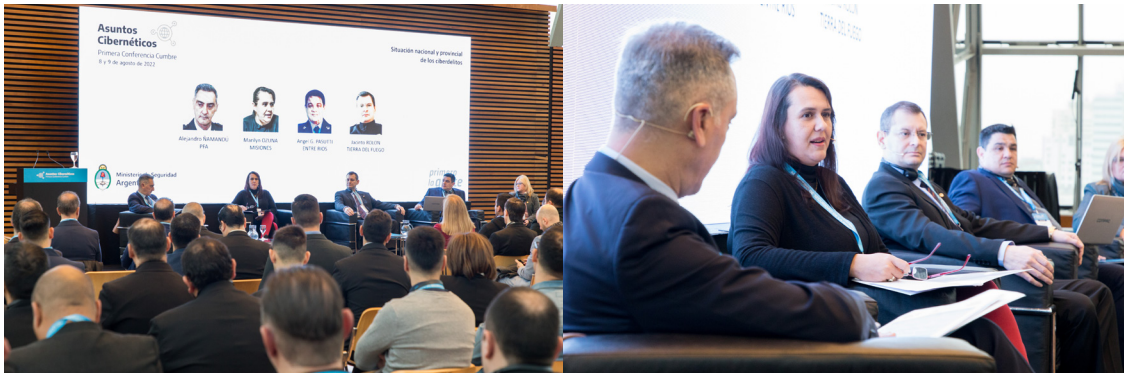
DIA 2 (09 AGOSTO 2022)

SITUACION NACIONAL Y PROVINCIAL DE LOS CIBERDELITOS

Conferencistas: Crio. Ins. Marilyn OZUNA (MISIONES), Crio. Myr. Ángel PASUTTI

(ENTRE RIOS), Crio. Gral. Jacinto ROLON (TIERRA DEL FUEGO), SubCom. Sandra IÑIGUEZ (CORDOBA)

Moderador: Crio. Gral. Alejandro **ÑAMANDU** (Policía Federal Argentina)



Los y las conferencistas abordaron las diferentes realidades que cada provincia presenta a la hora de encarar los ciberdelitos desde una visión y perspectiva federal del mismo. Se destacó la problemática territorial y la falta de acciones que permitan mantener una comunicación fluida y eficaz con el resto de las provincias más alejadas. Siguiendo con esta línea, el aspecto económico geográfico también fue profundizado debido a la baja cantidad de recursos materiales y de oferta especializada y actualizada en la formación de los actores que integran cada etapa del proceso de investigación.

Los y las conferencistas concordaron que estás asimetrías son producto de la expansión digital acelerada, de la administración de los recursos económicos y fundamentalmente de los cambios culturales de cada grupo social que integran las comunidades en cuestión. También coincidieron en fijar lineamientos federales para estandarizar recursos y equipamiento, capacitar e incentivar al personal propio e implementar mecanismos que permitan la articulación y cooperación entre los distintos sectores intervinientes.

Señalaron que es necesario que todas las provincias adopten un abordaje preventivo hacia los ciberdelitos, acercando a las Fuerzas hacia el ciudadano con tareas de sensibilización y concientización a través de charlas con estudiantes de diferentes edades en los establecimientos educativos, como también en diferentes espacios sociales y culturales, además de trabajar de manera continua para fortalecer el enfoque preventivo hacia los mismos. En este sentido, se recalcó la necesidad de informar y capacitar a la ciudadanía en la materia, sobre todo en aquellos en mayor situación de vulnerabili-

dad, tales como adultos mayores, niños/as y adolescentes clarificando y agilizando el cómo y dónde realizar las denuncias en el caso de ser o conocer alguna víctima.

Por su parte, otra de las conferencistas hizo mención a la importancia de contar con mecanismos agiles de cooperación a nivel federal entre los sectores público y privado, destacando la creación de canales exclusivos y la designación de puntos de contacto para solicitudes de información, y señalando la importancia de conversatorios como este que genera mayor relación y conocimiento de todos los actores que velan por la seguridad del ciberespacio en todo el territorio nacional, tanto compañeros de las fuerza, como fiscales, empresas del sector público y organismos internacionales.

Conclusiones

Estado de la cuestión

1.- Las asimetrías entre los recursos de las provincias en materia de ciberseguridad y ciberdelito son producto de la expansión digital acelerada, de la administración de los recursos económicos y fundamentalmente de los cambios culturales de cada grupo social que integran las comunidades en cuestión.
2.- Se evidencia en diferentes provincias una baja cantidad de herramientas tecnologicas, así como de oferta especializada y actualizada en la formación de los actores que integran cada etapa del proceso de investigación, debiendo muchos de ellos a recurrir a clases on-line o presencialmente a otra locación con ofertas académicas generando mayores costes de tiempo y económicos.

