Vol. Nº 4
Noviembre/2020
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

CIBERVIOLENCIA CONTRA LA MUJER

Cifras y sucesos que debemos saber

Ransomware
Evolución de una amenaza

Cooperación Internacional
Rosa Díaz Moles, Directora General de Incibe

Tendencias
Cryptojacking: Amenaza virtual y silenciosa

Comunidad Hackers
Mujeres unidas por la ciberseguridad

Legal
Protección legal para la violencia de género

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes
Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Carolina Covarrubias
Cristobal Hammersley
Patricio Quezada

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Noviembre conmemora el día Internacional de la Eliminación de la Violencia contra la Mujer, un flagelo que persigue a la sociedad incluso en el mundo virtual en la medida que estas inaceptables conductas trascienden en sitios, redes sociales y otros medios que hoy son una extensión de nuestras vidas. Los números, en su frialdad, reflejan este mal: en Chile, un 62,9% de las mujeres asegura haber sido víctima de algún tipo de violencia en internet.

En nuestra cuarta edición de Cibersucesos queremos abordar como tema central la violencia de género a través de los distintos canales digitales, con el objetivo de entregar recomendaciones sobre qué hacer en caso de ser víctima e identificar las formas que se pueden manifestar el ciberacoso.

Así también, hablaremos sobre cómo hemos avanzado en materia legislativa sobre este tema en nuestro país. Actualmente, se encuentra en el Congreso la Ley Gabriela que busca sancionar la violencia de género contra las mujeres con tipos penales específicos como el femicidio. Además, se está trabajando en el proyecto de ley boletín Nº 11077-07 que tiene como fin asegurar el derecho de las mujeres a una vida libre de violencia.

En la sección "Comunidad Hackers" quisimos conversar con dos comunidades que están integradas sólo por mujeres, quienes nos contaron cómo se formaron y qué une a estos grupos que a diario trabajan por crear nuevos proyectos para fortalecer la ciberseguridad en nuestro país.

Por otra parte, y abordando los temas de contingencia nacional, en esta edición explicaremos el Ransomware, un malware que se ha hecho famoso por el daño y consecuencias que puede traer en una organización y para las personas. Ahondaremos en su definición, origen y cómo estar preparados para evitar ser una víctima de este ciberataque.

Y en esta misma línea, en la sección "Tendencia Digital" quisimos investigar más sobre el Cryptojacking o también conocido como "minería de criptomoneda maliciosa", una nueva forma de apoderarse de un equipo o dispositivo móvil y cada vez va tomando más fuerza en el mundo, y que busca extraer diversas formas de monedas digitales como las criptomonedas.

España se encuentra en el séptimo lugar en el Índice de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones. Cómo han llegado hasta esta posición, quién ha sido el encargado de dirigir esta transformación y mucho más, nos cuenta en la sección "Colaboración Internacional" Rosa Díaz, Directora General de Incibe.

Como ustedes verán, este número de Cibersucesos tiene la ambición de explicar temas contingentes y complejos en una perspectiva simple, pero no por ello superficial. La invitación general es reflexionar y estimular cambios para cuidarnos, tomando precauciones sobre amenazas tan avanzadas como el ransomware o el cryptojacking, hasta otras tan arraigadas como la violencia contra la mujer, y también, y como siempre es nuestra intención, compartir experiencias de esfuerzos y desarrollos de grupos y organizaciones en nuestro país y en el mundo.

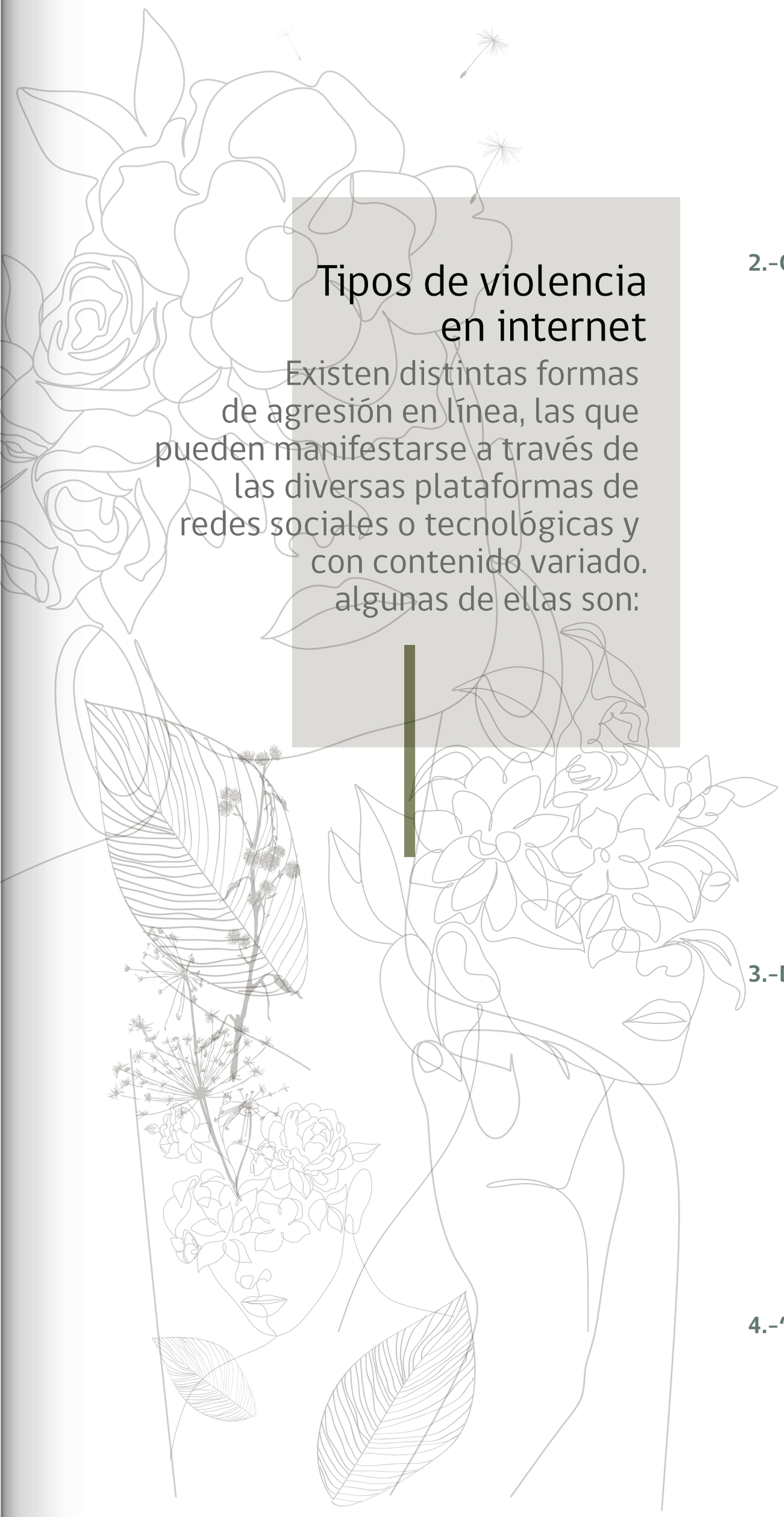
CIBERVIOLENCIA CONTRA LA MUJER

Cifras y sucesos que debemos saber

En el mundo virtual, un 62,9% de las mujeres asegura haber sufrido algún tipo de agresión. Este mes se conmemora el Día Internacional de la Eliminación de la Violencia contra la Mujer, el cual busca erradicar esta conducta que afecta cada año a miles de mujeres.

