CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

Vol. Nº 2
Agosto/2020
www.csirt.gob.cl

CIBERBULLYING Y GROOMING

Los niños ante los riesgos invisibles.

Tercera edad en la era digital
Inclusión tecnológica segura

Cooperación Internacional
Alison Treppel
OEA

Tendencia Digital
Cookies

Comunidad Hackers
Cyberwomen Challenge

Legal
Proyecto Ley
Delitos Informáticos

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informatica 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 Improving Security Together · CSIRTamericas.org · MERIDIAN Connecting and Protecting

ÍNDICE

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
Carlos Silva
Patricio Quezada

Diseño y diagramación: black-book.cl

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

El uso de internet es cada día más indispensable y la pandemia ha subrayado muchos de sus beneficios en nuestra vida cotidiana. Hoy, por ejemplo, ya no tenemos la necesidad de ir realizar trámites en bancos o servicios públicos, lo que nos permite administrar mejor nuestro tiempo. En Chile, desde 2013, más de 5 millones de personas se han sumado al uso de Internet, atraídos por estas y otras bondades de la transformación digital.

Pero el uso de internet tiene riesgos inherentes y víctimas insospechadas. La mayor parte del tiempo hablamos sobre las amenazas a los activos informáticos, comerciales o bancarios, pero también existen riesgos en ámbitos cuyo valor trasciende lo económico. Las plataformas informativas, educativas o de ocio, pueden ser blanco de atacantes para llegar a los usuarios más vulnerables del internet, como lo son las niñas, niños y adultos mayores.

En los menores, el ciberbullying y el grooming representan los mayores peligros. En esta edición de Cibersucesos abordaremos estas formas de acoso y violencia, entregando recomendaciones y compartiremos algunos esfuerzos que como CSIRT estamos realizando para educar y guiar a las familias para enfrentar unidos estas amenazas.

En el caso de los adultos mayores, la transformación digital representa un desafío que los pone a prueba por el desconocimiento y natural desconfianza al momento de usar nuevas tecnologías, lo que conspira para que los cibercriminales vean en ellos a blancos predilectos a la hora de realizar sus ataques. En esta edición también hablamos de la necesidad de acompañar con educación y apoyo a una generación con menos competencias en el uso de las tecnologías de la información.

También mostraremos el avance del Proyecto de Ley de Delitos Informáticos, enviado al Congreso en octubre de 2018, y cómo podrá esta legislación ayudar a crear un ciberespacio más seguro, especialmente para los grupos más vulnerables.

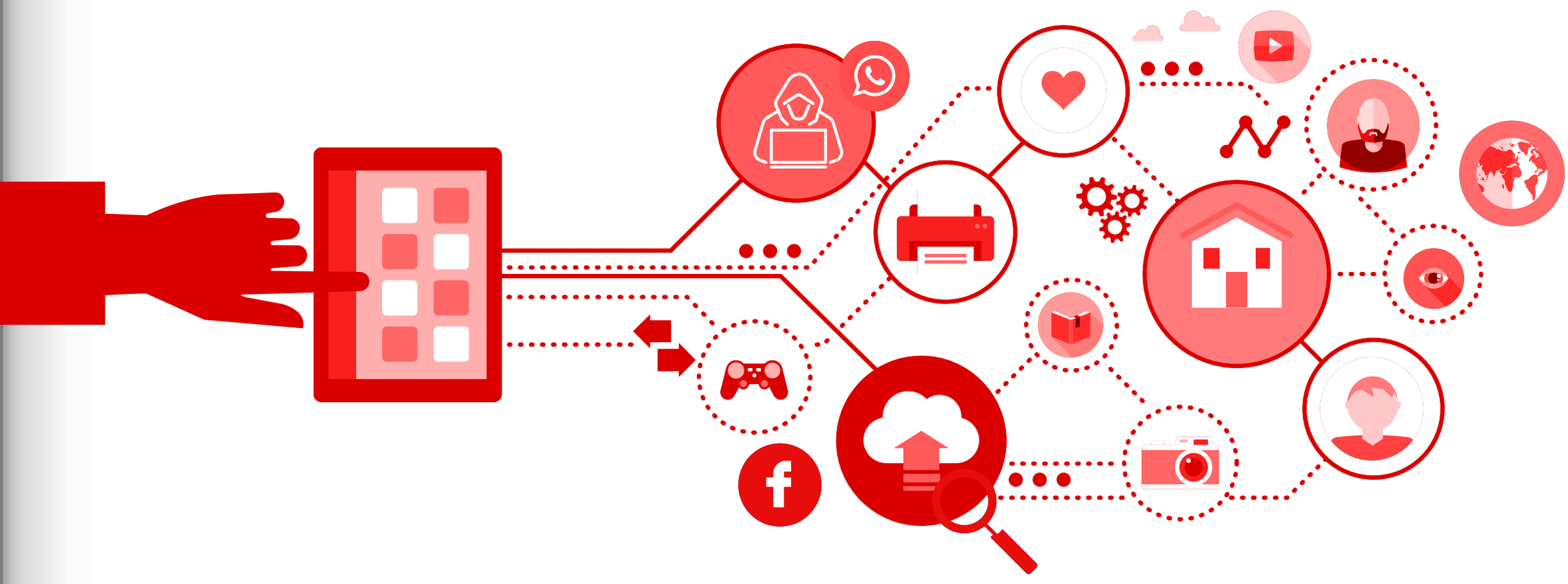
La privacidad de la información será también parte de esta edición, en un reportaje sobre el uso de una infraestructura digital conocida como cookie, la que facilitan la navegación en la web, pero que puede llegar a almacenar muchos de nuestros datos y sin consentimiento.

Y para cerrar esta edición, invitamos a participar de la tercera edición del OEA Cyberwomen Challenge Chile, un desafío para mujeres hackers que se realiza en toda América Latina y que por tercera vez también será realizado en Chile. Para ello, hemos preparado un artículo que narra los testimonios en esta competencia de tres mujeres de destacada participación en versiones anteriores y que hoy forman parte del CSIRT.

CIBERBULLYING Y GROOMING

Los niños ante los riesgos invisibles.

El bullying y los delitos de explotación sexual en niños y adolescentes también son un riesgo en el mundo digital. Los abusadores han buscado nuevas maneras de llegar a sus víctimas, como por ejemplo mediante las redes sociales u otras plataformas con acceso a Internet. Conocer estas amenazas permite estar preparados y evitar ser blanco de estos delitos.



"En su mayoría, las agresiones eran por mi físico, los comentarios eran ofensivos, incluso me llegaron a decir que me harían un juicio, es decir, que me dirían todas las cosas feas que tenía. Yo estaba en 4to básico cuando comenzaron a hacerme bullying. Era tanto el acoso que para evitar a mis compañeros, iba durante los recreos a la biblioteca y dejé de hacer educación física. Lo peor era cuando le decía a mi mamá, la situación empeoraba. Sentía que no había solución, solo quería desaparecer. El gran problema del bullying para mí fue sentirme vulnerable, sin confianza y desprotegida. Sentirse así, te destruye". Estas son las palabras de Valeria, quien hoy tiene 38 años, pero recuerda cada momento de su etapa escolar como la peor, a causa del acoso que sufrió por parte de sus compañeros. En la actualidad, testimonios como el de Valeria continúan repitiéndose en los establecimientos educaciones, pero aún peor, ya que en ocasiones este hostigamiento se extiende en el mundo digital, por lo que la víctima no sólo se siente vulnerable en clases sino también está expuesta en cualquier lugar, incluso en la seguridad de su propio hogar.