Propuestas

1.- Fijar lineamientos federales para estandarizar recursos y equipamiento, capacitar e incentivar al personal propio e implementar mecanismos que permitan la articulación y cooperación entre los distintos sectores intervinientes.
2.- Se debe promover la adopción federal de un abordaje preventivo hacia los ciberdelitos.
3.- Se debe incentivar a realizar campañas de concientización y sensibilización de la temática.
4.- Se debe desarrollar e implementar ofertas de capacitación y formación específica y actualizada de forma regional.

SIGUIENDO EL DINERO: DELITOS FINANCIEROS, FRAUDES, LAVADO Y CRIPTOACTIVOS

Conferencistas: Kristofer DOUCETTE (CHAINALYSIS), Joseph COURTESIS (VOYAGER LABS)

Moderador: Hernán ZAVALÍA LAGOS (ADEBA)

Se propuso un espacio para conversar respecto de la técnica investigativa dirigida al seguimiento del dinero y los criptoactivos. Mediante las experiencias internacionales y nacionales de los conferencistas, se compartió la versatilidad que posee esta estrategia toda vez que existe la posibilidad real y concreta de seguir el dinero y que puede operar como (i) un medio de investigación para poder identificar a la organización criminal que está detrás del mismo; (ii) una forma de reparar y recuperar el daño patrimonial que los distintos delitos generan; y (iii) una manera de comprobar la comisión de un delito autónomo, es decir, el lavado de activos.

Siguiendo estas posibilidades, los conferencistas fueron desgranando distintos ilícitos para demostrar la efectividad que se logra en el plano investigativo con la utilización de esta táctica de seguimiento del dinero, el cual además permite conocer la integración y relación de las distintas personas que forman parte de una organización ilegal, pues las vinculaciones dinerarias que se llevan adelante -pagos, transferencias, depósitos, etc.-, pueden ser utilizadas en los casos policiales y judiciales como un elemento de prueba perfectamente válido. Asimismo, se conversó sobre las diversas herramientas tecnológicas existentes en la actualidad, las que brindan soluciones para el investigador frente a la dificultad que implica el seguimiento de los criptoactivos. Instrumentos tecnológicos que permiten además conocer el contenido y movimiento de los mismos en las distintas billeteras digitales utilizadas, como así también de los distintos operadores del mundo de activos digitales, considerando sus regímenes jurídicos y sus obligaciones.

Por su parte, uno de los conferencistas destacó que en su país la incautación de activos digitales se suele utilizar para la adquisición de herramientas de investigación, fortaleciendo las capacidades de preservación y recolección de evidencia electrónica de los actores intervinientes. Además, hizo hincapié en que para las investigaciones utilizan herramientas que pertenecen a distintas empresas pero que tienen la misma finalidad de asistir a la tarea investigativa. Se pudo observar que, en algunos países, la

carencia de acceso a tecnologías que puedan analizar grandes volúmenes de transacciones, tanto de dinero como de criptoactivos, son uno de los problemas, que se suman a la formación en la operatoria de investigación del lavado como en la capacitación del uso de las diferentes herramientas tecnológicas que posibiliten su análisis y demostración, así como a las herramientas jurídicas que regulen ciertos mercados.

De esta interacción entre los conferencistas y los asistentes, se debatió sobre la importancia del seguimiento del dinero como una técnica que debe iniciarse desde el origen mismo de toda investigación criminal, a los fines de poder vislumbrar las relaciones entre las personas investigadas, la detección del grupo criminal objeto de la pesquisa, el recupero de los bienes y la determinación -en su caso- de un delito autónomo pasible de sanción penal para sus autores.

Durante el transcurso de este panel, los conferencistas estuvieron de acuerdo en que los criptoactivos plantean un gran desafío a la incautación de activos digitales, en virtud de las diversas problemáticas legales de jurisdicción y competencias que acarrean. Por ello, coincidieron en la necesidad de involucrar a todos los actores necesarios para lograr un enfoque integral y colaborativo que permita lograr un régimen de prevención de lavado de activos que sea efectivo.

Conclusiones

Estado de la cuestión

1.- Se evidencia que, en algunos países, la carencia de acceso a tecnologías que puedan posibiliten el análisis y la investigación de estos delitos, así como a las herramientas jurídicas que regulen ciertos mercados financieros.
2.- Si bien existen herramientas tecnológicas que ayuden a analizar grandes volúmenes de datos estas no son incorporadas por todos los Estados, en algunos casos por sus altos costos y en otros por no tener regulaciones sobre ese sector que los obligue o les posibilite hacerlo.

