Octubre/2021 www.csirt.gob.cl

ESPECIAL CIBER SUCESOS

Investigación, Tendencia y Concientización

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Mes de Ciberseguridad

Mes de la Ciberseguridad:
Concientización a nivel mundial

Riesgos cibernéticos a los que se enfrentan los menores de edad

Kit de herramientas para pymes más cibersegura

Personas mayores más digitalizadas

Cooperación Internacional:
CSIRT Americas

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

145 8712 7864
096 4321 5541

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 Connecting and Protecting

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
Ramón Rivera
Hernán Espinoza

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Este octubre que termina es internacionalmente reconocido como Mes de la Ciberseguridad, y por ello se desarrollaron gran número de actividades para promover prácticas seguras del uso de internet entre la población en general, con foco en los grupos más vulnerables. Por eso, nuestro CSIRT de Gobierno propuso a sus pares reunidos en CSIRTAmericas —a su vez, inserta en el marco de la Organización de los Estados Americanos (OEA) — llevar nuestros tradicionales ciberconsejos a toda América, iniciativa que fue positivamente recibida.
Así, durante todo octubre, las recomendaciones de 12 CSIRT del continente fueron plasmadas en publicaciones ilustradas, diseñadas por nuestra institución en Chile y difundidas desde Estados Unidos a nuestro Cono Sur, gracias a la participación de los CSIRT y CERT en EE.UU., República Dominicana, Jamaica, Costa Rica, Panamá, Colombia, Ecuador, Paraguay, Uruguay y, en Argentina, los de Neuquén y Buenos Aires.

Con ese mismo espíritu es que decidimos dedicar esta edición de nuestra revista CiberSucesos para resumir y poner a disposición de la comunidad las recomendaciones más importantes que es necesario conocer al disfrutar del mundo en línea, y específicamente aquellas dirigidas a los niños, niñas y adolescentes, a las pequeñas y medianas empresas (pymes) y a los adultos mayores. De esta forma, en lugar de las secciones habituales de nuestra publicación, compartiremos una guía para cada uno de estos tres segmentos de la población.

Los consejos para niños, niñas y adolescentes (NNA) se centran en describir los siete mayores riesgos que apuntan a ellos en internet —como el grooming, el sexting y los retos virales peligrosos—, y las principales formas en que pueden protegerse. Está elaborado de forma de ser leído por padres y tutores solos o en conjunto con los menores.

La guía para adultos mayores se aboca, por su parte, primero a describir y explicar los principales conceptos del mundo digital, y solo tras ello explica varias formas para que los ancianos estén más seguros en línea. Estos consejos sirven a toda edad, por lo demás, así que no está de más para todos nosotros echarle una mirada y recordar las mejores prácticas al disfrutar de internet.

Finalmente entregamos recomendaciones de ciberseguridad para pequeñas y medianas empresas —pymes—, incluyendo herramientas y controles que mejoran la defensa digital de una organización de forma gratuita y accesible, poniendo la ciberseguridad a disposición de firmas que no pueden pagar grandes soluciones en esta materia.

Mes de la Ciberseguridad

CONCIENTIZACIÓN A NIVEL MUNDIAL

Octubre es un mes en el que muchos países promueven buenas prácticas e impulsan distintas iniciativas enfocadas en la concientización de la ciberseguridad. Este camino comenzó el año 2004 en Estados Unidos y desde entonces se refuerza la importancia de educar sobre el uso de la tecnología, considerando que vivimos cada vez más conectados.

"La seguridad de los datos" considerado como "un mal necesario" eran los conceptos que se utilizaban en los años 80 para hablar de lo que hoy conocemos como ciberseguridad. La evolución de las amenazas cibernéticas ha hecho que la ciberseguridad tome un rol más protagónico en los países, empresas y ciudadanos.

Y la historia lo avala. En 1971 se descubrió "Creeper", el primer virus informático y desde entonces se ha visto cómo han aparecido nuevos tipos de ataques cada vez más sofisticados y peligrosos, afectando a organizaciones reconocidas a nivel mundial como la Nasa, Google, Play Station, Sony, Yahoo, así como a los gobiernos de todo el mundo.
En vista de las amenazas y lo transversal que resultan ser los ataques cibernéticos, es fundamental educar y concientizar para proteger y resguardar la información que está en línea. Por esta razón, el año 2004 el Departamento de Seguridad Nacional de EE.UU. y la Alianza Nacional de Seguridad Cibernética, declararon octubre como el "National Cyber Security Awareness Month (Mes Nacional de la Concienciación en Seguridad Cibernética).

Tiempo después, en el año 2012 se sumó a esta iniciativa Europa creando el "Mes Europeo de la Ciberseguridad". En el caso de Chile, desde 2018 se reconoce octubre el "Mes Nacional de la Ciberseguridad", siendo el primer país latinoamericano en conmemorar esta fecha.

Las iniciativas del Mes de **la Ciberseguridad**

Poco a poco ha ido tomando fuerza la concientización y, si en sus inicios se entregaban consejos sobre cómo actualizar un antivirus, hoy vemos importantes campañas que se despliegan en Estados Unidos, Canadá, Chile y Europa, con un gran alcance, mayor participación y abordando distintos temas que involucran a la ciberseguridad.

Este año, por ejemplo, en Estados Unidos el slogan de la campaña, al igual que en años anteriores, es: "Do your part. Be cyber smart" (Haz tu parte. Sé ciberinteligente). El tema invita a las personas y organizaciones a asumir su rol en la protección del ciberespacio y enfatiza en la responsabilidad que tiene cada uno en toma medidas para mejorar la ciberseguridad.

Por otra parte, en Europa, el slogan de este año fue "ThinkB4UClick" (Piensa antes de hacer clic), en el que abordaron dos temas principales. Uno llamado "Primeros auxilios cibernéticos", en donde se buscó compartir pautas útiles y consejos sobre qué hacer en caso de un ciberataque, y un segundo tema fue "Sea ciberseguro en casa", instancia en el que se entregaron consejos sobre cómo reconocer los riesgos de ciberseguridad y mantenerse seguro en línea.

Mes de la **Ciberseguridad en Chile**

Cada año, nuestro país conmemora de diferentes maneras este mes. Por su parte, el CSIRT de Gobierno elaboró tres ciberguías que se difundieron a través de las redes sociales, y que estuvieron enfocadas en tres públicos diferentes.

En esta edición de Cibersucesos encontrarás un resumen de estos temas. El primero de ellos consiste en una completa guía donde se explican los siete principales riesgos cibernéticos para niños, niñas y adolescentes, cómo enfrentar las amenazas y consejos para evitar que un menor se convierta en una víctima.

El segundo tema estuvo dirigido a las personas mayores con ciberconsejos para guiarlos en el mundo digital. En esta publicación, se trataron conceptos básicos sobre el uso de internet, la navegación, manejo de las redes sociales, creación de contraseñas, entre otros tópicos.

La tercera guía estuvo enfocada en las pymes y cómo lograr la transformación digital sin olvidar la ciberseguridad. Para esto, se elaboraron kits con herramientas para analizar la seguridad, de concientización y legal.

Si bien muchas instituciones concentran sus campañas de ciberseguridad en el mes de octubre, no hay que olvidar que la concientización en ciberseguridad debe ser un trabajo constante, permanente y que perdure en el tiempo, ya que de esta forma la lograremos integrar en nuestra cultura y que sea parte de nuestro día a día. Así como cerramos la puerta de la casa al salir, los mismos cuidados se deben tomar al usar un equipo o dispositivo.

El CSIRT de Gobierno los invita a mantenerse informados sobre los riesgos y amenazas del mundo digital, a tomar las precauciones necesarias en nuestros equipos, a cuidar la vida privada que hoy está tan expuesta y a guiar a los menores en este camino, para que todos logremos construir una sociedad más cibersegura.

RIESGOS CIBERNÉTICOS **A LOS QUE SE ENFRENTAN LOS MENORES DE EDAD**

En nuestro país, 9 de cada 10 menores tienen un celular. Esto demuestra lo expuestos que están los niños a los riesgos que conlleva navegar por Internet, los que en ocasiones son desconocidos tanto para los hijos como sus padres, madres o tutores. A continuación, explicamos en qué consisten siete riesgos a los que se pueden ver afectados los niños, niñas y adolescentes.