Durante el 2019, hubo un incremento de un 7,1% respecto al año anterior, de denuncias por ciberbullying, de acuerdo a cifras entregadas por la Superintendencia de Educación en junio de este año. Estos datos reflejan la importancia de enseñar y educar sobre los riesgos que existen en el mundo digital, considerando que actualmente el principal canal de comunicación y de entretención son las plataformas digitales, y que la vida digital durante los últimos años y, sobretodo en los últimos meses, ha cobrado gran importancia especialmente para los jóvenes.

Los canales por los que las personas acosan a sus víctimas son mediante el correo electrónico, mensajes de texto o las redes sociales. En este último caso, existe una tendencia conocida como "confesiones", perfiles creados especialmente para que cualquier persona pueda enviar mensajes de forma anónima, los que pueden ser desde una declaración de amor hasta mensajes violentos.

Y así como el ciberbullying es un peligro latente en el mundo digital, también existe otro tipo de amenaza como el grooming, un delito en el que un adulto se hace pasar por un menor para engañar a jóvenes o niños y ganar su confianza, crear lazos emocionales y poder abusar de ellos sexualmente u obtener contenido pornográfico.

> Aproximadamente, en el año 2002 se comenzó a usar el término ciberbullying y se refiere a cuando un niño o niña es acosado, humillado, avergonzado o abusado constantemente por sus propios pares, mediante alguna plataforma o dispositivo digital. El problema del ciberacoso es la velocidad y alcance con el que llegan las publicaciones.

Sólo en el 2019, la PDI realizó más de 4.000 investigaciones por delitos asociados a la explotación sexual de menores a través de internet. Las redes sociales y los juegos online son algunas de las vías por las que los delincuentes cometen estos actos, por eso es fundamental que los menores tengan conciencia de los peligros y que no entreguen información personal a desconocidos.

Según el estudio Radiografía Digital 2019, realizado por VTR, a niños entre 10 y 13 años, un 54% de ellos ha jugado en línea con desconocidos. Y si bien, una de las atracciones de este tipo de entretención es jugar con personas de distintas partes del mundo, es necesario que los padres estén en conocimiento de los juegos que utilizan sus hijos, los riesgos y los preparen para evitar ser víctimas de acoso sexual.

Para lograr su objetivo, el abusador busca ganarse la confianza del menor poco a poco, puede ser por ejemplo con regalos a través de los juegos en línea y/o escuchando sus problemas. Además, intenta aislar a su víctima de su red de apoyo para dejarlo desprotegido y mantener todo en secreto. A medida que va ganando su confianza, comienza a tener conversaciones sexuales de forma paulatina.

En ocasiones, puede llegar a utilizar la información que le entregó el menor para manipular su comportamiento y así lograr su cometido.

El rol de los padres, fundamental en la prevención de estos delitos:

Para disminuir los riesgos en los niños, niñas y jóvenes es importante que los padres les enseñen a sus hijos reglas de convivencia básica en internet y a poner los límites para que puedan navegar de forma segura. La educación digital debe comenzar desde pequeños, especialmente si tienen acceso a internet, aplicaciones o las distintas plataformas.

Algunas recomendaciones que te pueden ayudar en este camino son:

- Asegúrate que el perfil de tu hijo(a) en redes sociales sea privado.
- Explícale a los menores que no se entrega información personal a desconocidos.
- En caso de que tu hijo(a) sea víctima de ciber-bullying o grooming es importante realizar la denuncia correspondiente.

cuentos **PARA EDUCAR**

La seguridad cibernética es una de las mayores preocupaciones del CSIRT por eso queremos acompañar a los padres en este camino de concientización. Para ayudarte, el CSIRT desarrolló dos cuentos para niños desde los 5 hasta los 12 años, los que buscan mostrar de una forma amigable los peligros que puede haber en el uso de las tecno-logías a través de internet.

Te invitamos a descargar y leerle estos cuentos a tus hijos, sobrinos o nietos en:

https://www.csirt.gob.cl/recomendaciones/4kids-01-2020/

TERCERA EDAD EN LA ERA DIGITAL

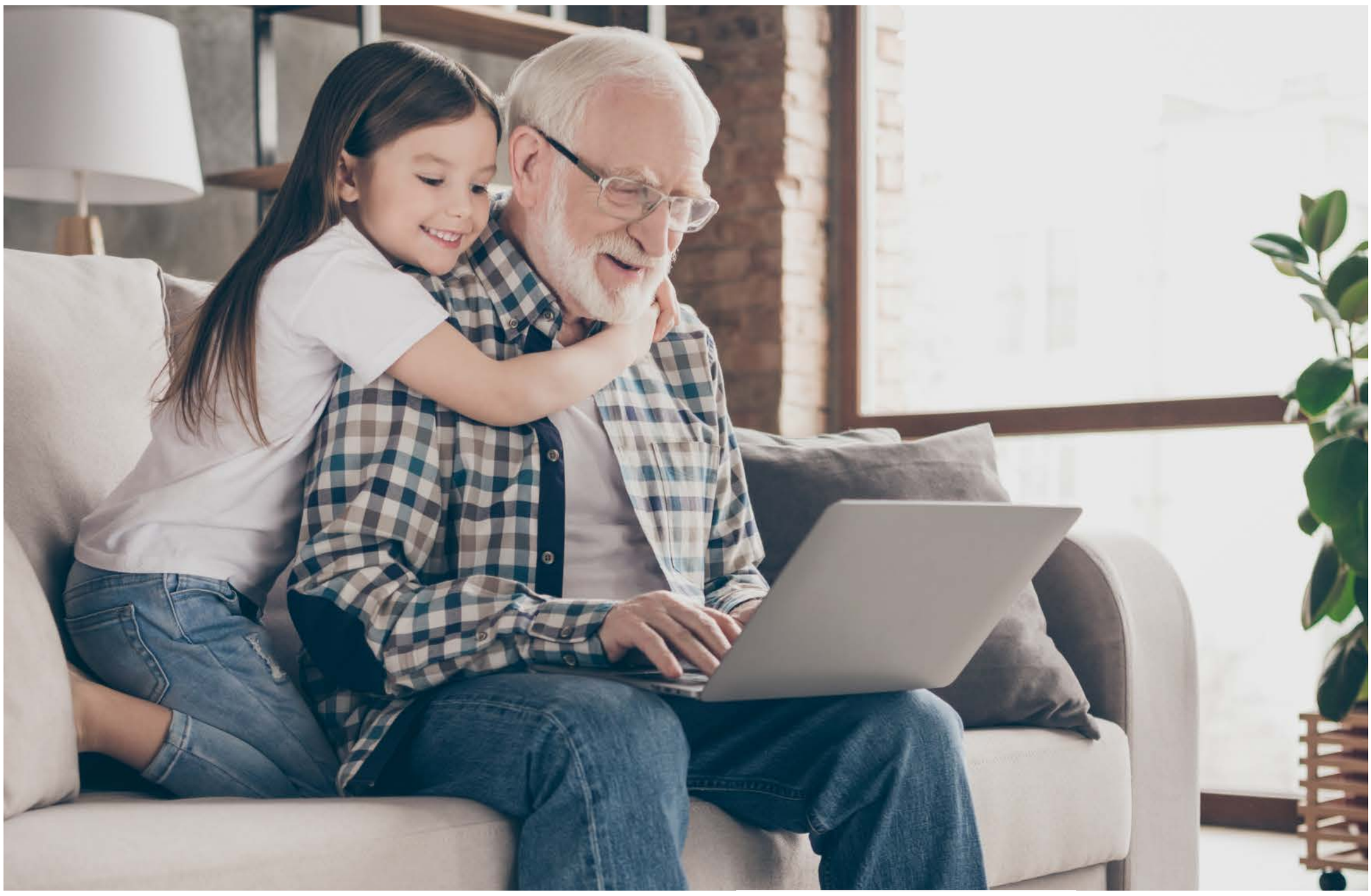
Inclusión tecnológica segura

Sólo un 38% de los adultos mayores entre 75 y 79 años han usado internet para operaciones de banca electrónica, una cifra bastante baja si consideramos que actualmente la mayor parte de nuestras vidas se está desarrollando a través de internet. La tercera edad ha debido adaptarse a los nuevos cambios, pero para algunos tal vez no ha sido muy fácil.