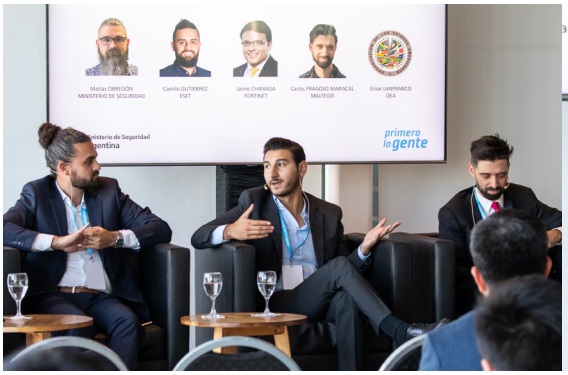
Propuestas

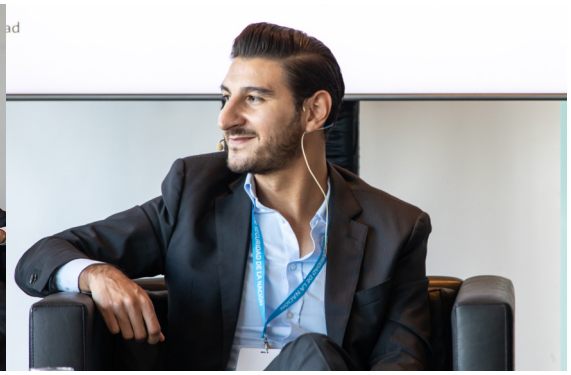
1.- Se debe vincular a todos los actores necesarios para lograr un enfoque integral y colaborativo que permita alcanzar un régimen de prevención de lavado de activos que sea efectivo.
2.- Se debe regular sobre ciertos mercados como el de criptoactivos de forma más profunda, así como invertir en tecnologías de grandes volúmenes de datos y en la formación y capacitación de investigadores que puedan sacarles provecho a estas herramientas.

PREVENCIÓN Y DETECCIÓN DE INCIDENTES

Conferencistas: Camilo GUTIERREZ (ESET), Arturo TORRES (FORTINET), Carlos FRAGOSO MARISCAL (MALTEGO), Einar LANFRANCO (OEA)

Moderador: Matías OBREGON (Ministerio de Seguridad)





Los conferencistas concordaron en que los servicios esenciales de los Estados y el normal funcionamiento de sus infraestructuras de información, así como el bienestar y la seguridad de sus ciudadanos dependen, en gran medida, de la cooperación en la esfera de asuntos cibernéticos a nivel federal e internacional y de la adopción de medidas preventivas para poder abordar de manera efectiva los nuevos riesgos e incidentes que acaecen día a día afectando al orden público, impactando en áreas críticas de la información, exponiendo y vulnerando a la sociedad en general, así como también al sector público y privado. Además, destacaron que todos los actores que componen el ecosistema del ciberespacio, entre los que se encuentra el sector público, el sector privado, las entidades académicas y la sociedad civil deben encontrar y generar mecanismos de actualización, cooperación y respuesta conjunta y coordinados para proteger sus infraestructuras, sistemas y servicios.

Por otro lado, uno de los conferencistas afirmó que, para lograr una articulación conjunta, centralizada y eficaz, es necesaria la conformación de equipos de respuestas ante incidentes en los distintos ámbitos de interés, con la responsabilidad de coordinar y respaldar la detección de vulnerabilidades, colaborar con la respuesta ante incidentes, así como proponer medidas a fin de brindar una respuesta eficaz ante nuevos riesgos y posibles incidentes.

Además, se hizo hincapié en que para potenciar el accionar de los equipos de respuesta a incidentes, será de vital importancia que cada una de las Fuerzas Policiales y de Seguridad Federales cuente con su propio centro de operaciones de seguridad -SOC, por sus siglas en inglés-, el cual debe necesariamente ser capacitado y dotado de recursos de manera continua para llevar adelante sus actividades diarias de control y prevención. Se destacó la información de zero-days y los informes tempranos de vulnerabilidades y

de amenazas que los diferentes actores de organizaciones y empresas producen, dado que son importantes para prevenir y responder proactivamente a los posibles incidentes, tomando medidas de prevención, destacando la alta importancia que tiene el relacionamiento -networking-, y la comunicación entre todos los actores. Además, se problematizó la falta de mecanismos agiles que permitan la solicitud de información o preservación de contenido a los proveedores de servicios que se encuentran alojados de manera distribuida, generalmente, en jurisdicciones extranjeras. Junto a las carencias, vuelve a surgir el desarrollo de nuevos recursos humanos con ejercitación práctica en la administración de gestión de incidentes, así como en la forensia de los mismos.