1.- GROO**MING**

Consiste en la manipulación de un niño, niña o adolescente (NNA) por parte de un adulto, a través de internet, para crear gradualmente lazos emocionales y finalmente acosarlo sexualmente y/o generar pornografía infantil. Si el niño se niega, el adulto procede a chantajearlo (flagelo conocido como sextorsión). Generalmente, para ganarse la confianza del niño, el victimario se hace pasar por otro menor de edad.

Cómo enfrentarlo **junto a tus hijos:**

- **Explícales** qué es el grooming.
- **Enséñales** a desconfiar de desconocidos en internet.
- **Refuérzales** que nunca deben entregar datos personales o fotos íntimas a nadie.
- **Explícales** que deben avisar a sus padres si alguien les pide datos o imágenes personales.

Ante un caso **de grooming:**

Los padres deben evitar contactarse con el abusador, nunca acceder a sus chantajes y denunciarlo ante la Policía de Investigaciones (PDI).

Recomen**daciones:**

Los padres deben mantener una relación de confianza y comunicación con sus hijos, y acordar normas de uso de internet con ellos.

Pueden decidir de común acuerdo un contrato de uso del internet, con detalles como los horarios y sitios permitidos y que los menores se comprometan a no contactar desconocidos. Un ejemplo es nuestro Acuerdo Parental.

Los menores deben comenzar a utilizar internet bajo supervisión de sus padres. Su uso autónomo debe ser progresivo según su edad y madurez. Cuando son más pequeños se pueden usar controles parentales, como los que delineamos en nuestra Guía de Mediación Parental.

2.- CYBERBULLING / **CIBERACOSO**

Se trata del tradicional acoso, pero efectuado a través de medios digitales, lo que posibilita que la intimidación sea realizada en todo momento y lugar, y con mayor alcance y potencial de permanencia.
Es importante recordar, asimismo, que cuando se realiza en el contexto escolar, los colegios tienen la responsabilidad legal de adoptar medidas disciplinarias, y de no hacerlo, pueden ser denunciados.

Cómo **enfrentarlo:**

- Los niños deben tener claro que pueden confiar en padres y profesores para contarles lo que están sufriendo.
- Motivar a los menores a actuar cuando vean a amigos o compañeros ser objeto de acoso.
- Lo mismo para los chicos que abusan de otros, debe hacérseles ver que eso no está bien y deben dejar de hacerlo.

Recomen**daciones:**

Como en todo problema que afecte a los menores, es indispensable que exista un ambiente de confianza con sus padres para que recurran a ellos cuando sean víctimas de ciberacoso. Es ideal formarles la costumbre de contar lo que les sucedió durante el día, como algo normal.

3.- OVER**SHARING**/ COMPARTICIÓN DE EXCESIVOS DATOS PERSONALES

Muchos usuarios de internet, ya sean niños o adultos, publican más información de la que es conveniente. Esto es particularmente peligroso con los NNA, que pueden no tener conciencia de los riesgos de dejar en línea fotos o direcciones que los pueden hacer identificables a adultos peligrosos, como potenciales abusadores sexuales, secuestradores o ladrones.

Cómo **enfrentarlo:**

- Tanto los niños como los adultos deben publicar lo menos posible, idealmente nunca fotos de ellos mismos, de sus hijos y jamás donde viven, donde estudian o donde van a estar en determinado momento. Tampoco difundir de forma pública el número de teléfono.

- Esto mismo se debe extender a imágenes e información de los familiares y amigos, especialmente si piensan compartir estos datos sin el consentimiento de sus dueños.

Recomen**daciones:**

Como en todo problema que afecte a los menores, es indispensable que exista un ambiente de confianza con sus padres para que recurran a ellos cuando sean víctimas de ciberacoso. Es ideal formarles la costumbre de contar lo que les sucedió durante el día, como algo normal.

4.- SEX**TING**

Se trata de enviar o recibir fotos o videos de connotación sexual de forma voluntaria a través de internet. Es un problema porque el entregar imágenes sensibles a otros nos expone a chantajes y, especialmente en el caso de los menores de edad, a humillaciones y cyberbullying. Los adultos pueden hacerse pasar por otros menores para intercambiar imágenes y luego chantajear a los NNA a cambio de favores sexuales.

Cómo **enfrentarlo:**

- Nuevamente, la clave es tener conciencia de los riesgos. Recordar a los NNA que una vez algo es compartido en internet, es imposible estar seguro de que haya sido borrado, que hay adultos haciéndose pasar por menores de edad para aprovecharse de ellos y que incluso aunque diga que no las compartirá o que las borrará después de recibirlas, es muy probable que si nos piden fotos de connotación sexual éstas sean guardadas y compartidas por el receptor con sus amigos.

Recomen**daciones:**

- Lo ideal es nunca compartir fotos privadas a través de internet y, en caso de hacerlo, evitar que aparezcan en ellas la cara del menor u otros elementos fácilmente identificables, como tatuajes y lunares.

- La confianza es esencial. Para que los niños, niñas y adolescentes tengan confianza de avisarles si han caído en alguna extorsión por sexting, por ejemplo, los padres y tutores deben evitar culpar excesivamente al menor de lo sucedido y enfocarse en primer lugar en realizar la denuncia ante la PDI.

5.- COMPRAS **EXCESIVAS ONLINE**

Muchas aplicaciones y juegos exigen u ofrecen la opción de pagar por mejoras o personalizaciones, sin embargo, hay niños que no saben cómo funciona el dinero, o que pueden comprar sin saber, dejando con abultadas cuentas a sus padres.

Cómo **enfrentarlo:**

- Los NNA deben tener conciencia de que no pueden comprar nada sin hacerlo en presencia y con la aprobación explícita de sus padres.

Recomen**daciones:**

Si se le va a entregar un dispositivo a un niño para que se conecte a internet, asegurarse antes de que no tenga medios de pago, como tarjetas de crédito y claves bancarias registradas para facilitar el pago. Lo más seguro es ingresar los datos cada vez.

6.- RETOS VIRALES **PELIGROSOS**

Abundan en las redes sociales distintos desafíos o “challenges”, en inglés, que invitan a los seguidores a repetir conductas a veces inocuas, otras peligrosas, como el llamado a consumir cápsulas de detergente que enfermó a varios niños en EE.UU. en 2017.

Cómo **enfrentarlo:**

- Es muy difícil instruir a los NNA para resistir los retos de sus pares, ya sea en el mundo físico o en el digital, ya que el temor a ser excluido es uno de los más fuertes en los menores. Sin embargo, es clave instaurar la importancia de no dejarse arrastrar por conductas peligrosas y recordar siempre que el verdadero valor de una persona no se mide por sus vistas o likes.

Recomen**daciones:**

Permitir que los niños y niñas solo accedan a las redes sociales cuando tengan edad y madurez suficiente. Acompañar y vigilar su uso de las redes, si quieren imitar todo lo que aparece se debe poner aún más atención. Mantener la confianza y comunicación y, de ser necesario, usar aplicaciones de control parental.

7.-CONTENIDO **INAPROPIADO**

Se refiere a comentarios, textos, fotos o videos que pueden resultar perturbadores para los menores de edad si se encuentran con ellos en internet. Esto, debido a múltiples motivos, como corresponder a contenido violento, chocante, sexual o malicioso.

Cómo **enfrentarlo:**

- Los chicos deben saber que en internet se puede ver, casi literalmente, de todo. Y que si se enfrentan a imágenes que los hagan sentir incómodos o asustados pueden contar con sus padres para conversar.

Recomen**daciones:**

Los controles parentales y aplicaciones para niños son una forma de evitar el acceso a contenido inapropiado por parte de los más pequeños y les permiten ver contenido seguro. Entre ellas se cuentan:

- Google Family Link
- Kaspersky Safe Kids
- McAfee Safe Family
- Surfie

CONSEJOS GENERALES QUE TAMBIÉN **DEBEMOS ENTREGAR A NNA**

Hay recomendaciones que todos debemos seguir, sin importar la edad, y tenemos que asegurarnos que nuestros niños también conozcan y sigan:

Usar contraseñas seguras.

Se sugiere que sean mínimo 9 caracteres de largo y se usen símbolos, números, mayúsculas y minúsculas.

Una buena idea es utilizar secuencias de palabras inconexas, por ejemplo, una combinación de “persona”, “acción” y “objeto”, incluyendo además las reglas anteriores.

Nunca entregar nuestras claves, por mucho que prometa que no se la entregará a nadie más o diga ser un amigo.

Las actualizaciones parchan vulnerabilidades conocidas en los programas que usamos en computadores y celulares.