En los últimos meses, y a raíz de la pandemia, la digitalización se ha intensificado en nuestras vidas. Todos tenemos una evaluación de este proceso, y en ese balance, a los innegables beneficios que proporcionan las tecnologías de la información y comunicación, se oponen los riesgos que van aparejados al cambio, los que tenemos que enfrentar con aprendizaje. Para la gran mayoría, este cambio se puede solucionar con la profundización de conocimientos en el uso de tecnologías con las que están familiarizados. Pero para las generaciones mayores que crecieron acostumbradas al uso de sistemas analógicos, el salto a la digitalización implica superar una serie de barreras de lenguaje y pensamiento.

A la natural incomodidad con el uso de dispositivos y aplicaciones, se suma el temor a revelar la condición de analfabetismo digital y no ser vistos como carga para el resto, lo que muchas veces conspira para que el distanciamiento social se transforme en aislamiento social, y con ello, liquidar su sentido de futuro. Las condiciones excepcionales de esta pandemia, han precipitado a esta generación a dos alternativas posibles: la resignación o la reinvención.

Las sociedades se deben esforzar en impedir que ocurra lo primero, y fomentar que todos puedan ser parte de la era digital. Y más importante aún, desmitificar que la edad es una barrera de entrada o una condición que los predispone a ser menos confia-



bles para otros usuarios. Es fundamental crear motivaciones y competencias, para que tomen conciencia de que la tecnología, a pesar de la edad, puede ser una herramienta muy útil para satisfacer sus necesidades cotidianas. Un elemento central en esa educación es la sensación de seguridad al momento de utilizar plataformas y dispositivos electrónicos, lo que contiene sus impulsos, al principio, pero luego sirve como catalizador del cambio.

CURIOSIDADES

La sociedad chilena, en comparación al contexto latinoamericano, se debe concentrar aún más en abordar este problema con una solución de largo plazo. La razón tiene que ver con la longevidad promedio del país, la que sitúa a nuestro país en un estado de envejecimiento moderado a avanzado. Chile es un país que se precipita irremediablemente al envejecimiento de su población y a la obsolescencia de sus políticas, lo que demanda actuar en el corto plazo en medidas que permitan integrar a una población que, teniendo un poder adquisitivo y necesidades, se ha visto inmovilizada de participar en la economía y la sociedad producto de la pandemia, y de su falta de competencias digitales.

¿Cómo ayudarlos?

Si bien, gracias a la tecnología es posible acceder a una gran cantidad de servicios, lo mejor es comenzar por algo sencillo y fácil de manejar.

1.- Si el adulto mayor tiene una aplicación o un sitio web favorito, no te apures por adoptar otras plataformas. Ayúdalo a navegar mejor por las soluciones que lo hacen sentir más cómodo.

2.- Para hacer más llevadero el confinamiento social, enséñale a usar las aplicaciones para comunicarse en línea, así se sentirán más cerca de sus familiares y amigos.

3.- Enséñales a involucrase en el e-commerce. Ahora que la pandemia hizo que sea más difícil comprar en persona, explícales cómo comprar en línea para satisfacer sus necesidades diarias y reducir la exposición.

4.- En ocasiones, la falta de visión puede ser un factor que complique a la tercera edad para manejar un Smartphone. Ayúdalos aumentando el tamaño de texto o subiendo el brillo de la pantalla en las aplicaciones o en el computador.

5.- Guíalos para crear contraseñas seguras y cómo almacenarlas para que las puedan recordar, tomando las precauciones de seguridad.

6.- Ayúdalos a configurar la privacidad en sus redes sociales. Es muy importante que les expliquen los riesgos de la exposición de información, pues sólo de esa forma es posible garantizar el acceso seguro.

7.- Concientízalos sobre los riesgos que existen. Es importante enseñarles para que no sean víctimas de alguna estafa en línea, pídeles a tus mayores que no hagan clic en nada, sin importar lo que les prometan.

8.- Explícales el concepto de “Fake News” y que ignoren los mensajes alarmistas, ofertas de cualquier vacuna, cura o tratamiento contra el COVID-19. Los avances médicos no circularán a través de correos electrónicos o anuncios en línea. Comparte con ellos link de páginas oficiales en donde pueden informarse de manera confiable.

9.- Es importante que los usuarios de más edad tengan fuentes confiables a quienes puedan recurrir: hijos, nietos o sobrinos. Se empático, dales confianza y muéstrate abierto y paciente para escuchar sus inquietudes y guiarlos.

programa Adulto Digital

A principios de este año, el Gobierno impulsó este programa, que apuntaba a la inclusión de aprendizajes de las nuevas tecnologías en los adultos mayores a través de clases de alfabetización digital, capacitando en el uso de teléfonos inteligentes que les permitieran desarrollar habilidades para, entre otras cosas, realizar trámites en línea. Iniciativas como éstas permiten ser el punto de partida para la inserción de los adultos mayores en la era digital y están directamente asociadas al objetivo planteado por el ejecutivo, a través del Instructivo de Transformación Digital, cuyo fin es erradicar los trámites innecesarios en papel dentro de los servicios públicos, al menos en un 80% para 2021, y en un 100% para 2023.

COOPERACIÓN
internacional

La igualdad de género en ciberseguridad, también pendiente en Latinoamérica y el Caribe

La ciberseguridad está de moda. Antes de la irrupción del COVID-19 ya era una de las industrias con mayor crecimiento a nivel mundial. Desde el advenimiento de la pandemia y la traslación de muchos ámbitos de nuestra vida diaria al mundo online, su papel se ha redoblado hasta convertirse en esencial. Ese renovado protagonismo ha dejado también al descubierto una evidencia: en la ciberseguridad tampoco existe la igualdad de género. En particular, en Latinoamérica y el Caribe persisten dos principales problemas que debemos destacar: el aumento de la violencia de género en línea y la existencia de barreras para el ingreso de las mujeres al sector.

El acceso a internet por parte de las mujeres del mundo y de Latinoamérica tiene diferentes aristas que afectan su relación con el universo online. Para empezar, muchas mujeres en la región carecen de una adecuada alfabetización digital, descrita como las habilidades técnicas y la capacidad de interactuar críticamente con contenido en línea, de acuerdo a un estudio publicado por la organización GSMA. Esto las hace inconscientes de los riesgos de usar internet relacionados con acoso, fraude digital y robo de datos, entre otros.

Prueba de ello, es que la Comisión Interamericana de Mujeres (CIM) de la Organización de los Estados Americanos (OEA), a través de su publicación "COVID-19 en la vida de las mujeres" ha reportado que desde el inicio de las medidas de distanciamiento físico por COVID-19, en Latinoamérica se ha registrado un aumento en los ataques en línea hacia niñas y mujeres, debido a la generación de nuevas formas de exposición de las víctimas en internet.

Alison August Treppel

Secretaria Ejecutiva Comité Interamericano contra el Terrorismo (CICTE) de la OEA

Alison August se ha desempeñado en este cargo desde agosto de 2016, donde es responsable de promover la agenda antiterrorista de la OEA en América Latina y el Caribe. Además, gestiona las operaciones diarias de la Secretaría de la CICTE, dirige los esfuerzos de asistencia técnica de la OEA en esferas como la ciberseguridad, la gestión de los controles fronterizos, la prevención de la financiación del terrorismo y la proliferación de armas de destrucción masiva, entre otros.