Por último, otro de los conferencistas hizo mención a la importancia de formar parte de los distintos grupos internacionales de intercambio de información establecidos, tales como CSIRT-AMERICAS entre otros.

Conclusiones

Estado de la cuestión

1.- De la cooperación en la esfera de asuntos cibernéticos a nivel federal e internacional dependen los servicios esenciales de los Estados y el normal funcionamiento de sus infraestructuras de información, así como el bienestar y la seguridad de sus ciudadanos.
2.- Reviste cada vez más importancia la información de zero-days y los informes tempranos de vulnerabilidades y de amenazas que los diferentes actores de organizaciones y empresas producen, dado que son sustanciales para prevenir y responder proactivamente a los posibles.
3.- Se experimenta la carencia de recursos humanos con ejercitación práctica en la administración de gestión de incidentes, así como en la forensia de los mismos.

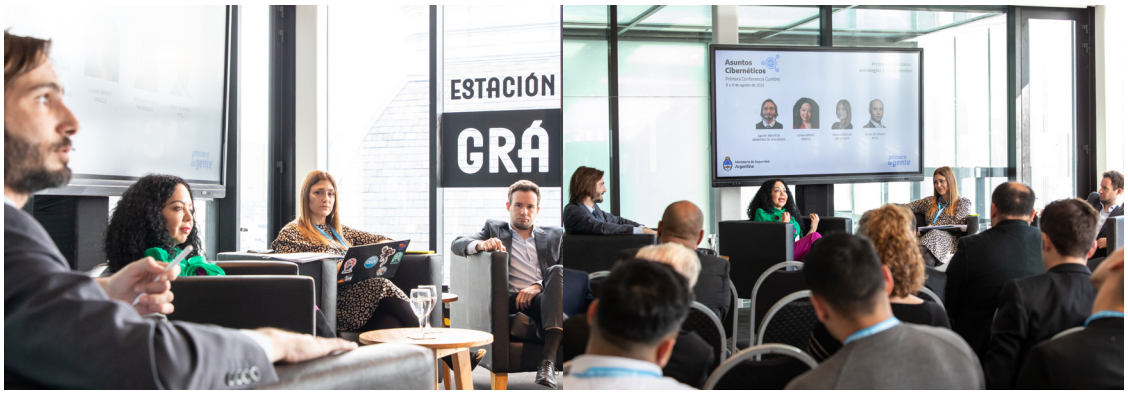
Propuestas

1.- Se debe fomentar la articulación conjunta para la conformación de equipos de respuestas ante incidentes en los distintos ámbitos de interés, con la responsabilidad de coordinar y respaldar la detección de vulnerabilidades, colaborar con la respuesta ante incidentes, así como proponer medidas a fin de brindar una respuesta eficaz ante nuevos riesgos y posibles incidentes.
2.- Se debe propender a la creación de centros de operaciones de seguridad para cada uno de los operadores de justicia y fuerzas intervinientes.
3.- Se debe propiciar el compromiso en la participación de los distintos grupos internacionales de intercambio de información establecidos, tales como CSIRT-AMERICAS entre otros.

PROTECCIÓN DE DATOS: ESTRATEGIAS Y HERRAMIENTAS

Conferencistas: Lorena BRAVO (ORACLE), Marina BERICUA (MICROSOFT), Adrián DE GRAZIA (INTEL)

Moderador: Agustin MALPEDE (Ministerio de Seguridad)



Durante el mismo se trataron las diferentes iniciativas y acciones que se llevan adelante desde las empresas del sector privado a través de sus programas a nivel interno, los cuales incluyen acciones para proteger la integridad, la disponibilidad y la confidencialidad de los datos que almacenan, recopilan y procesan en sus operaciones diarias.

Se destacó de manera transversal, la necesidad de adoptar un enfoque preventivo hacia los incidentes y contar con una política de seguridad de la información que permita conocer los roles, las responsabilidades y las medidas que el personal debe adoptar para la protección de la información, la cual representa un activo para las organizaciones. En este sentido, una de las panelistas mencionó que algunos de los aspectos más importantes para lograr un abordaje eficaz a la problemática son: el control de acceso de los usuarios a los sistemas informáticos, el inventario de los activos y la información de la organización, así como la clasificación de los mismos, según el grado de criticidad que tengan.