Estas actualizaciones deben ser descargadas exclusivamente desde las tiendas oficiales correspondientes a los sistemas operativos de nuestros dispositivos.

Los más chicos deben ser supervisados en internet y darles autonomía en su uso según su madurez.

DIGITALIZACIÓN **DE LAS PYMES**

Kit de herramientas para una empresa más cibersegura

La vida cotidiana de las personas y empresas está cruzada por servicios tecnológicos. En este contexto, las pymes deben tratar de aprovechar las ventajas de los procesos de digitalización y el creciente despliegue de conectividad, tanto a nivel nacional como mundial. Sin embargo, esta travesía no está exenta de riesgos, por eso es necesario tomar en cuenta diversos aspectos para evitar naufragar a mitad de camino. ¿Qué se debe considerar? Te contamos a continuación.

La transformación digital de las empresas y pymes ha tenido un importante avance en los últimos años. Para contextualizar, según la encuesta TIC del año 2018, sólo el 7% de las empresas en Chile tenían un área, rol o cargo dedicado a la seguridad TIC. Por otra parte, un 31% de las grandes empresas declaró tener un área para resolver incidentes TIC, mientras que en las pymes solo fue el 5%.

En el año 2019, un estudio realizado por IPSOS llamado "Ciberseguridad en las empresas chilenas" evidenció que:

a. 4 de cada 10 empresas reconocen haber tenido algún ataque cibernético.

b. El 40% de las micro, 45% de las pequeñas y el 56% de las medianas empresas se consideran vulnerables frente a ciberataques.

c. El 65% de las empresas consideran que un ataque cibernético afecta la imagen y reputación corporativa.

d. Menos del 40% de las empresas creen tener los recursos humanos suficientes para la ciberseguridad.

e. A la hora de buscar información sobre ciberseguridad, sólo el 20% de las microempresas lo hacen, aumentando a cerca del 50% en pequeñas y medianas.

Con la llegada de la pandemia, muchas organizaciones adoptaron más tecnologías digitales. De acuerdo a un estudio publicado por la OCDE, en el que se comparó el proceso de digitalización entre las pymes del bloque, un 62% de las pequeñas y medianas empresas chilenas aumentaron el uso de tecnologías digitales y un 90% de ellas cree que este cambio será permanente.

No obstante, la urgencia no necesariamente se tradujo en una adopción que considera la ciberseguridad como parte importante de este proceso.

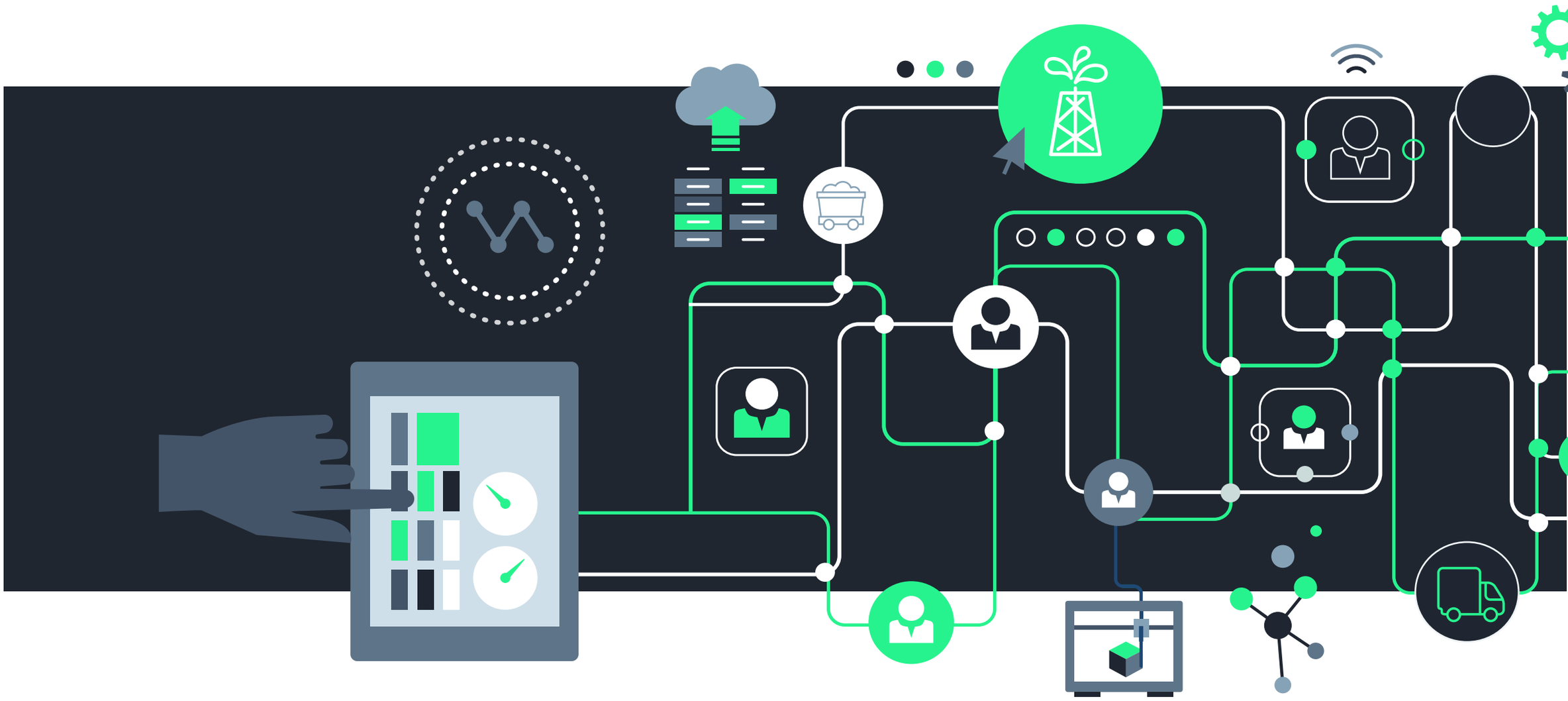
Transformación digital **y ciberseguridad**

Ante esta nueva realidad, se debe tener claro que si una pyme comienza a utilizar sistemas digitales como redes sociales, puntos de venta, CRM, ERP, entre otros, es fundamental implementar medidas adecuadas de ciberseguridad, ya que de lo contrario están arriesgando la pérdida de todos sus activos y reputación en caso de sufrir un incidente.

Por lo general, los principales ataques que sufren las empresas son:

- Pérdida temporal de acceso a archivos
- Eliminación de sitios web
- Corrupción de programas o sistemas
- Pérdida permanente de archivos y del acceso a servicios

Frente a las distintas amenazas, es necesario que las empresas implementen un plan integral que les permita evaluar sus procesos, conocer los riesgos a los que están expuestos, educar a sus trabajadores, informarse de las tecnologías que contribuyen a monitorear y analizar amenazas, etc., con el objetivo de garantizar la privacidad de los datos de los clientes, proteger los activos de la empresa y mantener la continuidad de los servicios.



Antes de comenzar a tomar decisiones, lo primero que se debe hacer es conocer la situación actual. Para esto, se debe realizar un diagnóstico que identifique el nivel de madurez de la ciberseguridad de la organización, la cual posteriormente nos guiará en la resolución de los aspectos que necesiten mejoras.

Algunos de los factores que se tienen que revisar internamente al momento de ingresar al ciberespacio son:

Teletrabajo:

1.– La tecnología permite a los emprendedores trabajar desde sus casas, pero al hacerlo, ¿tomamos las mismas precauciones que en la oficina? ¿Realmente conocemos todas las medidas de seguridad que necesitamos? ¿Aumentan los riesgos al utilizar computadores personales? ¿Crecen los riesgos al aumentar las interacciones y transacciones de productos o servicios que realizamos digitalmente?