Desde temprana edad, algunos niños y niñas tienen un comportamiento abusivo hacia sus pares, un patrón que se repite cada año y que trae consecuencias negativas para quienes las reciben, especialmente las mujeres, ya que en su mayoría las agresiones son dirigidas a ellas, una conducta que se repite no sólo en el mundo real, sino que también en el virtual.

Esta práctica es conocida como "acoso en línea" y consiste en la difusión de datos personales, sextorsión, acoso, hostigamiento, abuso sexual, entre otras formas de manifestación, mediante canales digitales, siendo los compañeros, amigos, ex parejas u otros los principales agresores.



Tipos de violencia en internet

Existen distintas formas de agresión en línea, las que pueden manifestarse a través de las diversas plataformas de redes sociales o tecnológicas y con contenido variado. algunas de ellas son:

1.–CIBERACOSO O CIBERBULLYING:

El ciberacoso tiene que ver con el hostigamiento, humillación e injurias sufridas a través del uso de medios digitales. Comprende la suplantación de la identidad, creación de perfiles falsos online, e incluso la vigilancia a través de spyware o acceso a los perfiles de redes sociales. En muchos casos los atacantes se escudan detrás del anonimato e incitan su campaña de odio mediante el uso de hashtags y publicaciones para que sean compartidas por grupos de personas.

2.–CIBERACECHO O CYBERSTALKING:

Puede ser definido como el hostigamiento físico por medios digitales, esto es, el seguimiento reiterado de una persona a través de internet u otros medios electrónicos (como por ejemplo, cámaras de vigilancia, dispositivos de escucha electrónicos, software para computadores o aplicaciones para celulares, y dispositivos GPS), incluyendo conductas como el envío de comunicaciones no deseadas, avances o peticiones de carácter sexual, amenazas de violencia, y la vigilancia o monitoreo de la localización de la víctima, sus actividades cotidianas y/o sus comunicaciones.

RECOMENDACIÓN:
Al sufrir estos ataques, es conveniente bloquear al acosador e intentar cortar las vías de comunicación de inmediato. En el caso de que los mensajes abusivos sigan llegando, deberíamos guardar copias de las comunicaciones, no borrarlas. Esto servirá de prueba para el siguiente paso: DENUNCIAR.
Debido al aumento de los casos y a que cada vez más mujeres han alzado la voz, la legislación está cambiando para contemplar y dar atención a estos casos.

3.–DOXING:

Esta práctica consiste en la liberación de datos personales en Internet en forma fácilmente accesible, puede incluir nombres legales completos, direcciones personales, números únicos de identificación, documentos comerciales y fotografías personales y de sus familiares. Es posible que mucha de esta información ya se encuentre disponible públicamente, pero en formatos de difícil acceso o distribuidos en varias fuentes que los oculten de un descubrimiento casual, pero también puede tratarse de registros del gobierno, una empresa u organización obtenidos a través de una violación de seguridad.

4.–“PORNO VENGATIVO” O “PORNOGRAFÍA NO CONSENSUADA”:

Es cuando alguien publica contenido como fotos o videos sin el consentimiento de la afectada, ya sea para provocar humillación o vender el contenido a terceros. Tanto en el caso de que las fotos hayan sido obtenidas por hackeo, como por acceso físico a dispositivos o incluso por confianza debemos entender que dichas acciones corresponden a una violación a nuestra intimidad por tanto todos y todas tenemos derecho a la intimidad y a poder desenvolvernos en ella con libertad.

“Deepfakes”: una nueva arma contra las mujeres

Son videos que utilizan técnicas de aprendizaje automático para intercambiar la cara de una persona con la de otra. Dichas tecnologías surgieron en 2017 y se están utilizando en diferentes contextos, pero las más comunes están relacionadas con política y pornografía. La cantidad de videos falsos en línea está creciendo exponencialmente y se debe en parte al hecho de que ahora es más fácil para los no expertos usar ciertas tecnologías.
las mujeres son los principales objetivos cuando se usan deepfakes en pornografía. También comienzan a aparecer casos relacionados con el uso de dicha tecnología para atacar a las mujeres en la política. Un ejemplo es una conocida política estadounidense, que en 2019 apareció en un video como si estuviera ebria. El video se volvió viral rápidamente en Facebook

¿Qué pasa en Chile?

Las cifras de acoso a través internet hacia las mujeres en nuestro país dan cuenta de una triste realidad y confirman cómo los canales digitales potencian y complementan la violencia de género. Entre abril y junio de este año, el Proyecto Aurora de la ONG Amaranta realizó una encuesta sobre violencia digital y se centró en la experiencia de 531 mujeres, cisgénero, transgénero y personas no binarias.

LOS RESULTADOS DE ESTE ESTUDIO ARROJARON LOS SIGUIENTES RESULTADOS:

62,9% había sufrido algún tipo de violencia en Internet

- **66,4%** Violencia verbal
- **59%** Acoso y/o hostigamiento
- **49,6%** Envío de videos o fotografías de penes sin consentimiento
- **24,5%** Difamación
- **23,6%** Amenazas
- **16,5%** Pérdida de cuenta o acceso no consentido por parte de terceros

EN SU MAYORÍA, LOS AGRESORES SON:

- **41,9%** De usuarios anónimos o perfiles falsos
- **18,1%** Parejas o ex parejas
- **14,8%** Ataques de uno o más hombres del entorno cercano.

LA MAYOR CANTIDAD DE CASOS SE REGISTRARON EN LAS SIGUIENTES PLATAFORMAS:

Facebook
Instagram
WhatsApp
Twitter
Gmail

¿Cómo protegerse en redes sociales?

- Configura tu perfil como privado para asegurarte de sólo tener personas conocidas en tu comunidad.
- No aceptes a desconocidos en tus redes sociales.
- Cuidado con la información e imágenes que publicas en tus redes sociales. Toda actividad que se realiza en internet permanece de manera indefinida.
- Evita compartir fotografías y videos de contenido sexual con desconocidos.
- En caso de que tu dispositivo móvil sea robado o perdido, es factible saber en un rango aceptable donde podría estar, o realizar un borrado a distancia para eliminar los documentos o imágenes sensibles que tengas.

EL 25 DE NOVIEMBRE

Fue designado por la Asamblea General de las Naciones Unidas como el Día Internacional de la Eliminación de la Violencia contra la Mujer. En esta instancia se invitó a los gobiernos y otras organizaciones a promover actividades que sensibilicen a las personas sobre este problema a nivel mundial.