Por otro lado, una de las conferencistas señalo que la protección de los datos es una tarea continua, que requiere un proceso de revisión periódica y actualización constante para poder minimizar los riesgos de ocurrencia de incidentes en torno a los mismos. Para ello, mencionó la importancia de llevar adelante auditorias, tanto a nivel interno como externo. Además, destacó que, dentro de su organización, adoptaron una estrategia de confianza cero, partiendo de la base de que este tipo de incidentes siempre van a ocurrir.

Otro de los conferencistas afirmó la importancia de dimensionar los incidentes para asignar los recursos necesarios para lograr la resiliencia de las plataformas. En este sentido, hizo hincapié en la posibilidad de solicitar asistencia a las autoridades correspondientes del sector público y la necesidad de contar con mecanismos efectivos de comunicación de incidentes, tanto a nivel interno como hacia las autoridades externas que intervengan en razón de sus funciones y competencias.

Por último, se señaló que el establecimiento de normas que ayuden a proteger los datos sin una real ejercitación y control, solo pasa a ser un cumplimiento temporal que terminará por impactar en las plataformas de información, por lo que se sugiere que se realicen ejercicios de prueba de phishing, evaluando su asertividad y complementándolos con cursos para aquellos que hayan resultado vulnerables, así como otros ejercicios que ayuden al usuario, cualquiera sea su rol o nivel, a tomar mayor precaución sobre el activo de la organización.

Conclusiones

Estado de la cuestión

1.- La protección de los datos es una tarea continua, que requiere un proceso de revisión periódica y actualización constante para poder minimizar los riesgos de ocurrencia de incidentes en torno a los mismos.
2.- Si bien en muchos casos existen normas de protección de datos aún falta trabajar más en el acompañamiento a través de ejercicios y talleres que involucren los diferentes estamentos de las organizaciones.

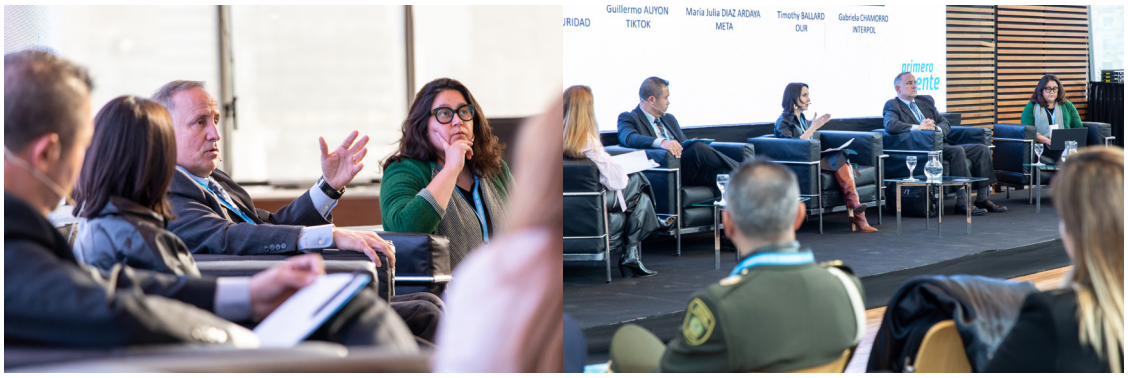
Propuestas

1.- Se deben desarrollar y adoptar estrategias con un enfoque transversal y preventivo hacia los incidentes, tanto en la prevención como en su resiliencia.
2.- Se debe impulsar una política de seguridad de la información que permita conocer los roles, las responsabilidades y las medidas que el personal debe adoptar para la protección de la información, la cual representa un activo para las organizaciones.
3.- Se deben fomentar la realización de talleres prácticos multidisciplinarios, con los diferentes actores involucrados en el proceso de la protección de los datos de la organización.

TRATA DE PERSONAS: PREVENCION, DETECCION Y ACOMPAÑAMIENTO A LAS VICTIMAS

Conferencistas: Guillermo AUYON (TIK TOK), María Julia DIAZ ARDAYA (Meta), Carlos MAZA (OUR), Gabriela CHAMORRO (INTERPOL)

Moderadora: Edith LEIVA (Ministerio de Seguridad)



Los y las conferencistas coincidieron en la necesidad de profundizar los recursos de sensibilización, las herramientas de protección, el abordaje integral, el trabajo colaborativo, la cooperación internacional y la importancia de compartir la información, debido a la utilización del ciberespacio tanto para la captación como para la organización y promoción de este tipo de delitos.