Comercio electrónico:

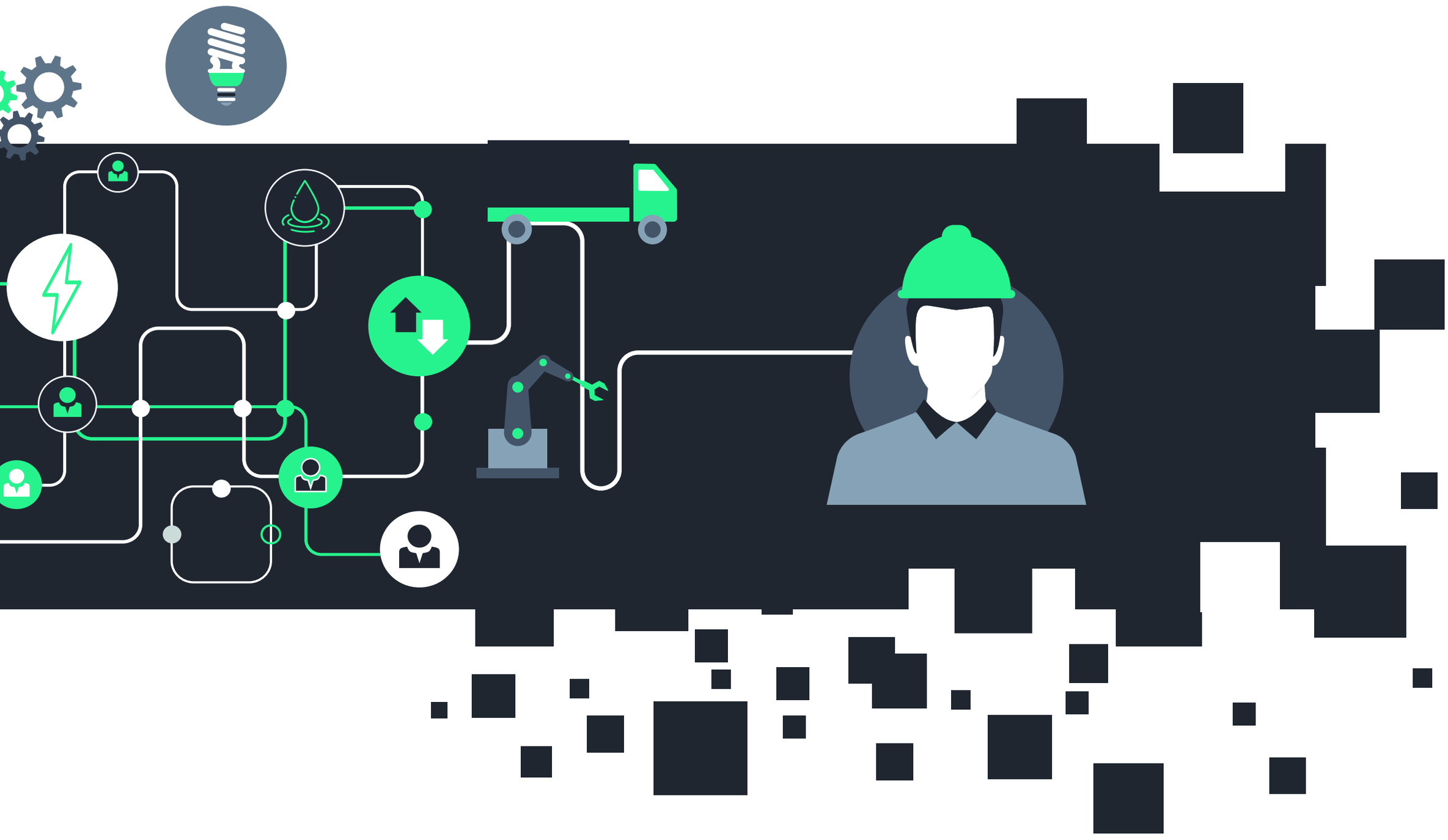
2.– En Chile, su tasa de penetración llega al 82%. Empresas de todos los tamaños deben adaptarse a estas condiciones, reinventando sus procesos y adoptando una estrategia de negocios e-commerce. La pandemia impulsó la transformación digital de las empresas, pero no necesariamente estuvo acompañada de la adopción de una cultura y sistemas ciberseguros.

Cloud:

3.– La computación en la nube (cloud computing) puede significar grandes cambios para las pymes, especialmente en relación con el almacenamiento de datos sensibles. Por eso, antes de implementar un servicio cloud o si ya se cuenta con uno, hay que evaluar los riesgos a los que se exponen en la nube y cómo se pueden minimizar; conocer el historial que tiene el proveedor garantizando la confidencialidad de los datos de sus clientes y revisar si los datos son tan valiosos que es más conveniente manejarlos en servidores propios.

Datos y su privacidad:

4.– Toda la información que maneja un negocio tiene valor, de ahí la importancia de identificar el capital digital de una empresa y resguardarlo adecuadamente.



Concienciación general para sus recursos humanos:

5.– A la hora de hablar de seguridad de la información, siempre suele hablarse de tecnologías y procesos, pero en realidad los protagonistas de la seguridad en las empresas son los empleados que gestionan y utilizan los dispositivos tecnológicos de la organización para trabajar con la información.

Una aproximación gratuita a este tipo de evaluación puede encontrar en la Guía de Ciberseguridad para Pymes de la Cámara Nacional de Comercio en el siguiente enlace:

https://pymecibersegura.cl/quest

KIT DE **CIBERSEGURIDAD**

A continuación, el CSIRT de Gobierno entrega tres kits de seguridad que contribuyen a resguardar la información y los sistemas en distintos aspectos:

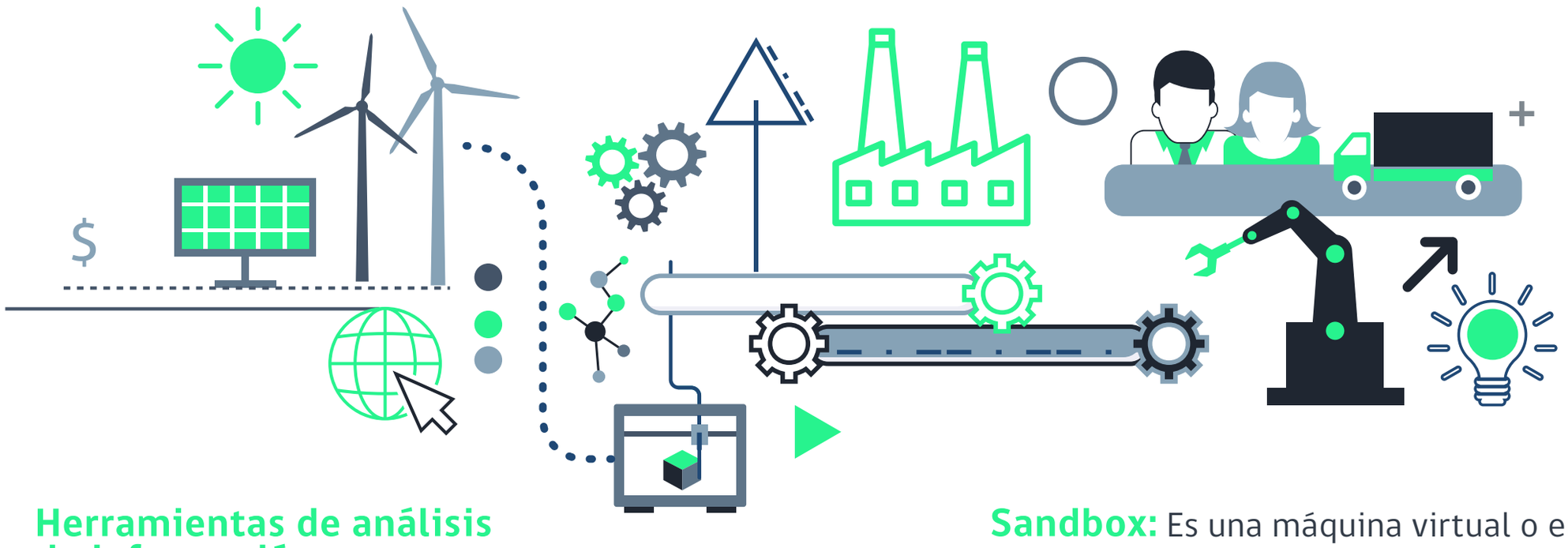
I Kit de Herramientas para analizar seguridad:

Tienen como objetivo analizar los riesgos informáticos y evaluar las vulnerabilidades a las que están expuestas las empresas, de manera de prevenir un ciberataque que ponga en peligro los activos de la empresa o se exponga al robo de información de los datos de sus clientes.

Para esto, se pueden utilizar tres tipos de herramientas: monitoreo, análisis y gestión de procesos. Algunas alternativas gratuitas son:

Herramientas de monitoreo de redes y seguridad:

- **WAZUH:** https://wazuh.com/
- **NAGIOS**: https://www.nagios.org/
- **GRAFANA:** https://grafana.com/



Herramientas de análisis de información:

- **Amap: https:**//www.kali.org/tools/amap/
- **cisco-torch:** https://www.kali.org/tools/cisco-torch/
- **DMitry: https:**//www.kali.org/tools/dmitry/

Herramientas para gestión de incidentes a través de ticket:

- **OTRS:** https://otrs.com/es/home/
- **JIRA:** https://www.atlassian.com/es/software/jira
- **GLPI:** https://glpi-project.org/

Analizadores online: Es una plataforma que permite analizar en línea archivos y URL sospechosas que puedan contener algún tipo de malware o se utilicen con otros fines ilícitos.