VIOLENCIA DE GÉNERO EN EL MUNDO

Algunas cifras que reflejan la violencia de género hacia las mujeres en todo el mundo, según datos de la ONU:

- El **35% de las mujeres** ha sufrido violencia física en algún momento de su vida.
- En la Unión Europea, **una de cada 10 mujeres** ha sufrido acoso en línea.
- En América Latina, **60 mil mujeres** son asesinadas al año.
- El **30% de las mujeres en América Latina** ha sufrido violencia sexual por parte de un conocido o desconocido, y solo el 40% ha pedido ayuda después del ataque.
- **Una de cada 2 de mujeres asesinadas** en 2017 fue asesinada por su compañero sentimental o un miembro de su familia.

https://www.csirt.gob.cl/recomendaciones/ciberguia-para-la-vilencia-contra-la-mujer/

Para mayor infromación CONTÁCTATE con nosotros 24x7 al CSIRT de Gobierno:

+56 2 2486 3850

E-mail con la información del incidente o anomalía detectada a **soc@interior.gob.cl**

Para DENUNCIA a la Unidad de Cibercrimen de la PDI:

+56 2 2708 0658

Si has vivido o sido testigo de violencia y tienes dudas sobre qué hacer y a donde acudir para obtener mas información **CONTÁCTATE al Ministerio de la mujer y equidad de género:**

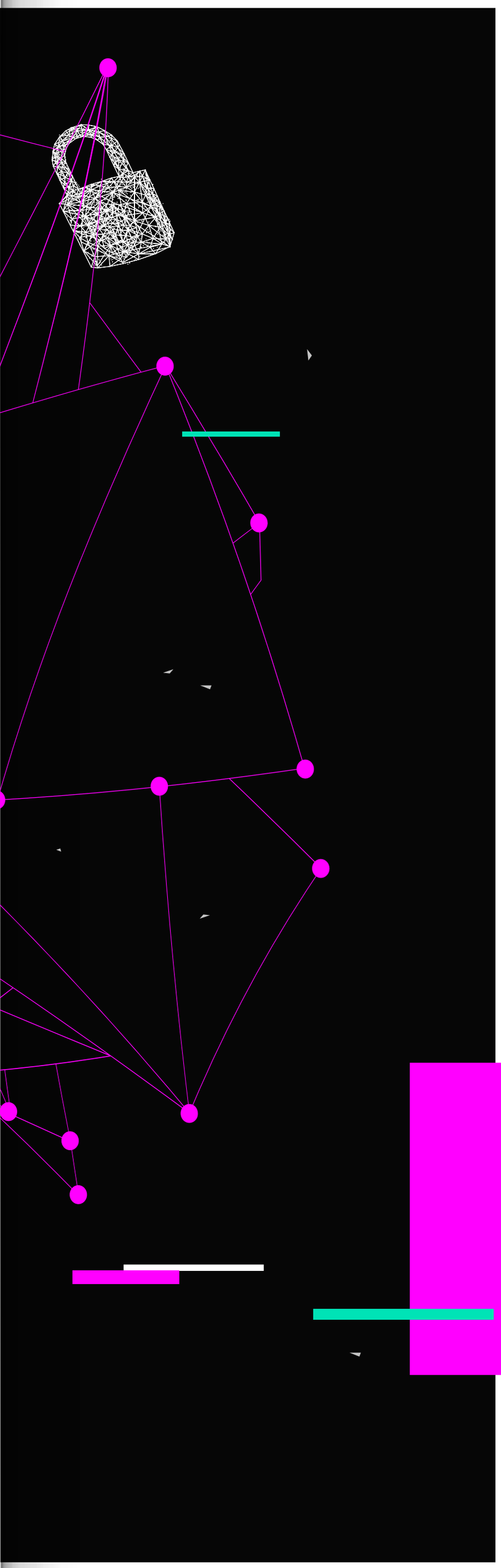
800 104 008

1455

RANSOMWARE

EVOLUCIÓN DE UNA AMENAZA

Todos los malware son dañinos, pero hay unos que pueden causar más daños que otros. Uno de los más complejos de combatir es el ransomware, el que ha pasado por diferentes etapas evolutivas. Ya sea encriptando archivos o bloqueando el acceso de los usuarios a carpetas, sistemas o dispositivos, el ransomware se ha consolidado como un negocio muy lucrativo para los atacantes, y recientemente, se ha transformado en una amenaza para la vida de las personas.



¿QUÉ ES UN MALWARE?

Malware es el término general utilizado para describir a cualquier tipo de software o programa malicioso diseñado por una persona u organización para infiltrarse en un sistema informático, con el fin de causar un daño. Su nombre proviene de las mezcla de las palabras “malicioso” y “software”, y existe una amplia variedad de tipos de malware que pueden atacar equipos, servidores o redes, entre ellos están los virus, los gusanos, los troyanos o los ransomware, entre muchos otros.

Este programa informático se ejecuta en el equipo o sistema de la víctima sin que ésta tenga conocimiento, y podrían pasar semanas o hasta meses antes de detectar la presencia del malware en un sistema. Muchas veces la constatación del perjuicio que genera un software malicioso es la única forma de advertir su presencia.

Los especialistas definen a los malware según sus características, la forma en que se propagan y por el daño que pueden producir.

Esta amenaza cibernética es cada día más diversa y compleja de perseguir, por las múltiples variantes que los cibercriminales producen a partir de una cepa específica. Hoy se pueden identificar varias familias de malware, lo que hace cada vez más difícil la labor de detección y prevención de ataques.

> La forma más utilizada para entregar un malware es a través de un enlace o un archivo dentro de un correo electrónico. Para ello, el atacante también recurre a técnicas de ingeniería social, y especialmente a un tipo específico de ataque, como el phishing, el que requiere que un usuario –la víctima– utilice un enlace malicioso o ejecute un programa adjunto en un correo electrónico para iniciar el proceso de descarga del malware.

La evolución de los malware ha llegado a tal punto, que hay ciertos tipos específicos de malware cuyo desarrollo sirve para la descarga de otros malware. Ese es el caso de Emotet, que pasó de ser un malware bancario, a un descargador de otros malware.

Ciberdato:

A propósito de lo ocurrido hace muy poco con el ataque ransomware que sufrió el Banco del Estado de Chile, Kaspersky publicó un informe con el actual panorama de amenazas informáticas que se registran en nuestra región latinoamericana con cifras para considerar detalladamente.

Según esta empresa de seguridad, entre enero y septiembre de 2020 registraron 1,3 millones de intentos de ataque de ransomware en América Latina. Esto significa un promedio de 5.000 ataques por día y entre los países más afectados están Brasil, México, Colombia, Perú y Ecuador.

EL RANSOMWARE Y SUS COSTOS

Todos los malware son dañinos, pero hay unos que pueden causar más daños que otros. Uno de los más complejos de combatir es el ransomware. Este malware, dirigido principalmente a organizaciones, tiene la capacidad de cifrar archivos en una computadora o en un sistema informático completo, de modo que secuestra los datos que son críticos para el funcionamiento de la institución afectada.

Igual que un secuestro, el objetivo principal de este ataque es exigir un rescate para devolver la información retenida, el que por lo general es valuado en criptomonedas, para de esa forma no dejar rastros del atacante. Por cierto, los riesgos en caso de acceder a las demandas del atacante es no obtener el resultado esperado y la eventual pérdida de la información. Es por eso que muchas organizaciones no están dispuestas a pagar los rescates, pero las que lo hacen, se inclinan por esa alternativa dado la criticidad de la información secuestrada, la que es fundamental para su operación.

Las pérdidas por ransomware se cuentan por varios cientos de millones de dólares anualmente. Purplesec, una firma norteamericana de ciberseguridad, estimó que el costo económico para las organizaciones víctimas de ransomware pasaron de $11,5 billones en 2019 a $20 billones este año 2020, aumentando el pago promedio por ataque en 104%. Solo en el área de la salud, el ransomware ha costado unos $157 millones de dólares.