Erradicar la violencia contra la mujer en todas sus formas y manifestaciones es un objetivo común y esencial en toda la OEA. Para lograrlo lo antes posible es indudable que todos los esfuerzos son necesarios. Tomando estas consideraciones, el programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) ha hecho un llamado constante a los representantes del gobierno y la sociedad en general sobre las situaciones de violencia contra las mujeres que se desarrollan a través de medios electrónicos, mediante diferentes iniciativas. En particular, se han analizado los métodos más comunes en casos de violencia de género por vías electrónicas y se ha promovido el diálogo entre países de América Latina y el Caribe para generar soluciones y recomendaciones. Estas acciones están contenidas en el white paper "Combatir la violencia en línea contra las mujeres: Un llamado a la protección", publicado en 2019.

El otro aspecto en el que se manifiesta la inequidad de género en ciberseguridad es en la escasa ocupación de puestos de trabajo de la industria por parte de mujeres. De acuerdo al reporte “Mujeres en ciberseguridad”, desarrollado por (ISC), en 2017, las mujeres ocupaban únicamente 11% de los puestos de trabajo en esta industria; en 2019, sin embargo, ya ocupaban el 24% de acuerdo al mismo artículo. A pesar de ser un crecimiento importante, la brecha aún está presente. Particularmente en Latinoamérica, diversos factores afectan y contribuyen a esta realidad, en especial la existencia de barreras sociales y culturales que existen en una industria predominantemente masculina, de acuerdo a la versión más reciente del reporte de (ISC).

Muchos gobiernos, empresas y profesionales han hecho importantes esfuerzos en los últimos años para generar mayores oportunidades de desarrollo, capacitación y espacios de liderazgo para las mujeres. Gracias a estas iniciativas, cada día más mujeres están uniéndose a este campo laboral y están ocupando posiciones de liderazgo para generar cambios en la industria y hacer un ciberespacio más seguro y con mayor respeto a los derechos humanos. Por otra parte, de acuerdo a un estudio de Fortinet publicado en 2019, el reclutamiento e inclusión de más mujeres en ciberseguridad no sólo llenará brechas de habilidades existentes, sino que simultáneamente generará y mejorará el rendimiento en las organizaciones.

En la OEA llevamos años impulsando iniciativas relacionadas con la capacitación e inserción de más mujeres en ciberseguridad. Una de las más importantes es el CyberWomen Challenge. Coordinado junto a TrendMicro, se trata de una serie de ejercicios para aspirantes a trabajar en ciberseguridad, basados en escenarios de la vida real, que busca fomentar la participación de más mujeres en esta área. Desde 2018, se han realizado más de 20 ejercicios cibernéticos en la región, en los que han participado más de 1.400 mujeres de 12 Estados miembros diferentes, incluyendo Chile. Esta actividad promueve el desarrollo y el fortalecimiento de habilidades y conocimientos técnicos, y aboga por un mercado laboral de seguridad cibernética más diverso. El CyberWomen Challenge, además, nos ha permitido constatar el impacto tan positivo del trabajo conjunto de muchas de nuestras sociedades para mejorar la situación de las mujeres en ciberseguridad. En este sentido, consideramos los siguientes tres puntos como algunos de los mayores aprendizajes que hemos obtenido a lo largo del desarrollo de actividades en estos frentes:

1.- La organización de actividades e iniciativas para mujeres en ciberseguridad deben tener un enfoque fundamental en cerrar la brecha de género.
Es decir, asegurarse que las actividades no sólo creen consciencia del poder de la tecnología y el papel que pueden tener dentro de la industria, sino que también alienten a las participantes a unirse a ella. Considerando el aumento de las oportunidades laborales en ciberseguridad, debemos asegurarnos de que esos trabajos estén llenos de mujeres que puedan contribuir positivamente a la industria, así como la existencia de medidas y recursos gubernamentales para que las mujeres puedan denunciar y solventar problemáticas de acoso en línea.

2.- Crear una cultura de inclusión, diversidad y colaboración para crear una mejor fuerza laboral de ciberseguridad. Esto comienza con la promoción de estos mensajes en todos los niveles de nuestras organizaciones y con un cambio de conciencia que es necesario en todos nuestros espacios.

3.- Las alianzas público-privadas, con insumos de la sociedad civil, funcionan. Este tipo de colaboraciones ha sido fundamental para nuestro trabajo, y esperamos que continúen allanando el camino para mejorar la industria de la ciberseguridad y hacerla más inclusiva.

La violencia de género en línea y la existencia de barreras para el ingreso de las mujeres a la industria de ciberseguridad no son los únicos problemas que afectan a la ciberseguridad, pero sí son problemas que no pueden esperar. Las personas afectadas por una brecha así tienen menos acceso a sus derechos sociales, culturales, económicos y políticos, tienen menos oportunidades y reciben menos servicios que las demás. No lo debemos aceptar, no lo podemos permitir.

Tendencia Digital

COOKIES

las huellas que vas dejando en internet

Cada vez que ingresas a un sitio web, tus movimientos, preferencias e incluso las compras quedan registrados por las empresas para conocer tus gustos y, en base a eso, ofrecer publicidad de acuerdo tus necesidades. Esta información es obtenida de distintas formas, una de ellas es a través de las cookies.
El CSIRT investigó más sobre este tema y cómo se compartan.

Entraste a la página web de una tienda comercial, porque estabas pensando comprar, por ejemplo, unas zapatillas. Cuando terminas de revisar el sitio, sales, ahí termina tu búsqueda. Pero después, al entrar a una de tus redes sociales mágicamente aparece publicidad de lo que estabas buscando. Esta misma situación ocurre con otros sitios como bancos, servicios de transportes, entidades educacionales, entre otros. ¿Qué pasó, cómo supieron las redes sociales u otro canal digital lo que buscabas? Todo lo que haces en internet va dejando huellas, las que son obtenidas por las cookies. Al ingresar a un sitio web, las cookies almacenan la actividad que realizaste en el navegador. Con esto, ese sitio web puede consultar la información recopilada previamente del navegador. Esto quiere decir que las cookies permiten que cuando regresas a esa página, sea posible recordar la contraseña de tu correo electrónico, guardar los artículos en tu carrito de compras como invitado o también te puede aparecer publicidad de la tienda comercial que visitaste.

Estas famosas cookies **tienen distintos fines**

- **Recopilar** información sobre las páginas visitadas, así como actividades realizadas en el sitio.
- **Permitir** que el sitio reconozca al usuario.
- **Personalizar** la experiencia de la navegación.
- **Entregar** anuncios dirigidos.

Reconoce **LAS COOKIES**

En Chile, no existe una legislación para la utilización de las cookies, pero sí cuenta con la Ley Nº 19.628 sobre Protección de la Vida Privada, que regula el tratamiento de datos personales. Y si bien las cookies permiten mejorar la experiencia del usuario, son comúnmente utilizadas con fines comerciales. Para que puedas entender cómo funcionan, te explicamos las características de cada una

- **Cookies propias:** Buscan mejorar la experiencia del usuario al entrar en la página y facilitar el funcionamiento correcto del sitio. Son creadas en el navegador desde el dominio del sitio web que se visitó.
- **Cookies de terceros:** Pueden monitorear la frecuencia de las visitas de los usuarios en un sitio, analizando su comportamiento y, de esa manera, entregar anuncios publicitarios adaptados a tus intereses.
- **Cookies de persistencia:** Tienen la particularidad de almacenarse desde minutos hasta años, pudiendo ser accedidas y tratadas por el responsable de la cookie, incluso cuando se finaliza una sesión en la web o al cerrar el navegador.
- **Cookies de sesión:** Tiene una breve existencia, pues se borran al momento de cerrar el navegador. Son creadas para recabar y almacenar información mientras el usuario está en el sitio web. Al cerrar o reiniciar el navegador se eliminan de forma inmediata. Por lo tanto, cuando la persona vuelve a visitar un sitio, la web no lo reconoce, obligando al usuario a crear nuevamente una sesión -si fuera el caso-, o volver a seleccionar preferencias y temas nuevamente.