Consideraron que la prevención, la investigación y la asistencia a las víctimas deben realizarse desde una política pública interseccional y desde los ámbitos públicos, privados, académicos y las organizaciones de la sociedad civil. Resaltaron como desafíos que la capacitación de las autoridades y de la ciudadanía en general sobre los riesgos en las plataformas debe ser continuo y llegar a todos los estratos sociales por todos los medios disponibles con campañas oficiales. Asimismo, invitaron a seguir invirtiendo en tecnología que cuide y proteja a las y los usuarios, remarcando que desde lo operacional las investigaciones muchas veces tienen un gran volumen de material para analizar y se requiere de herramientas que permitan acelerar ese proceso.

Uno de los conferencistas destacó que su empresa proporciona los controles parentales para garantizar las premisas de garantía de derechos de menores y destaca que no hay mensajes directos a las y los niños y que estos solo pueden acceder a contenidos que circulan en dicha red social, solo si se ha dado el ok voluntario de un o una adulta. Asimismo, destaca que los contenidos subidos, cumplen con controles de “recursos pre-aprobados”.

Otro compartió que en relación a los cuidados de derechos de niñas, niños y adolescentes y sus vínculos con esa red social, expone que existe un enfoque integrado, com-

puesto por políticas internas y de carácter nacional e internacional que determina que "se puede" y que no. También señalo que cuentan con desarrollo tecnológico, así como con personas capacitadas y equipos humanos que se forman para la detección y prevención de los delitos cibernéticos.

Entre los aspectos transversales señalo algunos como la educación y sensibilización, el fortalecimiento y articulación multiagencia en clave de Cooperación Internacional -actores articulados como organizaciones de la sociedad civil, fundaciones, estado, poder judicial-, la afectación real y trabajo con expertos, la detección y problematización de los diferentes delitos tecnológicos en su país, el conocimiento de documentos de carácter internacional en la materia específica como se los de la ONU, el Protocolo de Palermo, las nuevas dificultades de la esclavitud –migrantes-, y el cuidado de las víctimas a partir del trabajo articulado con las fuerzas de ley. También amplió la información sobre el ICSE que ya cuenta con 67 países miembros se destacó la necesidad imperiosa de establecer redes de trabajo conjunto en clave de Cooperación Internacional.

Por último, los conferencistas coincidieron en la necesidad de integrar los distintos ambientes que se dedican a la problemática, a fin de generar los mecanismos de cooperación necesarios para el intercambio de información, detección proactiva y apoyo a las víctimas.

Conclusiones

Estado de la cuestión

1.- Este tipo de delitos siguen vigentes y con alta presencia en el ciberespacio, y lejos de disminuir, van en aumento.
2.- Persiste la necesidad de educación y sensibilización, el fortalecimiento y articulación multiagencia con actores articulados como organizaciones de la sociedad civil, fundaciones, estado, poder judicial, y el cuidado de las víctimas a partir del trabajo articulado con las fuerzas de ley.

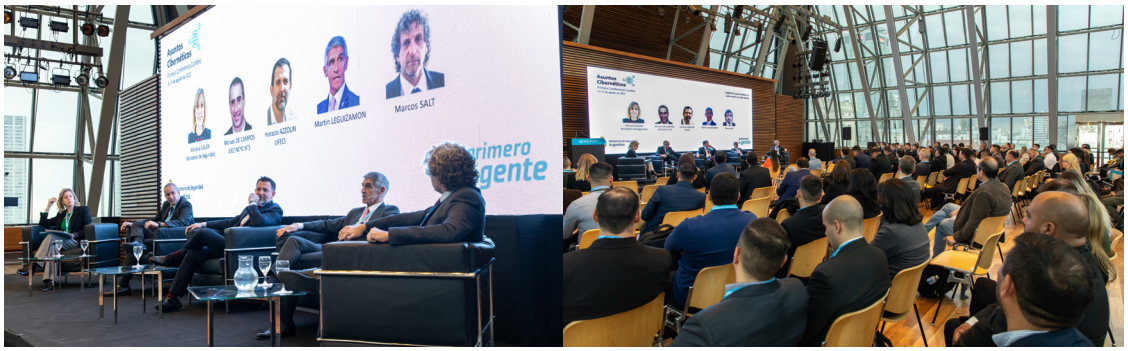
Propuestas

1.- Se deben generar más campañas nacionales que contemplen recursos de sensibilización, las herramientas de protección, el abordaje integral, el trabajo colaborativo, la cooperación internacional y la importancia de compartir la información.
2.- Se debe profundizar la capacitación de las autoridades y de la ciudadanía en general sobre los riesgos en las plataformas, debiendo ser continuo y llegar a todos los estratos sociales por todos los medios disponibles con campañas oficiales.