- **VIRUS TOTAL:** https://www.virustotal.com/es/
- **ANY.RUN:** https://any.run

Análisis forense: Consiste en un conjunto de técnicas y herramientas de investigación científica para extraer la información de cualquier soporte sin alterar su estado.
Cuando una empresa es víctima de un ciberataque, el análisis forense se encarga de recopilar datos sobre el incidente a través distintas etapas: Identificar el ataque, preservar los discos, analizar la información rescatada y presentar la evidencia. Algunas herramientas gratuitas disponibles en la web son:

- **CAINE:** http://www.caine-live.net/
- **DEFT Linux:** http://www.deftlinux.net/
- **SIFT:** https://www.sans.org/tools/sift-workstation/

Sandbox: Es una máquina virtual o entorno de prueba aislado que permite ejecutar un software o códigos sospechosos, a partir de archivos adjuntos o URL desconocidas, con el fin de observar su comportamiento, identificar el tipo de código y generar un reporte de acciones a considerar para no dañar los sistemas. Así también se utilizan para probar e implementar un software. Algunos sistemas de análisis recomendados son:

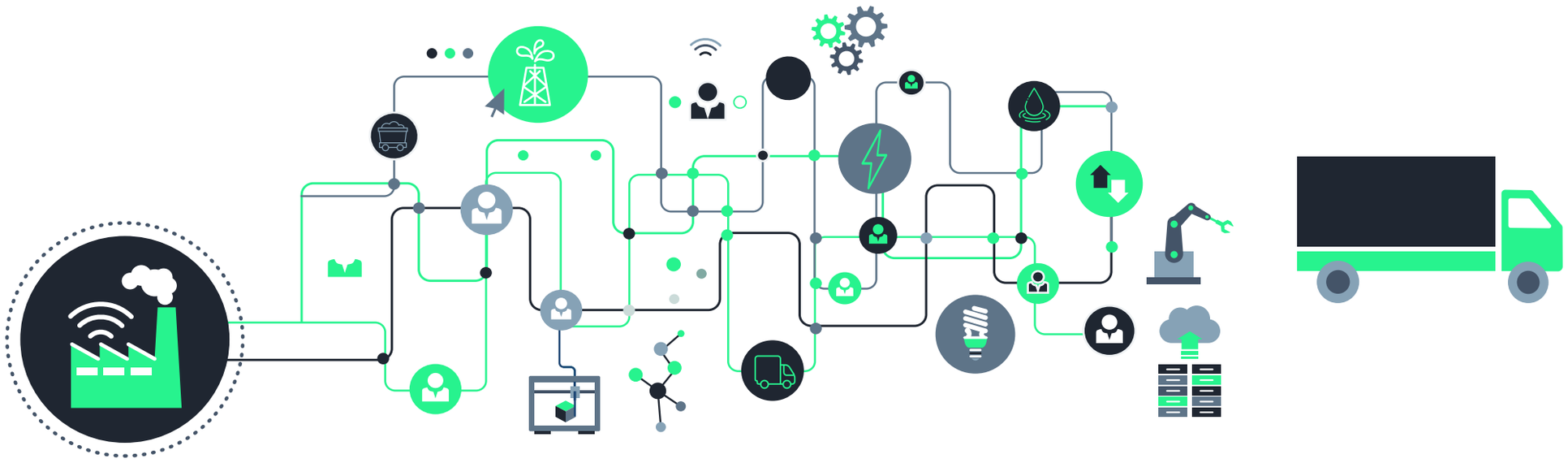
- **CUCKOO:** https://cuckoosandbox.org/
- **SANDBOXIE:** https://github.com/sandboxie/sandboxie
- **SNDBOX**: https://www.sndbox.com/

II Kit de Herramientas para analizar seguridad:

Educar a los trabajadores es primordial, ya que en su mayoría los ataques llegan por un phishing a través de emails a la empresa. El CSIRT de Gobierno pone a disposición de la ciudadanía material educativo sobre distintas amenazas presentes en el ciberespacio.

"Seguridad digital para pymes: Centros de monitoreo de bajo costo". Está dirigido a quienes administren plataformas digitales expuestas a internet en sus pequeños y medianos negocios, para que puedan proteger la confidencialidad, integridad y disponibilidad de sus activos. El autor, Carlos Montoya, fundador y director de Whilolab, detalla el uso de siete herramientas de código abierto.

Disponible en: **https://www.csirt.gob.cl/reportes/an2-2020-18/**



Ciberconsejos: Para contribuir en la prevención de un ataque, entregamos 4 consejos útiles y sencillos de aplicar para que las pymes protejan los datos de los ciberdelincuentes.

Encuéntralos en: **https://www.csirt.gob.cl/recomendaciones/ciberconsejos-de-seguridad-para-pymes/**
Además, puedes descargar más recomendaciones para tus trabajadores en: **https://www.csirt.gob.cl/recomendaciones/**

Controles Normativos: Cada semana se presentan los diferentes controles normativos que son prioritarios para todo Sistema de Gestión de Seguridad de la Información. Estas directrices no reemplazan el análisis de riesgo institucional, pero permiten identificar instrumentos, herramientas y desarrollos que mejoran la postura de ciberseguridad institucional.

Hasta la fecha, el CSIRT ha realizado 17 publicaciones, las que puedes encontrar en: **https://www.csirt.gob.cl/estadisticas**

III Kit legal

En el ámbito legal, el CSIRT de Gobierno elabora documentos que permitan guiar a los emprendedores cómo defender su marca ante la suplantación de identidad o publicando las mejores prácticas en materia de ciberseguridad.

A.- Manual de Resolución de Conflictos por Nombres en dominio .CL: Una forma en que nuestra empresa puede verse amenazada es a través de la suplantación en internet de la imagen y nombre, con el objetivo de robar sus ventas, dañar su reputación o robar información de sus clientes. Si nos vemos en esta situación, podemos hacer una solicitud de revocación de dominio ante NIC Chile, entidad que administra los dominios .CL.

Disponible en:
https://www.csirt.gob.cl/reportes/manual-de-dominio/

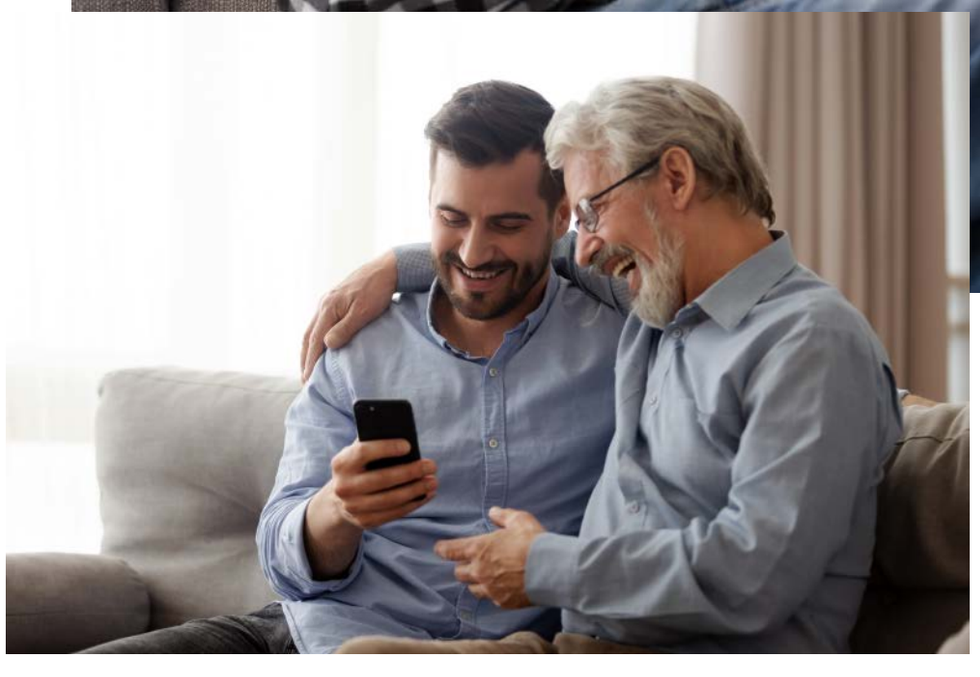
B.- Políticas: Varias de las mejores prácticas en ciberseguridad pueden implementarse a través de políticas, procedimientos que describen cómo materializar estas prácticas en cuanto a procesos, responsables, herramientas e indicadores de su eficiencia y eficacia.
Encuentra las políticas de seguridad de la información que hemos elaborado, aquí: https://csirt.gob.cl/matrices-de-politicas/