Análisis **CSIRT**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, analizó las cookies de terceros en Chile. La investigación recopiló información en dos momentos muy diferentes de este año, sobre un universo de 167 sitios y que abarcó a cinco grandes áreas de la economía: educación, comercio, construcción, transporte y bancos. La primera muestra se tomó en enero de 2020, cuando aún se sentían impactos del estallido social y luego se repitió el ejercicio en julio, a casi cinco meses del inicio de la pandemia. En estos contextos tan diferentes se pudieron ver diferentes situaciones con respecto a la cantidad de cookie y sus atributos..

El resultado más destacado fue el notorio aumento de cookies en general, que subieron desde 6.054 a 7.225, un 20% de alza, algo que los autores pronosticaban, ya que podría ocurrir debido a la mayor exposición de los usuarios a internet.

Otro factor que cambió notoriamente con respecto a la primera muestra, fue la cantidad de cookies con atributos de seguridad, las que subieron de un 50% a un 70% del total. Esto puede ser tomado como un signo positivo, pero también habla de la mayor precaución de las empresas que recolectan esta información, ya que se encuentran utilizando parámetros de seguridad para que las cookie no puedan ser interceptadas cuando es enviada a sus servidores.

Otro de los elementos destacables fue encontrar cookies que se repetían en varios sitios. Dos cookies de terceros analizadas se repetían en el 75% y 70% de las web visitadas, y estaban presentes en todas las áreas y rubros de la economía seleccionados.

Estas cifras nos demuestran la cantidad de información que recopilan las empresas a partir de la navegación de los usuarios, y la escasa protección de la privacidad a la que están expuestos, quienes a diferencia de Europa, por ejemplo, no tienen disponibles opciones de configuración de cookies para recibir información sobre su utilidad y rechazar su uso, si es que lo desean. Ante todo, los resultados aquí revelados son consecuencia principal de la falta de legislación y el poco conocimiento del tema a nivel de los usuarios.

Esta investigación dispone de diferentes tablas en la que se detalla el número de cookies, las que son propias, de terceros, de persistencia, la fecha de expiración promedio, el promedio de años que permanecen y cuantas de estas cookies son de sesión.

Si quieres conocer el informe en detalle, puedes ingresar al siguiente enlace

https://www.csirt.gob.cl/reportes/an2-2020-11/

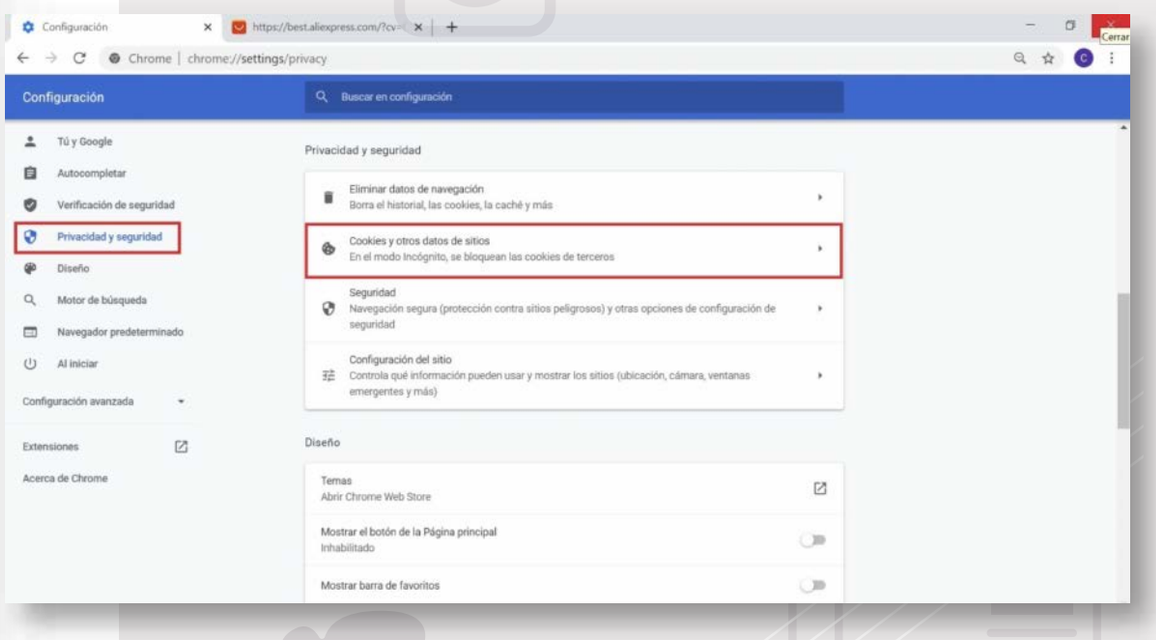
Cómo administrar **COOKIES EN TU NAVEGADOR**

1.–

En google Chrome debes ir a “Configuración”

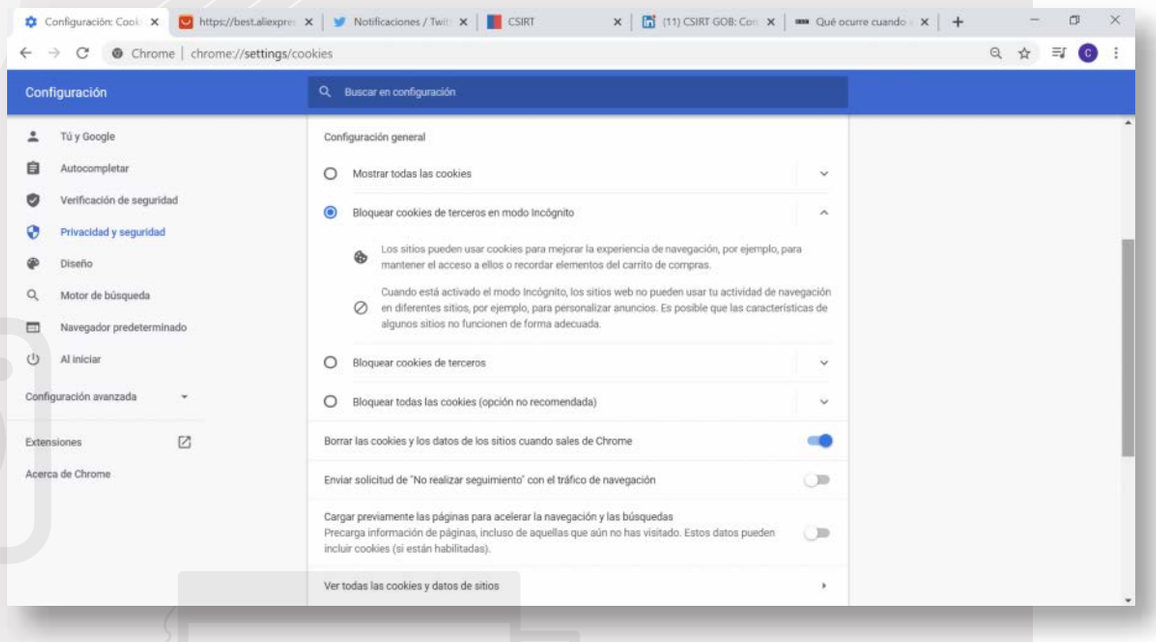
2.–

Luego, dirígete a “mostrar opciones avanzadas” > “Privacidad y seguridad” > Cookies y otros datos de sitios