LEGISLACIÓN PARA FORTALECER LA LUCHA CONTRA LOS CIBERDELITOS

Conferencistas: Manuel DE CAMPOS, (JUEZ NACIONAL EN LO CRIMINAL Y CORRECCIONAL), Horacio AZZOLIN (UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA), Martin LEGUIZAMON (ESTUDIO LEGUIZAMON), Marcos SALT (PROFESOR U.B.A.)

Moderadora: Mariana GALAN (Ministerio de Seguridad)



Los conferencistas plantearon que existen figuras que podrían ser modificadas como el fraude informático que habría que incorporar al Código Penal como las imágenes intimas no consentidas, la suplantación de identidad y la violencia de genero digital.

Asimismo, destacaron la prioridad de readecuar y actualizar el Derecho Penal Procesal, incorporando el concepto de infraestructuras críticas como un agravante y la problemática que se genera entorno a los criptoactivos.

Todos los conferencistas coincidieron en que es necesario aumentar las herramientas de investigación en el ámbito digital donde varias legislaciones procesales provinciales están avanzando. Sin embargo, algunos expositores enfatizaron que con las herramientas existentes se puede igualmente avanzar en las investigaciones penales, discrepando en el alcance de los medios de prueba o evidencia digital que el Código Procesal Penal enuncia.

Destacaron, que el cibercrimen es un asunto global y no solo local y remarcaron la importancia de poder contar con equipos conjuntos de investigación para ciertos delitos, ya que nos enfrentamos a delitos que tienen presentes acciones en varias jurisdicciones, siendo la dificultad principal la jurisdicción aplicable para avanzar en las investigaciones. Se volvió a señalar la situación actual en obtención de evidencia digital transfronteriza, viendo en ello nula o poco exitosa la cooperación por parte de las empresas en algunos casos.

Se manifestó la necesidad de mejorar esas colaboraciones a través de la implementación de los mecanismos internacionales vigentes, y la profundización de la cooperación publico privada, teniendo en cuenta la diferenciación entre el lugar físico donde se almacenan y quien ejerce el control o administración efectiva de los datos.

En total acuerdo, se manifestó la importancia de ratificar e incorporar los instrumentos vinculantes ya existentes a nivel internacional, tales como el Segundo Protocolo Adicional de la Convención sobre Cibercrimen, que podría mejorar la cooperación público privada tornándola más ágil y directa, y el Convenio de delitos a través de las tecnologías de la información y de las comunicaciones (TICs) de las Naciones Unidas que está siendo elaborado por los países en este momento. En este orden de ideas, también se destacó la importancia de contar con potestades sancionatorias suficientes para aquellos casos donde se configure un incumplimiento, especialmente en relación a las cuestiones que involucran a los datos personales.

Por último, se apreciaron los diferentes puntos de vista que pueden tener las medidas más innovadoras para investigar el cibercrimen, algunas debatidas desde hace años y que fueron incorporadas en diferentes legislaciones alrededor del mundo, así como en algunas provincias de nuestro país pero que, por la insuficiente capacitación o entendimiento técnico, jurídico y operativo, tienen poca o nula aplicación real.

Todos coincidieron en la necesidad de ampliar las herramientas jurídicas para dar una lucha efectiva, por cuestiones de inmediatez, complejidades tecnológicas y volumetría de información, contra las organizaciones criminales complejas en el ciberespacio, para lo cual es indispensable la participación del Poder Legislativo elaborando esos marcos de acción.

Conclusiones

Estado de la cuestión

1.- Se evidencia la existencia de figuras que podrían ser modificadas como el fraude informático que habría que incorporar al Código Penal como las imágenes íntimas no consentidas, la suplantación de identidad y la violencia de genero digital.
2.- El cibercrimen es un asunto global y no solo local, por lo que debe observarse de una manera transnacional.
3.- La obtención de evidencia digital transfronteriza es nulo o poco exitosa, en virtud de la falta de cooperación por parte de algunas empresas.

Propuestas

1.- Se debe propiciar la ampliación y actualización de herramientas jurídicas.
2.- Se debe incorporación del concepto de infraestructuras críticas al Código Procesal Penal y debe transparentarse la problemática que se genera entorno a los criptoactivos.
3.- Se debe contar con potestades sancionatorias suficientes para aquellos casos donde se configure un incumplimiento, especialmente en relación a las cuestiones que involucran a los datos personales.

REFLEXIONES FINALES

Con el transcurrir de los años y con el agravante de la Pandemia del Covid-19, las temáticas del ciberespacio y de los asuntos cibernéticos han adquirido una relevancia sustancial para los técnicos, especialistas, investigadores y todos aquellos que se encuentran relacionados en este campo debido al impacto que el mismo produce sobre nuestras sociedades.