El ransomware representa un gran negocio para los cibercriminales, lo que genera un incentivo entre éstos para desarrollar nuevas versiones, lo que respalda la noción de que esta amenaza está en constante crecimiento.

CRONOLOGÍA Y EVOLUCIÓN DE LA AMENAZA

1.- El primer ransomware fue creado en 1989 por el biólogo Jospeh L. Popp, y fue distribuido a través de disquets en una conferencia internacional de la OMS sobre el SIDA. Se le conoció como el troyano AIDS. El mensaje demandaba a las víctimas el pago de $189 dólares para desencriptar sus equipos.

2.- Un poco más de un cuarto de siglo después, los ransomware evolucionaron hasta su versión moderna. 2005 es el año "0" para los nuevos malware y GPCoder es señalado como el primero en su tipo. Su objetivo era infectar los sistemas Windows, copiar los archivos de forma cifrada y luego borrar los originales. El software malicioso utilizaba un sistema complejo de cifrado, el que volvía infructuoso cualquier tipo de desbloqueo. Ese mismo hizo su aparición Archievus, el que encriptaba la carpeta "Mis documentos" de los usuarios. Aunque permitía seguir utilizando los equipos, todos aquellos que almacenaban su información en esa carpeta, se veían impedidos de utilizarla.

3.- El desarrollo de antivirus acortó la vida de GPCoder y Archievus, hasta que en 2009 Vundu irrumpió, evolucionando desde otro tipo de malware hasta convertirse en ransomware. Uno de los factores que colaboró con la proliferación de Vundu fue la implementación de plataformas online de pagos anónimos.

4.- En 2011 aparecieron los ransomware locker o bloqueadores con el troyano WinLock, los que no buscan encriptar los archivos, sino simplemente impedir el acceso a éstos.

5.- La siguiente evolución fue Reveton, también conocido como virus policial, cuyo mensaje indicaba ser enviado por un organismo policial y advertía que poseía pruebas sobre el uso del dispositivo de la víctima en actividades ilícitas, y que el desbloqueo de los archivos supuestamente confiscados correspondía a una especie de soborno o multa.

6.- CrytoLocker hizo su aparición entre 2013 y 2015, y con él volvieron los ataques con cifrados, y amenazando a la víctima que en caso de no pagar el rescate sería la eliminación de la información secuestrada. La novedad de este nuevo ransomware fue que utilizó diferentes medios de propagación, desde web infectadas hasta phishing.

7.- 2017 fue un año emblemático para los rasomware cuando todo el mundo escuchó hablar de WannaCry, el que aprovechaba de explotar las vulnerabilidades que encontraba en los equipos. Este ransomware se propagó con enorme rapidez en diferentes sistemas y países, y alcanzó los titulares del mundo por atacar al Servicio Nacional de Salud del Reno Unido, el NHS. Luego de este ataque, muchos otros han adquirido gran fama, como Peyta, Leaker Locker, Buran, Cuba o Ryuk.

8.- El pasado mes de septiembre los ataques de ransomware adquirieron una nueva y oscura dimensión al cobrar por primera vez la vida de una persona luego de interrumpir el funcionamiento del Hospital de la Universidad de Dusseldorf, en Alemania. El ataque explotaba una vulnerabilidad de un sistema (Citrix, CVE-2019-19871) e hizo colapsar la continuidad operacional del servicio médico, lo que obligó a trasladas a la paciente afectada a otro centro de salud, falleciendo en el trayecto.

Estos últimos incidentes, especialmente en el contexto de pandemia, han cambiado la imagen del ransomware. Ya no solo se trata de un negocio ilícito. Hoy los ransomware, amenazando a las infraestructuras críticas, pueden llegar a ser letales.

BUENAS PRÁCTICAS
prevención y mitigaciones

- Mantener copias de seguridad periódicas de todos los datos importantes, sin conectividad con otros sistemas.
- Contar con la última actualización de seguridad de los sistemas operativos o software.
- Disponer de una correcta configuración de los cortafuegos a nivel de aplicación.
- No permitir que los usuarios puedan instalar aplicativos.
- Contraseñas seguras. Es importante que a nivel organizaciones se definan las características que deben tener las contraseñas de los equipos, correos electrónicos, etc.
- Evitar que los trabajadores usen sus propios dispositivos, ya que por lo general no cuentan con las medidas mínimas de seguridad, por lo tanto constituyen un riesgo para la empresa.
- Contar con sistemas antispam y antimalware a nivel de correo electrónico y establecer un nivel de filtrado alto.
- Usar bloqueadores de Javascript para el navegador que impida la ejecución de todos aquellos scripts que puedan suponer un daño para los equipos.
- Extender las medidas de seguridad a empresas proveedoras para que no ser infectado por un tercero.

Unidos **somos más fuertes**

Rosa Díaz Moles
Directora General de Incibe

Vivimos tiempos de cambio en los que nos hemos visto obligados a replantearnos nuestro presente y futuro, no solo como individuos, sino también como entidades que forman parte del relevante escenario global de la seguridad digital. Durante esta situación tan excepcional y extraña, que ha trastocado lo que antes conocíamos como normalidad, hemos tomado mayor consciencia de la importancia de la digitalización como una de las mejores soluciones a los retos que nos hemos ido encontrando en el camino. En este tiempo nos hemos replanteado muchas cosas que asumíamos como inalterables. Del mismo modo, hemos roto paradigmas digitales, como el del teletrabajo, desterrando falsos mitos y comprobando que, entre sus múltiples beneficios, destaca un notable aumento de la productividad. Pero si algo hemos aprendido durante estos meses es que, utilizando los recursos disponibles de manera segura, todos avanzamos y eliminamos las barreras que surgen a nuestro paso. Juntos, hemos contrastado que los problemas pueden ser globales y afectar por igual a todos, sin diferenciar entre territorios, y que, la única manera de afrontarlos con éxito es hacerlo unidos. Hoy, más que nunca, la tecnología acorta distancias y, por ello, es indispensable apostar por la ciberseguridad en nuestro día a día.

De esta manera, la seguridad en el ciberespacio se ha posicionado como unos de los objetivos prioritarios dentro de las agendas de muchos países, con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza y en la divulgación de la cultura de la ciberseguridad. España consolida año tras año su apuesta y contribuye al esfuerzo conjunto de la comunidad internacional desarrollando la colaboración coordinada como estrategia global de trabajo. Y en ese horizonte está sin duda España Digital 2025, la agenda digital que nuestro país desarrollará en los próximos años, y en la que la ciberseguridad tiene un papel relevante como uno de sus 10 pilares estratégicos. Este documento, en el que ha colaborado el Instituto Nacional de Ciberseguridad, constituye un auténtico cuaderno de bitácora sobre la digitalización, la conectividad y el desarrollo económico, y la investigación en España. Y en ese contexto resalta el rol decisivo de la ciberseguridad, no solo como protección a ciudadanos, empresas y gobierno en el ciberespacio, sino también como palanca para la generación de confianza y el crecimiento económico.