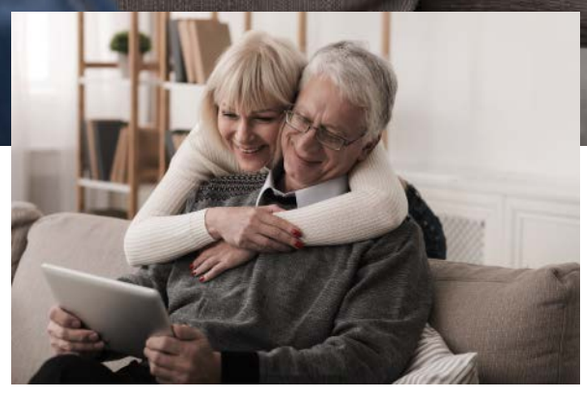
Puedes encontrar esta y más información en el sitio web **www.csirt.gob.cl** y en nuestras redes sociales.

PERSONAS MAYORES **MÁS DIGITALIZADAS**

Recomendaciones para una navegación más segura

Un importante avance en el uso de Internet se ha visto por parte de los adultos mayores, para quienes hoy también la tecnología es parte de su vida diaria ya sea para comprar, comunicarse o ver una película. Y mientras más conectados, más informados hay estar. ¿Qué se debe considerar para navegar más seguros?





Un 91% de las personas mayores entre 60 y 80 años considera que Internet es útil en su vida diaria, según la encuesta elaborada, en agosto de este año, por el Programa Convive Digital de VTR junto a Criteria sobre el uso de internet y dispositivos.

Otros datos interesantes que se aprecian en este estudio acerca del comportamiento de este grupo de personas en el mundo digital son:

- **80%** dice que durante el último año buscó noticias y películas en Internet.
- **86%** se conecta a Redes Sociales todos los días.
- **8 de cada 10** encuestados realiza trámites online.
- **95%** conoce el concepto de "huella digital".
- **9 de cada 10** personas mayores se ha comunicado con sus familiares y amigos por Redes Sociales. Tema 4 Personas mayores CORTO

Sin duda que esta son muy buenas noticias, por lo que queremos empoderar aún más a las personas mayores y entregarles ciertas recomendaciones y buenas prácticas para navegar más seguros.

1.– Conexión **segura a Internet**

Vivir en el mundo digital implica que todo aquello que nos mantiene conectados a internet y al uso de las tecnologías tiene beneficios y también riesgos. Todo lo que hacemos, desde que nos conectamos a una red wifi hasta la forma en que nos compartamos al navegar por Internet, puede tener consecuencias negativas si no tomamos las medidas de seguridad necesarias.

¿Cómo te conectas a internet? Generalmente se utiliza una red wifi que puede ser privada (nuestra casa) o pública (supermercado, Metro, etc.). En este último caso debemos tener mucho cuidado, puesto que en ocasiones estas redes no son confiables ni tampoco seguras, ya que detrás de éstas puede haber ciberdelincuentes que buscan:

1. Robar nuestras contraseñas, datos e información sensible.
2. Redireccionarnos a páginas fraudulentas.
3. Infectar el dispositivo con malware.

Dispositivos **Protegidos**

Tener un computador o smartphone requiere de ciertos cuidados, ya que los ciberdelincuentes logran sus objetivos gracias al descuido de las personas. Por eso, es fundamental contar con los elementos básicos de protección. Algunos de ellos son:

Antivirus: Herramienta esencial para cualquier tipo de dispositivo (computadores, Tablet, smartphone, etc.), ya que tiene como objetivo detectar, eliminar y prevenir los virus informáticos (malware) que circulan en internet o que, sin darnos cuenta, descargamos desde un correo electrónico o una página web.

Actualización de programas: Todos los dispositivos, programas o aplicaciones cuentan, cada cierto tiempo, con una actualización. Esto, permite que se agreguen nuevas funcionalidades o que el creador corrija alguna falla de seguridad. En la mayoría de los casos, esta actualización se descarga automáticamente, pero en ocasiones este proceso debemos hacerlo nosotros mismos.

Bloqueo de dispositivo: Tiene como fin evitar que cualquier persona pueda acceder a nuestro teléfono o computador, y a la información que tenemos ahí. Debemos configurar esta opción en los dispositivos, los que solicitarán una contraseña, huella dactilar, un PIN o patrón para poder ingresar una vez encendido el dispositivo. Todos los teléfonos inteligentes tienen esta opción, pero la forma de acceder a esta alternativa dependerá de la versión y el modelo del teléfono.

Por ejemplo, para un **Android** la forma de bloquear el dispositivo es siguiendo estos pasos:

1. Dirígete a "Ajustes"
2. Selecciona "Contraseña y seguridad"
3. Busca la opción "Seguridad"
4. Encontrarás "Bloqueo de pantalla"
5. Podrás seleccionar el tipo de contraseña que quieras utilizar para desbloquear: patrón, PIN, contraseña, huella dactilar, desbloqueo facial o con dispositivo Bluetooth.

En el caso de **IPhone**, debes:

1. Ingresa a "Configuración"
2. Elije la opción "Pantalla y brillo"
3. Selecciona "Bloqueo automático" y en cuánto tiempo que se bloquee el dispositivo.

¡Recuerda! : También puedes utilizar esta herramienta en un tablet y computador.

2.– Tipos de fraudes y **estafas en Internet**

Phishing: Es la técnica de ataque por excelencia en el mundo cibernético, y ocurre cuando una persona recibe un correo electrónico que trata de persuadirlo para visitar un link o abrir algún archivo adjunto con información, el que conduce a un sitio fraudulento o descarga malware en el equipo.

Por lo general, estos correos provienen supuestamente de una empresa confiable, por lo que la víctima no duda de la información, pero es posible identificar esta estafa si estamos atentos a:

1. Llama nuestro interés con ofertas u ofreciendo premios si hacemos lo que se solicita en el correo.
2. Nos pide actualizar nuestra información al ingresar a un link, en donde nos pedirán el usuario y contraseña, por ejemplo, de un sitio bancario.
3. Recibimos un e-mail con un documento adjunto que, supuestamente, habíamos solicitado.
4. Ofrecen beneficios económicos o reprogramar deudas bancarias. Durante el año 2020, este tipo de phishing fue uno de los más comunes, con motivo de la crisis sanitaria por COVID.

3.– Redes **Sociales**

Algunas de las redes sociales más conocidas son: Facebook, Instagram, WhatsApp, Youtube, Tik Tok, Linkedin, Snapchat, Twitter, etc. Y si bien la información que compartimos puede ser muy entretenida e interesante, también es un blanco muy atractivo para los ciberdelincuentes, quienes usan esa información para cometer distintos tipos de estafas, como:

1. Suplantación de identidad
2. Préstamos falsos
3. Concursos fraudulentos
4. Descuentos en productos de lujo
5. Phishing
6. Secuestro de cuentas de WhatsApp

En su mayoría, los fraudes a través de las redes sociales tienen como objetivo robar información o dinero. Evita ser una víctima, siguiendo estas recomendaciones:

a. **No aceptar** sugerencias de amistad de personas que no conoces o de famosos.

b. **Desconfiar** de los link que te envían, especialmente si es de un desconocido o, supuestamente, del equipo de soporte de la red social.

c. **Nunca aceptes** préstamos de dinero, aunque ofrezcan tazas de interés muy bajas.

d. **Nunca entregues** tu información sensible: cuentas bancarias, tarjetas de coordenadas, contraseñas.

e. **No compartas** códigos que te envían por WhatsApp

f. **Desconfía** de los mensajes directos de quienes no conoces, sobre todo si tiene errores gramaticales, se dirigen de forma genérica o su mensaje es alarmante.

g. **Nunca** transfieras dinero a desconocidos, especialmente si lo solicitan como requisito para ganar algún premio.

h. **Sé crítico** con la información que recibes. Si venden productos a muy bajo precio, en comparación con el mercado, o si ofrecen premios en dinero sólo con entregar tus datos, desconfía.

i. **Nunca** confíes 100%. Lo mejor siempre es investigar y verificar la información.

j. **Configura** tus redes sociales en modo privado para que sólo tus verdaderos amigos y conocidos puedan ver tu información.