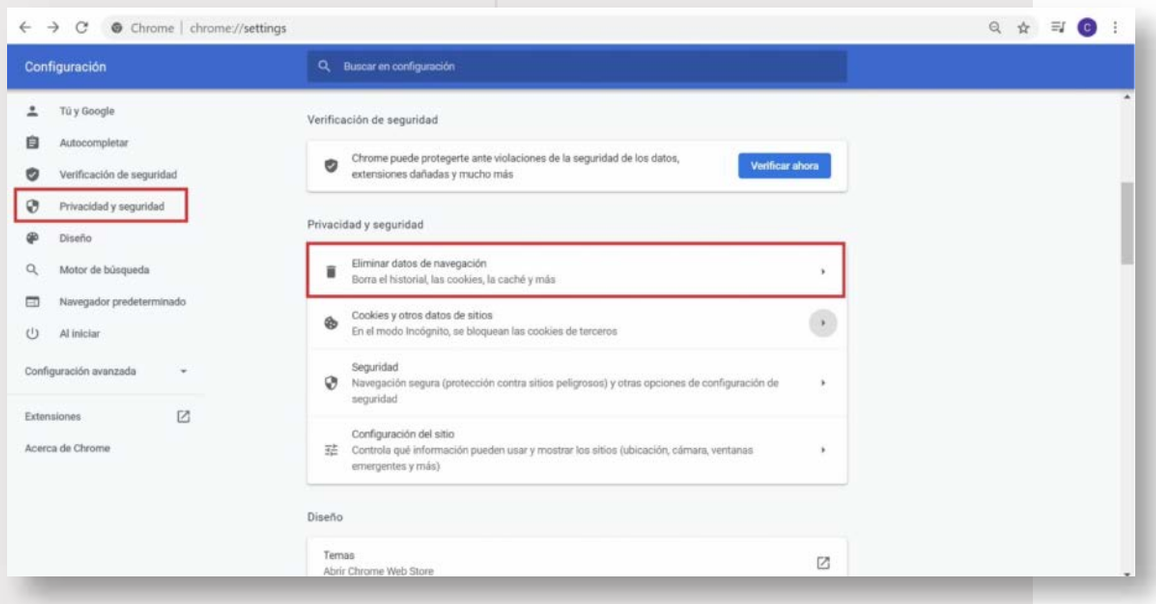
3.–

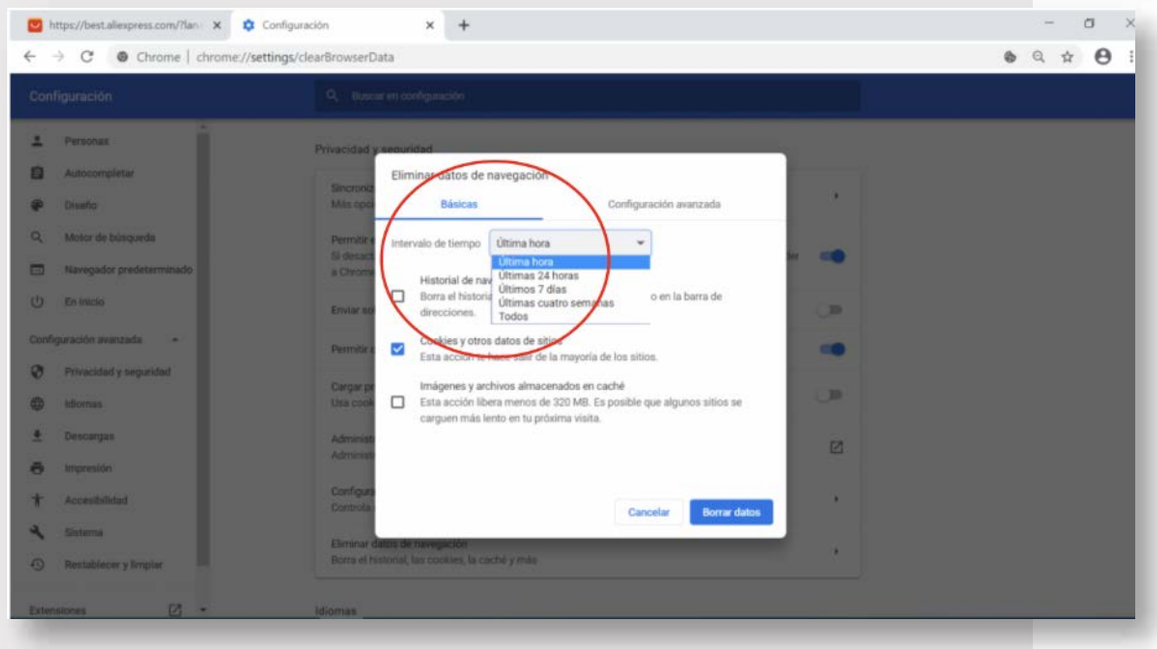
Una vez seleccionada esa opción, llegarás a “Configuración general”. Aquí puedes elegir la alternativa que más te acomode y prefieras. Por ejemplo, es posible bloquear todas las cookies o seleccionar los tipos de cookies que quieres que se activen al momento de navegar.