Actualmente, España ocupa la séptima posición en el Índice de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones. Como no podía ser de otro modo, INCIBE, la entidad que tengo el orgullo de dirigir, juega un papel destacado en el desarrollo de los objetivos de esta estrategia, por nuestro papel de centro de referencia para ciudadanos y empresas privadas. Somos conscientes de que los delitos cibernéticos son cada vez más sofisticados y la ciberdelincuencia ha experimentado un proceso de profesionalización que podría compararse al de estructuras empresariales eficientes y eficaces. Precisamente por eso trabajamos unidos, tanto desde el sector público como desde el privado, para mantener una posición destacada en seguridad digital. Tenemos un gran reto por delante, y desde INCIBE queremos aportar nuestro grano de arena para que España sea uno de los 5 países más ciberseguros del mundo, y ese esfuerzo debe ser un compromiso compartido.

Pero en este camino no queremos estar solos. Deseamos ir de la mano de muchos otros países que comparten nuestra visión y estrategia, y por ello desarrollamos alianzas internacionales que pretenden un crecimiento conjunto, defendiendo la vital importancia que supone la tanto la colaboración público-privada como la de entidades de carácter público. En nuestro caso, consideramos necesario el liderazgo público a través de nuestra institución, pero también creemos que es esencial el compromiso y la participación del resto de actores públicos y privados. La colaboración global es una herramienta imprescindible para poder fortalecer la protección de ciudadanos y empresas.

Desde INCIBE trabajamos en la creación de alianzas con otros países para mejorar la prevención, la respuesta coordinada ante incidentes de seguridad y posicionar a España como un referente internacional en ciberseguridad que facilite el acceso de las empresas a este nuevo escenario global que es el de la ciberseguridad. Mejorar la cooperación y el intercambio de información entre CERTs a nivel global es uno de los principales desafíos a los que actualmente se enfrenta el campo de la ciberseguridad, tanto a nivel de organizaciones públicas como privadas. Así, hemos suscrito en estos últimos años más de 200 acuerdos de colaboración con organizaciones públicas y privadas, tanto nacionales como internacionales, con el objetivo de trabajar conjuntamente en el desarrollo de la ciberseguridad.
El ciberespacio hace posible la conectividad universal y abre las puertas al flujo libre de información, ideas y servicios, constituyéndose en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. Solo mediante la información actualizada, contrastada y compartida podemos abordar de manera global esta lucha. Sin duda, esta estrategia define una dimensión fundamental para la estabilidad al preservar la defensa de los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.

En aras de unir lazos con otros países, de colaborar en esta labor conjunta internacional y siguiendo con ese espíritu de adaptación al cambio que ha definido nuestros pasos en los últimos meses, celebramos recientemente la quinta edición de nuestro Cybersecurity Summer Bootcamp, este año, con un novedoso formato virtual. Este programa internacional de capacitación en ciberseguridad, organizado por el Instituto Nacional de Ciberseguridad (INCIBE) y la Organización de los Estados Americanos (OEA), reunió a Policy makers, miembros de las Fuerzas y Cuerpos de Seguridad, especialistas de Centros de Respuesta a Incidentes Cibernéticos y personal del ámbito judicial y fiscal, al igual que otros interesados en seguridad digital, potenciando e incrementado sus capacidades y habilidades en ciberseguridad a través de keynotes, paneles y seminarios virtuales de la mano de prestigiosos ponentes. En total, reunimos a más de 1.000 personas de 62 países compartiendo conocimientos, estrategias y visión, y demostrando que la cadena se fortalece con cada nuevo eslabón que se suma.

Tal y como se recoge en la Estrategia Nacional de Ciberseguridad de nuestro país, debemos trabajar en la transición desde un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema proactivo y coordinado que incorpore elementos de mayor fuerza disuasoria obedece a un contexto global de mayor competencia geopolítica. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa como elemento fundamental de la acción de todos los Estados.
Compartamos información y conocimiento, aprendamos de los demás y reforcemos la seguridad digital. Ese debe ser el camino.

Rosa Díaz Moles

Licenciada en Ciencias Exactas por la Universidad Autónoma de Madrid y cuenta en su formación con un Programa de Dirección General por el IESE Business School. Ha formado parte del equipo de INCIBE desde junio de 2019, primero a través del puesto de Subdirectora de Empresas y Profesionales, después como Subdirectora de Apoyo a la Empresa e I+D+i desde septiembre de 2019 y a partir de noviembre como Directora General.
Con una sólida experiencia en el sector TIC, Rosa Díaz ha desempeñado diferentes cargos directivos en empresas como Sage España, donde llego a ser Directora de Operaciones en la división de Pymes y Autónomos y Formación, Santander Elavon Merchant Services S.L., donde fue Directora de Soporte, y Panda Security, donde desempeñó el puesto de Country Manager Iberia durante casi cuatro años.
Pertenece a diferentes grupos que tienen como objetivo dar visibilidad a la mujer en puestos de trabajo dentro del mundo de las TIC y en específico en el sector de la ciberseguridad, siendo además cibercooperante de INCIBE desde mayo de 2018 con el objetivo de difundir y concienciar a jóvenes y familiares de la importancia de la ciberseguridad para estar más seguros en nuestra vida digital.

CRYPTOJACKING

Amenaza virtual y silenciosa

Aunque aún desconocido por buena parte del público, el cryptojacking se ha convertido rápidamente en una de las formas más comunes de malware. Se diferencia de otros malware porque su objetivo apunta a utilizar la capacidad de procesamiento de los dispositivos de sus víctimas antes que el robo de datos. La necesidad de sacar ventaja de la potencia de procesamiento es utilizada para la extracción o minería de criptomonedas, tales como el Bitcoin o Ethereum.

En una forma simple de decirlo, el Cryptojacking es el uso ilegítimo de un dispositivo electrónico por parte de un atacante, con el objetivo de minar criptomonedas. Las víctimas de este tipo de ataques a menudo no tienen idea de que se está utilizando su dispositivo con ese propósito, pero si puede observar algunas señales de que algo malo está ocurriendo, como lentitud en la conexión a internet o lentitud general en el procesamiento de datos a pesar de no tener aplicaciones abiertas.

¿CÓMO FUNCIONA LA MINERÍA DE **CRIPTOMONEDAS**?

Se denomina como minería de criptomonedas a la acción de validar transacciones anteriores a la criptomoneda. Dicho de otra forma, los mineros son una suerte de auditores o verificadores de transacciones. El propósito de estos mineros es generar confianza en el intercambio de criptomonedas, pues sus verificaciones apuntan a eliminar la duplicación o falsificación de una criptomoneda, pues existe el riesgo que esta moneda pueda ser copiada para enviarla a un comerciante y mantener la moneda original.

De alguna forma los mineros verifican las transacciones para asegurarse de que los usuarios no hayan intentado de forma ilegítima gastar la misma criptomoneda dos veces. Cuando un minero ha verificado 1 MB (Megabyte) en transacciones -lo que se conoce como bloque- ese minero es "elegible" para ser recompensado con criptomonedas, pero eso no asegura que los vaya a recibir.

Para obtener la recompensa, además del laborioso trabajo de minar o verificar este megabyte de transacciones o bloque, debe tener algo de buena fortuna y ser el primero en resolver un problema numérico que se conoce como "proof of work", o prueba de trabajo, lo que requiere un esfuerzo no menor, pero factible.

Esta competencia entre los mineros es la que genera la necesidad por capacidad de procesamiento y el principal motor del cryptojacking.

Ciber**Dato:**

El aumento de los precios de las criptomonedas desde marzo ha ido acompañado de una ola de ataques de cryptojacking, según una nueva investigación publicada por la empresa de seguridad cibernética Symantec, según la compañía, hubo un aumento del 163% en la actividad de cryptojacking en el segundo trimestre de 2020.