4.– Contraseñas **Seguras**

Gracias a las contraseñas podemos mantener nuestra información segura y protegida. Pero para esto, es importante crear claves robustas, ya que de lo contrario el riesgo es que los delincuentes accedan a tus cuentas, usar tus plataformas y servicios, roben tu información, tus datos, tu dinero e incluso puedan suplantar tu identidad, es decir, una contraseña débil afecta tu privacidad y seguridad.

Para crear una clave segura necesitas:

1. Utilizar mínimo 9 caracteres.
2. Usa letras mayúsculas y minúsculas, símbolos y números.
3. Utiliza frases de canciones, poemas, libros, etc.
4. Usa claves diferentes en cada sitio o aplicación en la que estés registrado.

Cambia la contraseña periódicamente
Nunca crees una contraseña con:

1. Datos personales como RUT, fechas de nacimiento, direcciones, etc.
2. El nombre de algún familiar.
3. El número de teléfono o fechas de cumpleaños.

Chile:

Uniendo a los CSIRT y CERT de América y el Caribe en concientización

Durante el Mes de la Ciberseguridad, 12 entidades de la región publicaron ciberconsejos organi zados en una campaña temática por cada semana de octubre, siendo las recomendaciones idea das por cada participante y los diseños finales enviados desde Chile a cada uno de ellos.

La idea comenzó con conversaciones informales entre un par de organizaciones miembros de CSIRTAmericas, grupo que reúne a los CERT y CSIRT del continente, bajo el alero de la Organización de los Estados Americanos (OEA): Colombia, República Dominicana, Costa Rica y Chile. "¿Por qué no compartir los ciberconsejos que cada semana publica el CSIRT del Gobierno de Chile en sus redes sociales, y así llevar su impacto a nivel regional?", fue lo que se preguntaron estos países, recuerda Katherina Canales, Directora Operacional del CSIRT del Gobierno de Chile, principal impulsor de la iniciativa.

La representante de Chile rememora así como "el entusiasmo creció, y en la siguiente reunión de CSIRTAmericas se planteó el proyecto de realizar campañas en conjunto durante octubre, Mes de la Ciberseguridad. En definitiva, se subieron 12 CSIRT y CERT al proyecto: Estados Unidos, República Dominicana, Jamaica, Costa Rica, Panamá, Colombia, Ecuador, Buenos Aires y Neuquén en Argentina, Paraguay, Uruguay y Chile". Cada organismo envió unos consejos cortos en inglés y castellano, los cuales fueron convertidos en diseños por nuestro CSIRT de Gobierno en Chile, para luego ser publicados en Twitter por el CERT que ideó las recomendaciones y ese mismo día retwitteados por los demás partícipes del proyecto. El primer post fue hecho por la cuenta de ciberseguridad de la OEA (@OEA_Cyber).

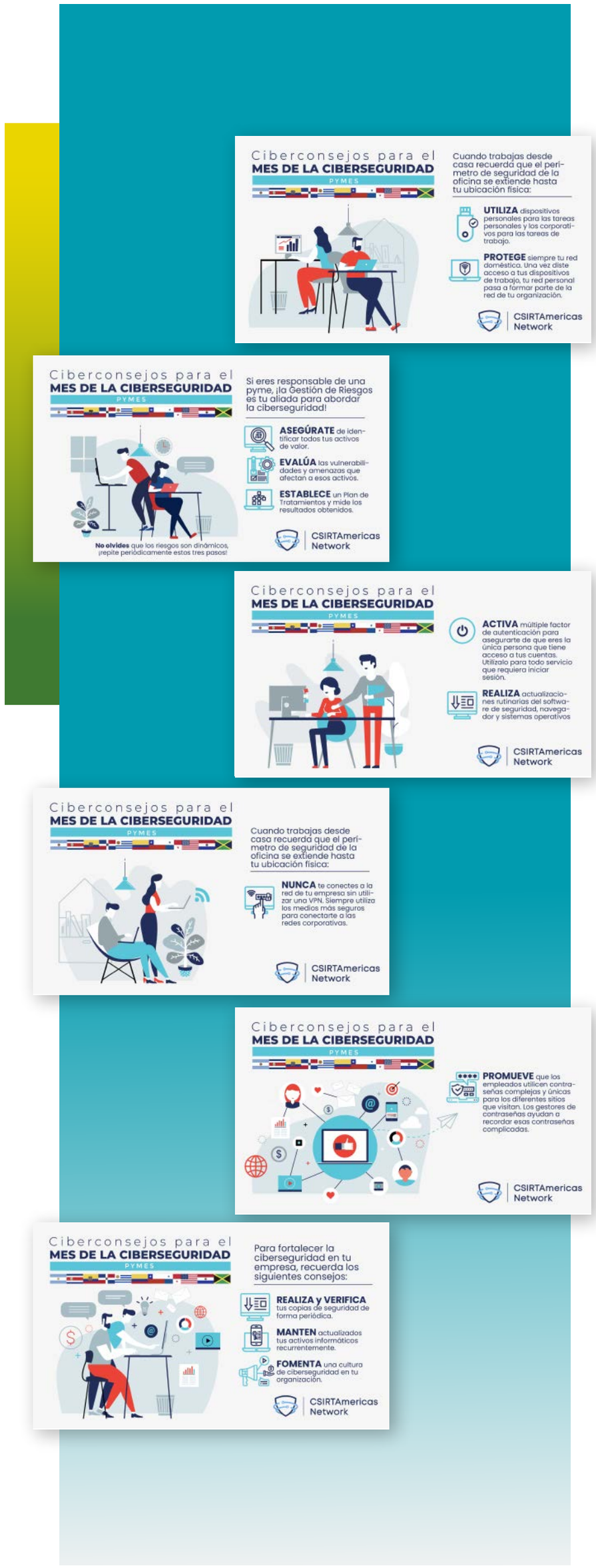
"Esta ha sido una tremenda iniciativa, la que nos permitió no solo difundir valiosos consejos de ciberseguridad de norte a sur del continente, sino que reforzó nuestras instancias de colaboración y trabajo en equipo entre 12 organismos de ciberseguridad de la región", destaca Carlos Landeros, Director Nacional del CSIRT del Gobierno de Chile.

Cada semana los consejos fueron destinados a un tema diferente

Primera semana: Consejos generales para toda la población. Publicados por la OEA, Chile y Costa Rica.

Segunda semana: Recomendaciones para niños, niñas y adolescentes. Publicados por Paraguay, Uruguay y Buenos Aires.

Tercera semana: Prácticas de seguridad asequibles para pequeñas y medianas empresas (pymes). Publicados por Panamá, EE.UU., Jamaica y Neuquén.



Cuarta semana: Consejos para adultos mayores. Publicados por República Dominicana, Colombia y Ecuador.