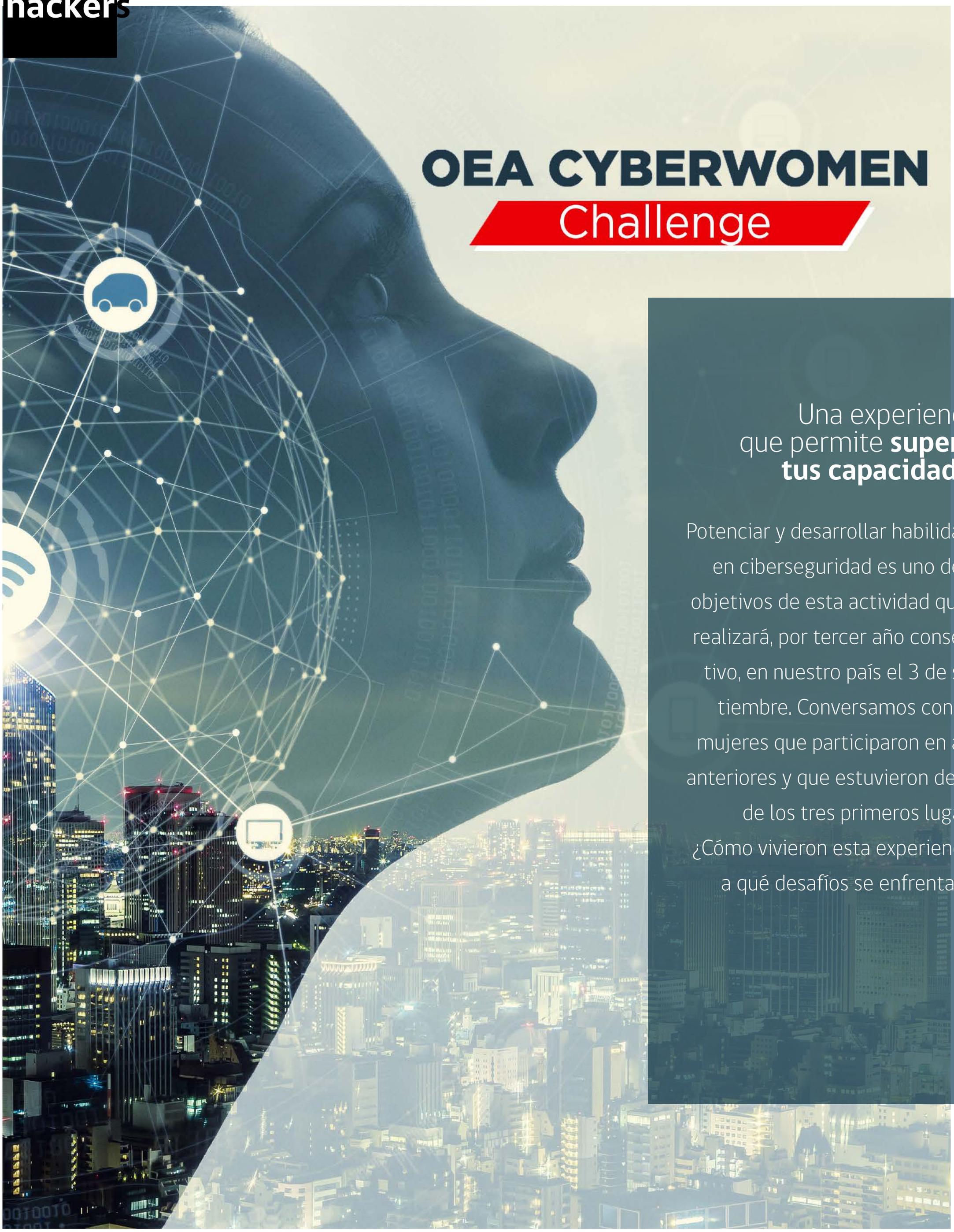
4.–

Otra altermativa de eliminar las cookies es a través de la opción “Eliminar datos de navegación”.





*Las fotos corresponden a la versión 84.0.4147.105 de Google Chrome.



Una experiencia que permite **superar tus capacidades**

Potenciar y desarrollar habilidades en ciberseguridad es uno de los objetivos de esta actividad que se realizará, por tercer año consecutivo, en nuestro país el 3 de septiembre. Conversamos con tres mujeres que participaron en años anteriores y que estuvieron dentro de los tres primeros lugares. ¿Cómo vivieron esta experiencia y a qué desafíos se enfrentaron?

"Cuando supe que existía una actividad sobre ciberseguridad dirigida sólo para mujeres me llamó mucho la atención, ya que era la primera vez que hablaban de un evento de este tipo. Nunca había participado de una competencia CTF (Capture The Flag), pero quise intentarlo. Cuando llegué al evento no conocía a nadie, así que formamos un equipo con las chicas que designaba la organización", recuerda Natalia Pérez, una de las participantes del OEA Cyberwomen Challenge en su primera edición el año 2018 y en el 2019.

Este evento consiste en una competencia de hacking entre equipos conformados solo por mujeres, quienes deben resolver 35 desafíos de ataque y defensa en un simulador lúdico. "La primera parte de la competencia fue ofensiva y luego tuvimos que defender, revisando logs, buscando credenciales, entre otras cosas. Si bien es agotador estar ocho horas, el trabajar en equipo es una experiencia increíble. Gracias a estos desafíos es posible conocer de forma tangible el nivel de tus conocimientos.

El Cyberwomen me dio la oportunidad de aprender, pasarlo bien y dar lo mejor de mí. Sin duda que la experiencia que viví fue muy buena", cuenta Natalia.

Natalia Perez

Natalia estudió Ingeniería Civil Electrónica en la Universidad de Concepción y trabaja en el área de ciberseguridad desde el año 2014. Si bien era un área poco conocida para ella en ese momento, poco a poco se ha ido capacitando y perfeccionando en este rubro. Tanto así, que además de participar en dos versiones del Cyberwomen y obtener el tercer lugar, es parte del Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT) y miembro de la primera comunidad de ciberseguridad de mujeres en Chile: Hackada.

Este evento ha tenido una muy buena recepción. En sus dos versiones ya han participado más de 200 mujeres de distintas edades y carreras.

Gabriela Sepúlveda

Un ejemplo de esto es el caso de Gabriela Sepúlveda, estudiante de Ingeniería Civil Informática de 5to año de la Universidad Técnica Federico Santa María.

Gabriela cuenta que cuando la invitaron a participar del Cyberwomen tuvo un poco de temor. "Pensé que no tenía tantos conocimientos, pero una vez que empezamos a resolver los desafíos me di cuenta que me pude desenvolver bastante bien. Además, trabajar con un equipo variado, unas estudiantes y otras profesionales, nos permitió resolver de buena manera los ejercicios, al tener distintas visiones y formas de solucionar cada reto".

En este mismo equipo participó Paula Moraga, estudiante de 4to año de Ingeniería Informática del INACAP. Ninguna de ellas se había enfrentado a una competencia de este tipo y ambas estaban comenzando a introducirse en el mundo de la ciberseguridad, pero su interés, ganas de participar y su contante preocupación por aprender de esta área llevaron a su equipo a obtener el primer lugar del Cyberwomen Challenge del año 2019.

"Los desafíos del Cyberwomen son variados y están bien elaborados. Partes de menos a más. Por ejemplo, comienzas la actividad con retos simples de criptografía, y lo interesante y atractivo es que paralelamente te van enseñando a utilizar algunas herramientas", cuenta Gabriela.

Por su parte, Paula recuerda que "cuando empezó el desafío intentamos definir roles para cada una. Por ejemplo, una investigaba los retos y otra llevaba la documentación de lo que habíamos hecho. A medida que avanzábamos, los desafíos eran más difíciles. Nuestro equipo nunca tuvo la delantera, es más, estuvimos entrampadas como dos horas, pero en los últimos cinco minutos logramos avanzar muy rápido y sacamos la última respuesta para ganar. Fue súper emocionante".

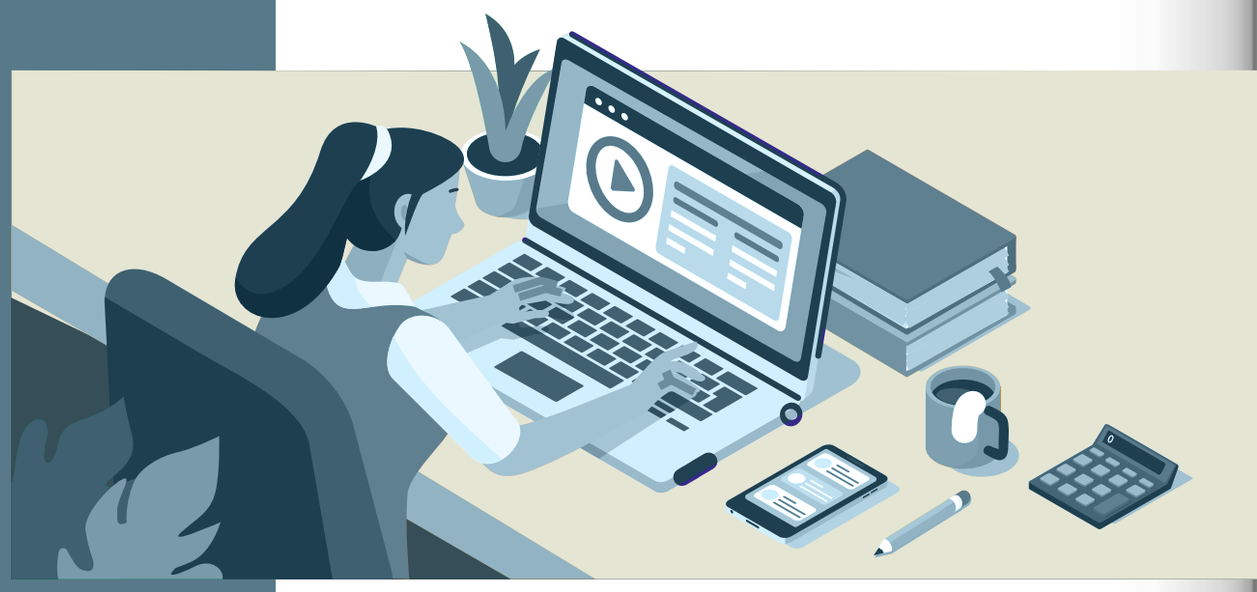
CYBER

Paula
Moraga

A Paula le encanta todo lo relacionado con la tecnología, programación y videojuegos, por eso cuando el director de carrera de su universidad la invitó a participar de este evento no dudó ni un segundo. "Cuando me preguntaron, pensé que tenía que participar, porque era la mejor oportunidad para aprender sobre seguridad, complementar mis estudios y aplicarla en mi carrera. Sentía que este evento, además de ser una competencia, sería el lugar ideal para aprender y así fue. Además, ver tantas mujeres que al igual que yo les interesa la tecnología es increíble, no me lo esperaba. Estoy muy feliz de haber participado en el Cyberwomen, porque se me abrieron las puertas para trabajar en el CSIRT y empezar a profesionalizarme", afirma Paula.