¿CÓMO FUNCIONA **EL CRYPTOJACKING?**

Los mineros de criptomonedas utilizan diferentes formas para capturar un dispositivo. Una forma –la más habitual– es mediante la distribución de malware a través de phishing, utilizando un enlace o un archivo adjunto en un correo electrónico. Cuando los usuarios utilizan el enlace o abren un archivo adjunto, el código de minería criptográfica se cargará directamente en la computadora, teléfono móvil o servidor. Cuando el atacante recibe la confirmación de la descarga, puede comenzar de inmediato a usar estos recursos de red para minar las 24 horas.

Los correos fraudulentos no son el único método para distribuir el malware para el cryptojacking, también se puede hacer a través de sitios web dañins y exploits kits. Por lo general, los objetivos de los atacantes son los dispositivos móviles, los servidores y los dispositivos considerados IoT (Internet de las cosas).

Junto con la lentitud general del dispositivo o de la conexión a internet, otros síntomas para reconocer el cryptojacking en un equipo pueden ser un procesador con una alta carga de cómputo sin que existan aplicaciones abiertas en uso, el sobrecalentamiento de los componentes o procesos no conocidos ejecutándose.

¿CÓMO PROTEGERSE **DEL CRYPTOJACKING**?

Como ocurre con muchas amenazas de malware, pueden pasar semanas o meses antes de detectar el incidente. Son los síntomas antes mencionados los que dan cuenta de lo ocurrido.

Si contemplamos que esta amenaza tiende a crecer en popularidad, es solo cuestión de tiempo para que nuestro ecosistema local también sea víctima de intrusiones de este tipo, las que además se volverán más sofisticadas. Por lo tanto, la prevención a nivel de administración es el mejor método de protección.

El llamado para las organizaciones es actuar a nivel de firewall mediante el uso de sistemas avanzados de prevención de intrusiones y firewalls de próxima generación. Si una red se ve comprometida por un cryptojacking, se deben tomar medidas para realizar un análisis de la causa que identifique cómo fue instalado el malware, de modo que se puedan evitar más ataques similares.

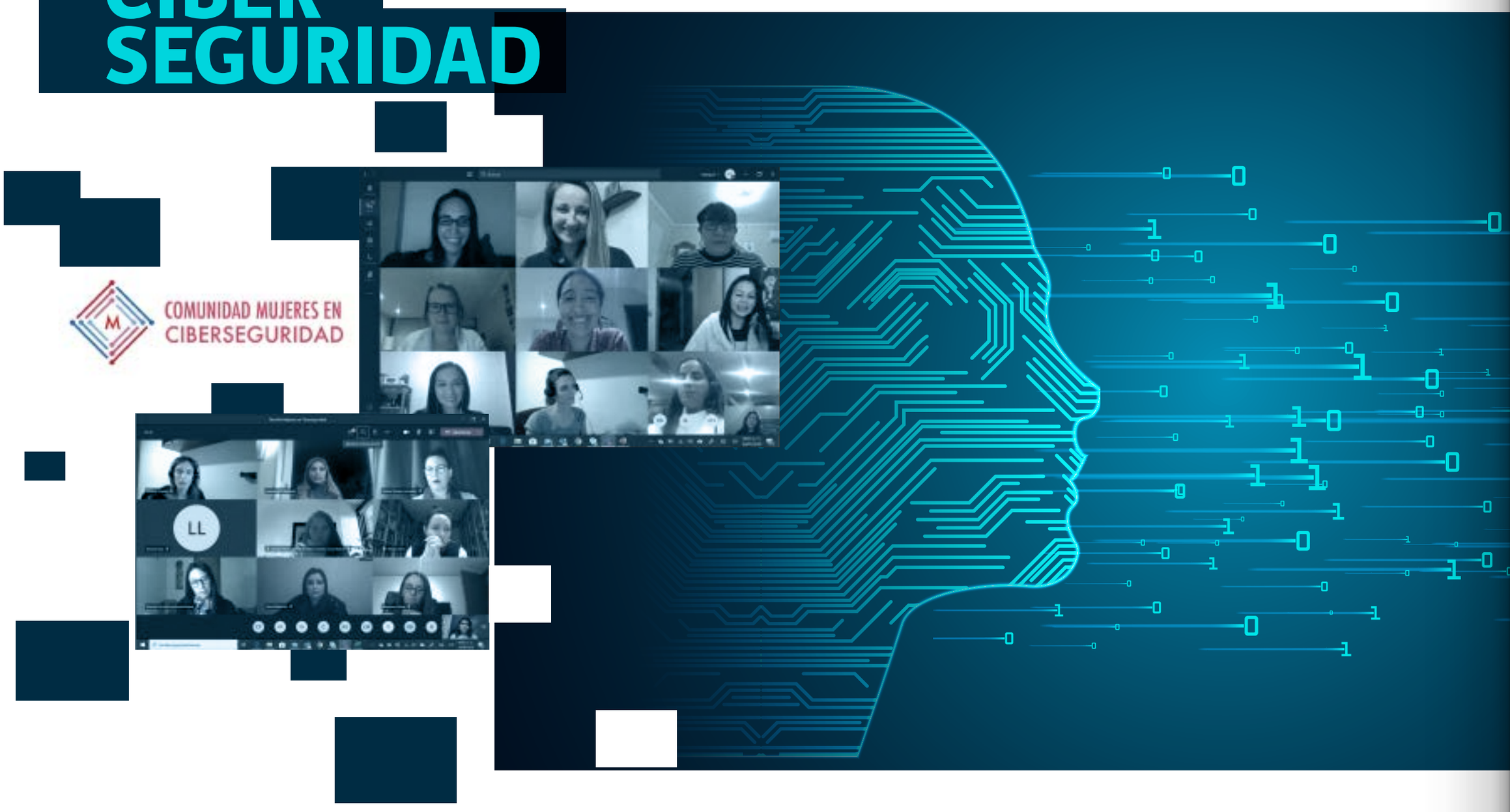
ALGUNOS CONSEJOS QUE PODEMOS COMPARTIR PARA **EVITAR SER VÍCTIMAS DE ESTA AMENAZA SON:**

- ✓ TENER ACTUALIZADO EL ANTIVIRUS
- ✓ USAR NAVEGADORES SEGUROS
- ✓ MANTENER ACTUALIZADO EL SISTEMA OPERATIVO
- ✓ USAR MÉTODOS DE BLOQUEO PARA VENTANAS EMERGENTES
- ✓ MOSTRAR LAS EXTENSIONES DE LOS ARCHIVOS

EN CASO DE SER VÍCTIMAS DE UN ATAQUE DE ESTE TIPO, **LO IDEAL ES:**

- **DESCONECTAR** EL EQUIPO DE LA RED.
- **ANALIZAR** EL DISPOSITIVO CON UN ANTIVIRUS ACTUALIZADO
- **ANALIZAR Y UTILIZAR** TECNOLOGÍAS DE ANTIMALWARE
- **FORMATEAR** EL EQUIPO PARA EL PROCESO DE LIMPIEZA