Este crecimiento no pareciera verse reflejado, en los distintos países, en el mismo orden de importancia por quienes tienen roles de gestión política institucional debido, entre otros factores, al nivel de desarrollo en la materia, al desconocimiento en cuestiones que atañen a los flujos geoeconómicos, al valor estratégico de las estructuras de las tecnologías de la información y las comunicaciones de las empresas que manejan esas infraestructuras esenciales y de los lugares donde estas residen, tanto por su marco jurídico como por sus compromisos internacionales. Asumiendo estas asimetrías, desde el Ministerio de Seguridad de la Nación Argentina se ha desarrollado la PRIMERA CONFERENCIA CUMBRE SOBRE ASUNTOS CIBERNETICOS.

Durante las dos jornadas especialistas nacionales e internacionales expusieron las problemáticas que atañen a este universo proponiendo planes trasversales, con participación multidisciplinaria, que faciliten una mayor descripción, análisis y propuesta de acciones de gestión para garantizar un ciberespacio seguro, abierto y resiliente que fortalezcan las políticas de estado.

Los ejes transversales que atravesaron las exposiciones y demandas fueron:

- La jerarquización de la cooperación internacional en materia de prevención e investigación del cibercrimen.
- La necesidad de una comunicación ágil y eficiente para la obtención de evidencia digital transfronteriza.
- La promoción de campañas de sensibilización de la sociedad que apunte a visualizar los riesgos del ciberespacio y la generación de una “cibercultura”.
- El fortalecimiento de las capacidades técnicas y humanas, en ciberseguridad y en investigación del cibercrimen.
- La cooperación público-privada tanto en la prevención como en la investigación.

- La formación y especialización de recursos humanos.
- Un mayor abordaje en los temas de criptoactivos puesto que dentro de nuestro país como a nivel internacional existen dificultades respecto del régimen jurídico aplicable a los mismos.
- La readecuación de las normas jurídicas existentes para contemplar los casos específicos que plantean los asuntos cibernéticos.

La Cumbre permitió que la circulación de la palabra de los expositores y los participantes, en el marco de un conversatorio presencial, expusieran problemáticas globales y específicas que, con el desarrollo de los encuentros, viabilizó las vinculaciones y redes de contacto volviendo a recuperar la cadena de confianza que solo se logra cuando se comparten valores y objetivos.

Es entonces que la concreción de estos conversatorios, entre los hacedores de políticas y los diferentes sectores involucrados en los asuntos cibernéticos, se vuelven críticos y necesarios tanto para el desarrollo y sustentabilidad del ciberespacio como para la seguridad nacional de todo país que propenda a trabajar en conjunto con todas las naciones para el bien común de sus sociedades.

APROXIMACIÓN A LOS ASUNTOS CIBERNÉTICOS

A los efectos del presente documento, se establece a lo “cibernético” como el modo de describir y analizar la organización interna y externa del ciberespacio, en su faceta de construcción y evolución reparando en las funciones regulatorias, de circulación y retroalimentación, de la información. Es así que uno de “los asuntos” de lo cibernético refiere a su aspecto técnico y social que engloba a la ciberseguridad y el ciberdelito.

Desde esta perspectiva definimos a “los asuntos cibernéticos” como las acciones o situaciones que tienen lugar en el ciberespacio que pueden afectar o contribuir a la seguridad nacional de un país de forma directa o indirecta.

En este campo se encuentran los temas relacionados a la prevención, detección y respuesta a acciones criminales, el fortalecimiento de las infraestructuras digitales y de las políticas de protección relacionadas al ciberespacio, las iniciativas que favorecen una mayor cultura de concienciación sobre ciberseguridad, los marcos regulatorios, las posibilidades de mejoras en eficiencia devenidas de la cooperación internacional, y todas aquellas que coadyuven al objetivo de lograr un ciberespacio abierto, seguro y confiable.

Con la mayor oportunidad de intercambio de información sin fronteras y en tiempo real, estos asuntos cibernéticos se han transformado en un requisito de análisis interdisciplinario y transnacional por las asimetrías económicas entre naciones, por las escasas medidas de seguridad tecnológica de algunos sectores, por la necesidad de una mayor y mejor oferta educacional en la materia, por la necesidad de regulación actualizada asi como por los efectos inmediatos que su vulneración o uso criminal del ciberespacio produce contra la ciudadania y la sociedad toda.

Atender los asuntos cibernéticos es, entonces, entender y comprender la problemática del ciberespacio en su complejidad para la construcción de políticas públicas, en vistas de aprender a producir seguridad y confianza en las infraestructuras digitales para el bien común.

Ministerio de Seguridad
Argentina

/minseg

/www.minseg.gob.ar