La misma alegría comparte Gabriela. "Me gustó mucho participar, fue una instancia muy fructífera y lo mejor de todo es que te ayuda a superar tus miedos y vencer ese sentimiento de creer que no se está preparado. Mi expectativa era participar y vivir la experiencia, y obtuve mucho más, ya que al ganar la competencia me propusieron trabajar en el CSIRT".

Además de compartir la experiencia de participar en el OEA Cyberwomen Challenge, Natalia, Gabriela y Paula, fueron una de las pocas mujeres o, en algunos casos, las únicas estudiantes de su generación. Contar con este tremendo equipo en el CSIRT es un orgullo y cada día nos demuestran con su talento las oportunidades de mejora para contar con un ciberespacio con menos riesgos y amenazas.



WOMEN

¡PARTICIPA **TÚ TAMBIÉN!**

La versión Online tiene una duración de 6 horas, una capacidad máxima de 100 participantes y se formarán grupos aleatorios de 3 personas.

Temas

- Containers, pipelines e imágenes
- Creación de containers
- Creación de servicios de containers
- Planeación e integración de la seguridad como código en los ambientes DevOPS

Pre-requisitos:

- Conocimientos en Windows y Linux, redes, seguridad
- Containers
- Conocer las herramientas de DevOps:
- Github
- Jenkins
- ECR (de Amazon)
- Kubernetes
- Docker
- APIs

Todas las asistentes deben tener:

- Conexión a internet estable
- Laptop
- Cliente de Zoom instalado

Premios:

1er lugar: AWS Credits/ Participación en el Cyberwomen Challenge Regional 2020.
2do lugar: Licencias de software de seguridad para proteger 5 dispositivos persona les por un año sin costo.

Si estás interesada en participar, inscríbete en el sitio web

https://women-challenge.interior.gob.cl/

En caso de duda, contáctanos al correo comunicaciones@interior.gob.cl

DELITOS INFORMÁTICOS

Proyecto de ley extiende sus efectos protegiendo a los más vulnerables

Los delitos cometidos a través de internet y del uso de plataformas han incrementado considerablemente el último tiempo y han ido cambiado con los años. El problema es que la ley no se ha ido actualizando tan rápido como evolucionan las formas comisivas de estos delitos, sin embargo, esto pronto cambiará al encontrarse en su segundo trámite constitucional en la cámara de diputados un proyecto de ley con importantes mejoras. Conoce de qué se tratan los futuros cambios.

El proyecto, que comenzó a ser trabajado por el Gobierno desde comienzos de la administración del Presidente Sebastián Piñera, busca actualizar la normativa en materia de Delitos Informáticos, además de dar cumplimiento a obligaciones internacionales, debido a que es insuficiente para responder al fenómeno delictivo informático en auge y que además se ve acrecentado por la crisis sanitaria.

En concreto, el proyecto tipifica en un cuerpo normativo específico los ilícitos penales informáticos, adecuando los actuales a los términos del Convenio de Budapest y agregando otros nuevos; entrega las normas procedimentales para la persecución y juzgamiento de tales delitos; define los conceptos comunes a estos tipos, modifica el Código Procesal Penal y la ley sobre Responsabilidad Penal de las Personas Jurídicas, estableciendo obligaciones y procedimientos para hacer efectiva la dificultosa investigación de estos ilícitos.
De la misma forma, la nueva legislación introducirá nuevos tipos penales como la falsificación y el fraude informático, así como el abuso de dispositivos.

El proyecto contiene tres títulos y artículos transitorios

- En lo sustantivo, el proyecto adecúa los tipos penales actuales a los establecidos en la Convención de Budapest los cuales son: ataque a la integridad de un sistema informático, interceptación ilícita, ataque a la integridad de los datos informáticos, acceso ilícito al sistema informático, falsificación informática, fraude informático y abuso de dispositivos.

- Se contempla una atenuante especial de cooperación eficaz que conduzca al esclarecimiento de los hechos o en el impedimento de la perpetración del delito; y agravantes especiales.

- Se otorga al Ministerio del Interior y Seguridad Pública y a los delegados presidenciales regionales y provinciales la legitimación activa para querellarse cuando los delitos interrumpen el normal funcionamiento de un servicio de utilidad pública.

- Se permite el uso de técnicas especiales de investigación, como los agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones; se establece una regla especial de comiso y la preservación o custodia de la evidencia electrónica, según la instrucción del Fiscal Nacional.

- Faculta al Ministerio Público para solicitar provisoriamente la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega.

Legal

Mayor pena para quienes abusen de las vulnerabilidades, confianza o desconocimiento de niños, niñas adolescentes o adultos mayores.

La frecuencia con que los menores acceden a internet exige incrementar las barreras de protección, incluso en delitos especiales.
El robo de credenciales, los accesos no autorizados y los ataques a sistemas informáticos, con el propósito de cometer delitos que puedan interferir en la sexualidad de un menor (indemnidad sexual) por medios telemáticos o del uso de tecnología son, entre otros, fenómenos cada vez más frecuentes para los cuales se requiere una solución específica.
Con estas propuestas de mejora, el Gobierno busca garantizar una mayor seguridad al momento de navegar por internet y utilizar las plataformas digitales, protegiendo a toda la ciudadanía.

UNA DE LAS mejoras más trascendentales está dada en materia de circunstancias modificatorias de la responsabilidad penal, ya que por primera vez se reconoce a los sectores más vulnerable e indefensos.

Esta agravante establece una sanción mayor para quienes cometan un delito informático y se aprovechen de la condición de vulnerabilidad intrínseca en que se encuentran las víctimas, por ejemplo, en el caso de los adultos mayores que sean nativos digitales y cuyas competencias tecnológicas son limitadas.

Esta misma condición aplica para los niños, quienes han estado expuestos al mundo digital desde edades tempranas, pero que en su mayoría no son conscientes de los riesgos y amenazas del ciberespacio. En el caso de los adolescentes, por ejemplo, cuentan con accesos y competencias e incentivos para ser parte del ciberespacio, pero no miden los riesgos asociados a sus decisiones a la hora de navegar, revelando vulnerabilidades que los cibercriminales pueden explotar fácilmente. Este grupo ha demostrado no tener complejos en compartir en detalle diferentes aspectos de su vida en Twitter, Instagram, Facebook o Tik-Tok. A menudo se unen a foros en línea, chatean con extraños, comparten fotos de sí mismos y arriesgan su información personal. Su falta de prolijidad al navegar no sólo los expone ante los criminales, sino que también ponen en riesgo a sus familias y entorno. Una expresión clara de la vulnerabilidad a la que están expuestos los menores en la web fue el juego llamado “La ballena azul”, el cual logró una tremenda popularidad entre menores, quienes siguiendo las reglas del mismo se terminaron quitando la vida.

DELITOS INFORMÁTICOS

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