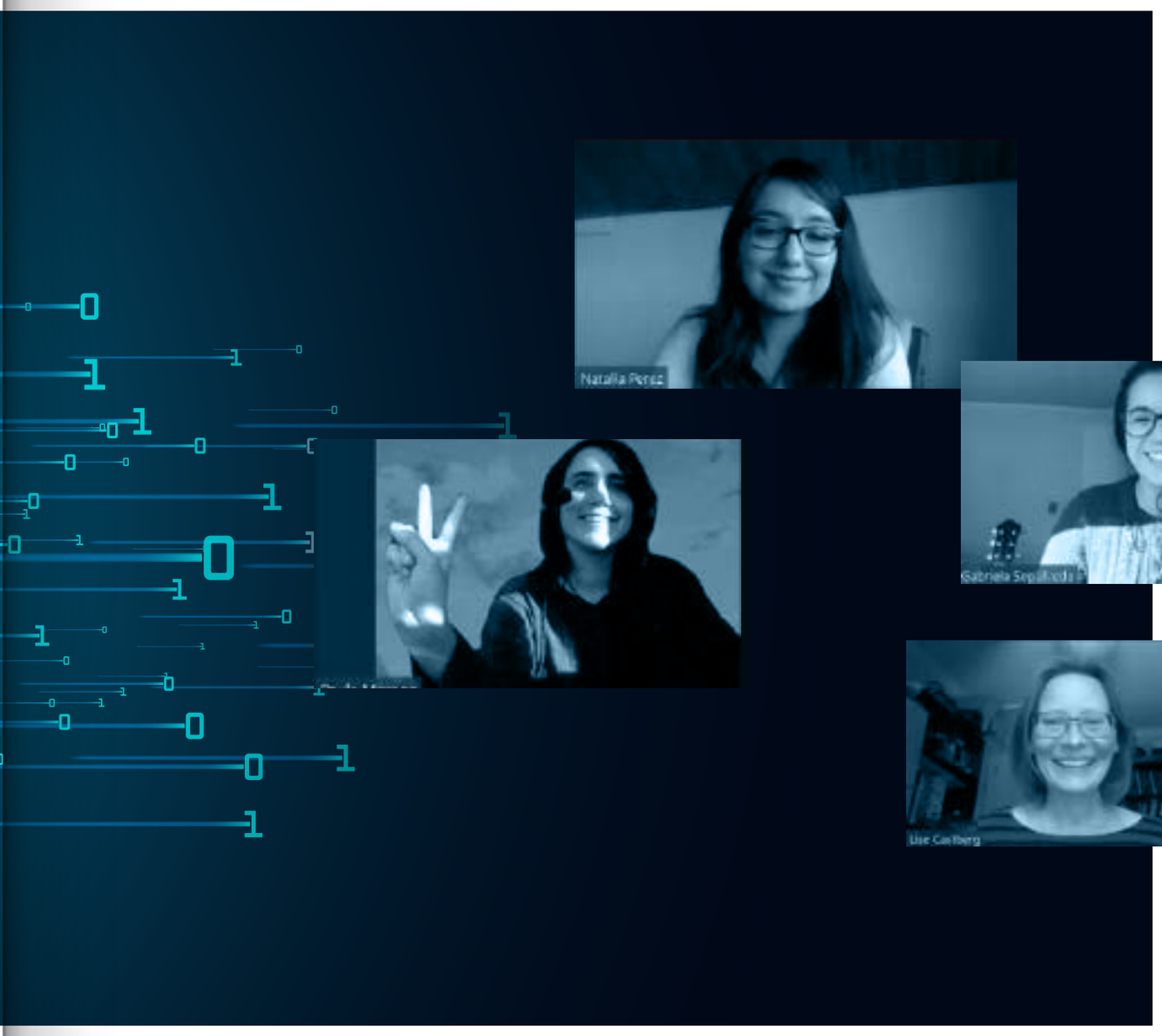
MUJERES UNIDAS POR LA CIBER SEGURIDAD



No se conocían entre ellas, pero sí las unió un tema en común: la participación activa de las mujeres en ciberseguridad. A través de distintas iniciativas y proyectos, dos grupos de mujeres se reúnen cada cierto tiempo para compartir experiencias e intercambiar sus visiones sobre esta materia.

Todo comenzó con la idea de visibilizar a las mujeres en ciberseguridad, debido a lo difícil que era ubicarlas para participar en eventos de este tipo. Así fue como a finales del año 2019, a cargo de la Alianza Chilena de Ciberseguridad, se realizó la primera nominación de mujeres destacadas en ciberseguridad.
A esta actividad se nominaron a 29 mujeres que se desempeñaban en distintas áreas relacionadas con la ciberseguridad, como técnicos, dirección, abogadas, etc., quienes se dieron cuenta que compartir sus experiencias y conocimientos podría ser muy enriquecedor tanto para ellas como para las organizaciones donde trabajaba cada una. Así nació la "**Comunidad de mujeres en ciberseguridad"**, que tiene como "objetivo intercambiar conocimientos técnicos sobre diversos temas que permitan contribuir a la labor de cada una. Esto nos motivó a juntarnos cada cierto tiempo y conversar, con las distintas miradas, sobre temas contingentes que ocurren en Chile. Por ejemplo, ya hemos abordado temas como el 5G y la normativa de ciberseguridad, además de la ciberseguridad industrial" cuenta Karin Quiroga, Directora de la Alianza de Ciberseguridad e impulsora de la iniciativa.
Y así como este grupo de mujeres motivadas por contribuir en este tema que cada día toma más relevancia en el mundo, también existen otros como es el caso de la **"Comunidad Lovelace"**, que se formó a partir de la necesidad de organizar una arista nueva de la conferencia de la 8.8 Computer Security Conference. En este caso, la conferencia solo contará con conferencistas mujeres y se desarrollará este 2 de diciembre.

Katherina Canales, Directora operacional del CSIRT de Gobierno e integrante de ambas comunidades, cuenta que "a mediados de este año nos juntamos cinco mujeres de diversas instituciones que lideran áreas de tecnología o ciberseguridad para planificar este evento, el cual representa un gran desafío por ser la primera conferencia de este tipo y que busca mostrar las habilidades y competencias técnicas que tienen las mujeres, y así motivar al género a participar de estas actividades y formarse en un área tan transversal y dinámica como es la ciberseguridad.



Y si bien todo empezó para organizar esta conferencia, el grupo se ha motivado y propuesto nuevos desafíos. Así fue como participó activamente en la realización de "Villa Mujeres", parte de la 8.8 Leyendas Sandbox, que se llevó a cabo entre el 28 y 31 de octubre, para celebrar los 10 años de creación de esta organización.
La formación de estos grupos contribuye a promover buenas prácticas y generar equipos de trabajo para fortalecer aún más la ciberseguridad de nuestro país, una tarea de todos y que gracias a la unión y sinergia de varias entidades es posible generar una cultura de ciberseguridad, tan necesaria en estos días que hemos visto la importancia de proteger nuestra información y la de todos los chilenos.

Por esto, cada una de las comunidades tiene sus proyectos y buscan a diario crear más instancias que permitan promover los conocimientos y hacerlos extensivos a más personas. La "Comunidad de mujeres en ciberseguridad" ya está planificando el cierre del año 2020 y un plan de trabajo para el 2021, con la realización de cursos u otras actividades que permitan contribuir en esta área. Por esta razón, durante las próximas semanas se activará por segundo año la nominación de mujeres destacadas en ciberseguridad y, como novedad, en esta nueva versión se espera contar con un comité de expertos para evaluar y dar a conocer la contribución de cada una de las nominadas en este rubro. Las bases y requisitos se darán a conocer prontamente.