PARTÍCIPES DESTACAN COLABORACIÓN INTERAMERICANA

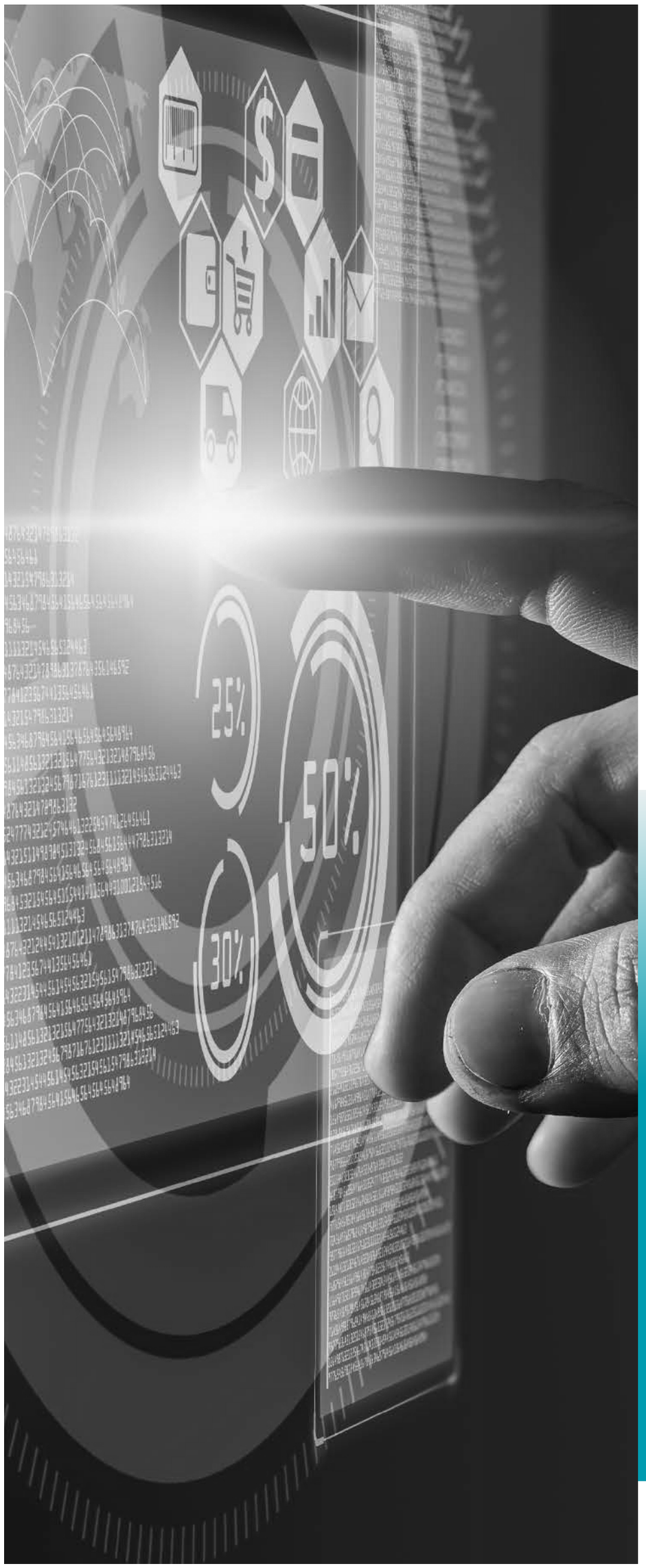
El factor colaborativo de la campaña es especialmente destacado por la secretaria ejecutiva del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), Alison August Treppel, quien señala: "Nos complace mucho que los miembros de CSIRTAmericas Network, el principal impulsor del pilar de construcción de capacidades del programa de ciberseguridad del CICTE, hayan colaborado en esta campaña, que tiene como fin común la concientización durante el Mes de la Ciberseguridad. A través de estos consejos prácticos, seguimos difundiendo conocimiento de valor para lograr una ciudadanía más segura en el ciberespacio".

En la misma línea reflejaron su experiencia los líderes de los países que participaron en esta iniciativa. Así, Roberto Lemaitre, Coordinador del Centro de Respuesta de Incidentes Informáticos de Costa Rica, explica: "Los diferentes informes regionales en materia de seguridad nos han mostrado que los países de la región compartimos retos en esta materia. Es por esto que los CSIRT nacionales, que tenemos un enorme reto dentro de nuestros países como directores de orquesta de la ciberseguridad, debemos trabajar unidos y con un contacto más cercano para ir mejorando estas capacidades".

Lemaitre resalta que "mientras a los cibercriminales no les importan fronteras, y se coordinan para sus actos, los países debemos trabajar unidos para enfrentar problemas comunes, uno de ellos el reto de la cultura digital. Un gran porcentaje de los ciberdelitos se evita educando a la ciudadanía, y la necesidad de formación la compartimos entre países", por lo que, concluye, "unir esfuerzos para mejorar la cultura digital resulta vital. Este mes de concientización de ciberseguridad nos motiva a seguir trabajando juntos, compartir conocimiento, experiencias y capacidades. Porque al final el tema no es solo de un país, hay que recordar que juntos somos más fuertes"

Victor Figueroa, Director de Seguridad de la Información del gobierno de la Provincia de Neuquén, en Argentina, señala que "en el marco de la Primer Campaña Regional de Concientización en materia de Ciberseguridad, que vinculó a los Equipos de Respuesta a Incidentes de CSIRTAmericas, y que tuvo al CSIRT de Chile como su principal promotor, debemos destacar que la iniciativa sienta un excelente precedente de cara al futuro para abordar los ciberriesgos con una estrategia regional".

Para Figueroa, asimismo, "el éxito de ésta iniciativa no solo se basa en el gran impacto que ha tenido la campaña en las redes sociales, sino también en el éxito de la coordinación entre los distintos CSIRT del continente para que sus equipos publicaran sus ciberconsejos a la comunidad, compartiendo recomendaciones a partir de la experiencia adquirida en la gestión cotidiana de la ciberseguridad".



Y es que “las amenazas en el ciberespacio son cada vez más complejas y diversas, y las vinculaciones colaborativas permiten aunar esfuerzos y conocimientos para hacer frente a estos retos”, concluye el experto de Neuquén.

Por su parte, Carlos Leonardo, Director del Equipo de Respuesta a Incidentes Cibernéticos de República Dominicana (CSIRT-RD), indica que “poner en marcha de acciones en conjunto para sensibilizar en ciberseguridad es un compromiso que hemos asumido”, ya que “como región hemos dado un gran paso al realizar esta campaña de cultura de seguridad cibernética entre miembros de la OEA, que nos integra y permite afianzar la comunicación, alinear esfuerzos en el fomento de una cultura de seguridad y crear canales unificados de comunicación efectiva”.

Por todo esto “agradezco especialmente al CSIRT de Chile por haber traído esta importante iniciativa a la mesa del grupo de trabajo, para juntos lograr un ciberespacio más confiable y seguro para todos”, concluye Leonardo.

“En virtud de los desafíos relacionados con los riesgos que enfrentamos en el ciberespacio”, explica Wilson Prieto, Coordinador Nacional de CERT Colombia, “es de la mayor importancia generar diferentes iniciativas regionales para concientizar, a través de ciberconsejos prácticos, a usuarios, padres, madres, tutores, adultos mayores y pymes, generando conductas de ciberhigiene digital. Esta iniciativa de cooperación internacional, liderada por la red CSIRTAmericas, permitió establecer una sinergia regional enfocada en la adecuada gestión de riesgos en el entorno digital”.

Gabriela Ratti, Directora general de Ciberseguridad y Protección de la Información del Ministerio de Tecnologías de la Información y Comunicación del Paraguay: “A través de CSIRTAmericas y mediante un esfuerzo coordinado y colectivo, sumamos las recomendaciones aportados por todos los países, logrando llegar con un único mensaje, mucho más fuerte y visible que si los esfuerzos fueran aislados. Al fin y al cabo, las amenazas cibernéticas no conocen fronteras”.

Agrega que “este tipo de campañas coordinadas son fundamentales, por una parte, para lograr mayor impacto y visibilidad, reforzando entre todos los consejos, y por otra, permite optimizar los esfuerzos, generando materiales útiles, completos y que llegan a muchos más ciudadanos de toda la región. Este tipo de campañas regionales tienen un valor multiplicador, ya que de nada sirve que la información se maneje solo en los círculos profesionales. Esta debe llegar a los niños, docentes, personas mayores y a todos los usuarios de las tecnologías”.

Desde Uruguay, Fabiana Santellán, Gerente de Gestión y Auditoría de Seguridad de la Información de AGESIC, explica que “la transformación digital que tanto personas como organizaciones han tenido que afrontar para mantener sus actividades y procesos de negocio se ha acelerado más allá de lo previsto en el último tiempo, volviéndose indispensable incluir en el proceso la visión de ciberseguridad”.

En dicho contexto, agrega, “la concientización es clave, por ello desde el CERTuy hemos desarrollado diversas iniciativas, con el fin de sensibilizar tanto a personas como organizaciones a nivel nacional. Y como los esfuerzos nunca son suficientes, las alianzas son extremadamente valiosas, como esta campaña propuesta por OEA, que con un lenguaje cercano propone concientizar en esta temática en las Américas”.

“Compartir información para concientizar a los usuarios, es una de las tareas que no puede faltar en una organización”, recuerda Silvia Batista, Jefa del CSIRT Panamá. Es así que, sigue, “desde CSIRT Panamá realizamos esfuerzos para que esos mensajes lleguen a cada uno de nuestros clientes. Para esto contamos con diferentes campañas, tales como: ¿Sabías Qué?, ¡No Te confíes! y Teletrabajo Seguro. Este año nos sumamos a la campaña regional con CSIRTAmericas, con la que compartimos consejos de ciberseguridad. ¡Estamos convencidos que entre más personas y organizaciones se sumen a este objetivo tendremos más usuarios ciberseguros!

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