"En representación de estos dos grupos a los que pertenezco, quiero invitar a todas las personas a que se motiven a participar de comunidades o actividades que fomenten de manera positiva la ciberseguridad, ya que es la mejor forma de contribuir, prevenir, aprender sobre los riesgos y de esta forma poder traspasar las mejores prácticas a nuestros equipos y a la ciudadanía", recalca Katherina.

PROTECCIÓN LEGAL **PARA LA VIOLENCIA DE GÉNERO**

Al 4 de noviembre de 2020, y según datos oficiales del Ministerio de la Mujer y Equidad de Género, se registran en Chile 34 femicidios consumados y 120 femicidios frustrados, es decir, cada dos días y medio un hombre intenta matar a una mujer y cada 9 lo logra.

Esto es solo el reflejo de las diversas formas de violencia que las mujeres, sólo por el hecho de ser mujeres, viven de parte de sus parejas o de su entorno, las que van desde el control hasta la agresión física. Esto es una manifestación más de la violencia de género, la que se justifica porque en muchas culturas, incluida la nuestra, se cree que los hombres tienen derecho a controlar la libertad y la vida de las mujeres.

Esta violencia lamentablemente afecta a mujeres de cualquier edad, condición económica, social y de cualquier etnia, orientación sexual, raza o religión y puede ocurrir al interior de la pareja, en el trabajo, en los lugares de estudio, en los espacios públicos, violencia que también puede ser de distintos tipos.

LA VIOLENCIA TIENE DISTINTAS CARAS

Podemos distinguir al menos 5 tipos de violencia de género:

1.– VIOLENCIA FÍSICA:
Corresponde a todas las formas de agresión a las mujeres que van desde los empujones y zamarreos a golpes, siendo la manifestación más grave el femicidio.

2.– VIOLENCIA PSICOLÓGICA:
Se relaciona con el intento de control a una mujer mediante amenazas, humillaciones y presión emocional, con el propósito de hacerla sentir insegura y sin control sobre su vida y decisiones.

3.– VIOLENCIA ECONÓMICA:
Se refiere al control hacia una mujer a través de la entrega del dinero para su mantención personal y/o de las hijas o hijos, o de otras personas que integran la familia. También constituye violencia económica cuando se apropian del dinero que la mujer ha obtenido en razón de su propio trabajo.

4.– VIOLENCIA SEXUAL:
Cuando una mujer es obligada, mediante la fuerza física o amenazas sicológicas, a tener relaciones sexuales o a realizar actos sexuales que le resultan humillantes o degradantes.

5.– VIOLENCIA OBSTÉTRICA:
Es un tipo de violencia contra las mujeres durante el embarazo, parto y postparto que constituye una violación a los derechos humanos.

¿QUÉ ES LA VIOLENCIA CONTRA LA MUJER?

Según el artículo 1 de la Declaración sobre la Eliminación de la Violencia Contra la Mujer de las Naciones Unidas es: "todo acto de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para la mujer, así como las amenazas de tales actos, la coacción o la privación arbitraria de la libertad, tanto si se producen en la vida pública como en la vida privada".

¿Qué estamos haciendo en Chile para hacernos cargo de la violencia de género?

El derecho de las mujeres a vivir sin violencia está consagrado en tratados internacionales como la "Convención sobre la eliminación de todas las formas de discriminación contra la mujer" (CEDAW), la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer Convención de "Belem do Pará", en especial a través de sus Recomendaciones Generales N° 12 y 19 y de la Declaración sobre la Eliminación de la Violencia contra la Mujer de las Naciones Unidas. Además, ONU Mujeres trabaja con los países para avanzar en la generación de marcos normativos internacionales que presten apoyo a procesos inter gubernamentales, tales como la Asamblea General y la Comisión sobre la Condición Jurídica y Social de la Mujer.

A nivel nacional, se ha estado trabajando intensamente en una agenda legislativa para hacernos cargo del problema de la violencia de género. Así, uno de los últimos proyectos en ser aprobados por el Congreso es la llamada "Ley Gabriela" (Ley N° 21212), ley conocida con dicho nombre en honor a Gabriela Alcaíno y su madre Carolina Donoso, quienes fueron asesinadas en manos del ex pololo de la menor. Dicha ley, sanciona la violencia de género contra las mujeres con tipos penales específicos como el femicidio por causa de género y una serie de agravantes que elevan las penas.

De este modo, las sanciones que enfrentan quienes cometan estos delitos son de presidio mayor en su grado máximo a presidio perpetuo calificado, es decir de 15 años y 1 día a 40 años.

Junto a lo anterior, y con el fin de generar una mayor conciencia en la sociedad respecto a este tipo de violencia, se encuentra actualmente en su trámite de finalización en la Cámara de Diputados el proyecto de ley que establece el día 19 de diciembre de cada año como el día Nacional contra el Femicidio.

Finalmente, destacar el proyecto de ley boletín N° 11077-07 que busca asegurar el derecho de las mujeres a una vida libre de violencia. Proyecto que se encuentra en su segundo trámite Constitucional en el

Senado y que tiene por objeto prevenir, sancionar y erradicar cualquier tipo de violencia contra las mujeres, para lo que regula mecanismos de protección, acceso a la justicia y atención a quienes sean víctimas de ella, tanto en el ámbito público como en el privado.

El proyecto reconoce distintas formas de violencia contra la mujer, tales como la física; psicológica; sexual; económica; simbólica; institucional; política; laboral y la indirecta; cada una de las cuales precisa.

Asimismo impone a los órganos del Estado que desarrollen políticas, planes y programas u otros actos relacionados con la violencia y sus diversas manifestaciones, el deber de propender, en el marco de sus competencias, a la adopción de las medidas apropiadas para dar cumplimiento a los objetivos y disposiciones del proyecto de ley.

Regula, en particular, las medidas que pueden adoptarse en los ámbitos de la educación y en lo relativo a los medios de comunicación, y establece normas especiales relativas a la protección y atención de las mujeres frente a la violencia.

Entrega a los ministerios de la Mujer, de Justicia y de Salud la promoción de la implementación de servicios de apoyo para asistir a las mujeres víctimas de violencia y a las personas que se encuentren bajo su cuidado.

También introduce una normativa tendiente a hacer más expedito y eficiente el acceso a la justicia de las mujeres que han sido víctimas de los hechos de violencia e impone a los jueces de familia el deber de considerar el hecho de existir antecedentes de violencia intrafamiliar entre las partes involucradas.

Como se puede apreciar, existe una extensa agenda legislativa en la materia, por tanto la responsabilidad del poder legislativo de darles la importancia y seriedad a su tramitación a fin que prontamente contemos con el reproche penal que estos ilícitos se merecen.

Otro importante proyecto es el proyecto de ley denominado "Ley pack" boletín N° 12164-07 que busca penar la difusión no consentida de imágenes con contenido sexual o "revenge porn" en el cual la víctima, si bien consiente en la producción del registro visual con contenido sexual, no lo hace respecto a la difusión del mismo. Pero nada de esto sirve si no se denuncian este tipo de conductas, por eso, si eres víctima de este tipo de violencia: **¡DENUNCIA!**

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl