Vol. Nº 1
Julio/2020
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

Riesgos CIBERNÉTICOS del COVID 19

Padres Empoderados
¨Internet segura para niños¨

Cooperación Internacional
Israel: Yigal Unna

Tendencia Digital
¨Teletrabajo¨

Comunidad Hackers
¨Hacktion¨

Legal: Dominios Web
El dilema de la inscripción de los nombres de ¨Dominio .cl¨

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
- INCOPORACIÓN 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

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

El esfuerzo multidisciplinario detrás de esta publicación es testimonio, por un lado, de una forma de trabajo en equipo que se ha consolidado entre los profesionales que conformamos el CSIRT, y por otro, del enorme aprendizaje acumulado fruto de las excepcionales circunstancias a las que nos hemos enfrentado en este último año y medio.

En este corto tiempo hemos enfrentando diversos retos internos, locales e internacionales. La experiencia ganada es incomparable. Hoy, somos capaces de adaptarnos rápidamente a los nuevos desafíos, una característica fundamental en un equipo de respuesta rápida como el nuestro.

La respuesta técnica que ofrecemos se complementa necesaria y equilibradamente con la concientización. Para nosotros es fundamental fomentar una cultura de ciberseguridad en las oficinas, las aulas, en el hogar y en cada lugar donde se utilice internet.

En CSIRT somos conscientes que las tecnologías están al servicio de las personas, pero sus beneficios no pueden hacer invisible los riesgos y amenazas asociados a su uso.

La concientización no es un valor agregado, sino parte del permanente reforzamiento que debe existir en una entidad que se dedica a promover la ciberseguridad en la sociedad chilena. Es por eso que hemos realizado numerosas charlas y seminarios, y organizado actividades como el Cyberwomen Challenge Chile y el Simposio de Ciberseguridad de la OEA en septiembre pasado.

Nuestra breve historia se nutre no sólo de esfuerzos para coordinar la seguridad cibernética del Estado, la economía y el país en general, también es abundante en esfuerzos permanentes por educar y fomentar buenas prácticas en el uso de las tecnologías. Por esa razón, también hemos fijado en esta revista un nuevo y permanente compromiso en este sentido con la comunidad.

Esta revista debe ser entendida como un esfuerzo concreto y permanente con la ciudadanía para extender esa vinculación con la sociedad.

Hoy, aun cuando muchos factores parecen conspirar en el éxito de los nuevos emprendimientos en medio de la emergencia sanitaria, hemos decidido celebrar un nuevo hito para el ecosistema de la ciberseguridad en Chile, aportando con una herramienta de concientización y educación cívica para la nueva sociedad digital que estamos creando en el contexto de la cuarta revolución tecnológica en la que vivimos.

EDITORIAL

Juan Francisco Galli Basil
Subsecretario del Interior

Mientras los principales esfuerzos del Gobierno se concentran en frenar el Coronavirus con un conjunto de políticas públicas sanitarias, económicas, laborales y humanas, nosotros como Estado, así como la industria y el mercado, no podemos ignorar los riesgos cibernéticos asociados a esta crisis.

Lo cierto es que Covid-19 encontró a personas mejor preparadas que a otras en cuanto a la seguridad cibernética. En el último tiempo, migramos al teletrabajo como alternativa para la continuidad de muchas actividades de la economía. Ese cambio puso a prueba nuestro real compromiso con la ciberseguridad, un tema en el que todos parecemos estar de acuerdo, pero en el que no siempre estamos dispuestos a invertir.

Lamentablemente, los cibercriminales no tienen compasión, lo que queda en evidencia con nuestras estadísticas que muestran un aumento de la creación de sitios fraudulentos y ataques de phishing, utilizando la crisis sanitaria como asunto. De esta manera, se consuman múltiples ataques contra la disponibilidad de los servicios en sitios web del sistema de salud, demostrando una carencia de humanidad tan vergonzosa como los actos criminales que buscan obtener ganancias económicas.

La buena noticia es que contamos con una respuesta profesional y multidisciplinaria frente a las crisis. El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) es un enorme apoyo y guía en el proceso de virtualización de las relaciones humanas. El CSIRT nos advierte de las amenazas que emergen diariamente en el mercado. Todos los días nos informa de nuevos sitios fraudulentos, campañas de phishing, malware y ransomware. Además, nos proporciona información oportuna para actualizar las diferentes herramientas que abundan en el mercado, y constantemente nos entrega estadísticas que reflejan el estado de la seguridad cibernética en nuestro país.

Depende de nosotros disminuir las brechas de seguridad. La gran tarea por delante es adoptar las buenas prácticas de las oficinas en nuestros hogares. Los dispositivos son utilizados por personas y si no nos comprometemos a su uso cuidadoso, ponemos en riesgo negocios, empleos y los servicios públicos. Para esto, el CSIRT dispone de una serie de protocolos e instrumentos de comunicación como esta revista que estamos seguros se volverán lecturas necesarias.

Este primer número de Cibersucesos, que tengo el gusto de presentar, contiene un interesante análisis de los riesgos cibernéticos asociados al Covid-19, demostrando la indolencia criminal al crear sitios fraudulentos y campañas de phishing. Además, se aborda la complejidad de la relación cotidiana de padres e hijos frente a la mayor exposición a internet. Así también, tenemos el gusto de compartir en este número la colaboración de uno de nuestros socios estratégicos en seguridad cibernética: el INCD de Israel, en las palabras de su Director Nacional, quien analiza la ciberseguridad y la colaboración de ambos países a través de sus equipos de seguridad cibernética. Finalmente, presentamos los esfuerzos de la comunidad hacker de la Universidad Federico Santa María, que desde las aulas están desarrollando una contribución al futuro de este campo.

Riesgos CIBERNÉTICOS del COVID 19

“fraudes y desinformación”
Cómo los cibercriminales toman ventaja de la pandemia:

Con la misma rapidez que el Coronavirus se expande, las campañas de phishing, los sitios de fraude y las noticias falsas se multiplican en internet. Los cibercriminales no han mostrado compasión ante la preocupación y el dolor ajeno, utilizando la búsqueda de información como motivo para sus estafas. Gobiernos y agencias de ciberseguridad en todo el globo se esfuerzan por contenerlos, pero la tarea es difícil cuando la amenaza está a un clic de distancia.

La amenaza

Una de las primeras entidades que a nivel global advirtió de la acción de los cibercriminales fue la Organización Mundial de la Salud. Correos y mensajes de WhatsApp con enlaces y archivos maliciosos en que citaba el contenido del asunto se masificaron en cada nación en la medida que su población era afectada por la enfermedad. En febrero de 2020, la OMS envió un mensaje a los gobiernos dando cuenta de campañas de phishing que, a nombre del organismo, solicitaban información personal o derivaban a enlaces fraudulentos.

Si el Coronavirus ya representa un riesgo para la salud y la seguridad de individuos, familias y organizaciones, las amenazas cibernéticas asociadas a la pandemia pueden resultar en un daño financiero irreparable para las personas y las sociedades que avanzan a una recesión económica mundial.

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

La pandemia ha beneficiado doblemente este tipo de fraude. Primero, porque el encierro, voluntario o forzado, nos lleva a utilizar los correos electrónicos con mayor frecuencia, aumentando la posibilidad de que un fraude sea perpetrado. Y segundo, debido a que el Coronavirus es el principal tema de discusión y búsqueda en internet, por lo que el desconocimiento permite que una serie de mitos y mentiras se propaguen con facilidad. En ambos casos, nos llega información falsa elaborada por los cibercriminales y que envían a nuestras bandejas de entrada, tratándonos de convencer de entregar información, ir a un enlace o descargar algún archivo. Un ejemplo de cómo el encierro y la desinformación ayudan a crear el ambiente para la estafa, se puede extraer de un correo de phishing donde el atacante se hace pasar por el Banco de Chile, uno de los bancos con mayor reputación y con más clientes en el país. El mensaje destaca el compromiso de la entidad bancaria con la salud y llama a las personas a quedarse en casa, para evitar aglomeraciones en las sucursales bancarias mientras dure la crisis. Para ello, se usa como señuelo un enlace que permite autorizar la poster postergación del pago de créditos y otros servicios.

El phishing no llega sólo por correos. En general, varía de acuerdo a la tecnología a través de la cual se propaga. Por ejemplo, existe el **vishing** que consiste en una estafa que se realiza vía teléfono y el **smishing** que se realiza por mensaje de texto.
Un ejemplo de smishing que ha circulado últimamente, asociado a la cuarentena, imita al servicio de streaming Netflix, ofreciendo cuentas gratuitas por medio de un enlace, entendiéndose, para sobrellevar mejor el período de cuarentena.

Hay otros tipos de ataques más específicos, como el spear phishing. Éste se produce cuando el ataque es dirigido a un individuo específico, como el CEO de una organización, con el fin de apropiarse de credenciales, información confidencial o esparcir malware en un sistema. Otra variación del phishing es el malware-phishing. Su método es similar a un phishing, pero siempre su principal objetivo es que la víctima, al ingresar a un enlace o descargar un archivo, ejecute un malware con contenido malicioso.

Para identificar este tipo de ataques es bueno seguir algunas recomendaciones, entre ellas: asegurarse de la autenticidad del remitente del correo;

- Que la ortografía sea apropiada, especialmente si dice provenir de una institución seria.
- Que el contenido no sea alarmante.
- Rechazar el correo cuando solicite contraseñas o información personal. Por lo general, ninguna institución solicita este tipo de datos a través de esta vía.
- No ingresar a enlaces adjuntos ni descargar archivos y
- Siempre descartar correos que no estén personalizados, pues podría tratarse de una estafa masiva.

Sitios Fraudulentos:

La mayoría de los phishing necesitan de un sitio fraudulento para cometer una estafa y en internet este tipo de sitios abundan. Estas páginas se caracterizan, en la mayoría de los casos, en imitar cada detalle del portal oficial de una marca, producto o entidad conocida. Las copias suelen ser imperceptibles para los usuarios, especialmente para aquellos que no pierden mucho tiempo en revisar detalles y son precisamente esos detalles los que hacen la diferencia.
Por esto, prestar atención a los detalles es la primera recomendación que podemos compartir, especialmente en la URL o la barra de dirección. Tener la buena costumbre de ver la dirección podría librarte de una estafa.
Otra forma de discriminar rápidamente un sitio legítimo de uno falso, es revisando que el Protocolo Seguro de Transferencia de Hipertexto (HTTPS) sea seguro. Si el sitio antes de la dirección comienza con "http", puedes descartarlo inmediatamente. Si por el contrario, inicia con "https", puede ser más seguro, pero aún necesitas verificar otros detalles, pues lamentablemente los criminales evolucionan y están obteniendo certificados gratuitos para sus web fraudulentas.
Por último, recomendamos una herramienta del popular navegador Google para revisar la seguridad de un sitio: Google Safe Browsing, un sitio que permite identificar una página fraudulenta. Sólo tienes que agregar la dirección web en la que estás navegando y te avisará si se han encontrado contenidos seguros o no.

Fake news o Noticias falsas:

Lamentablemente, el temor y la incertidumbre que ha generado el Coronavirus es un campo fértil para sembrar confusión entre la internet. Los atacantes crean contenidos alarmantes o extraordinarios para capturar la atención de sus víctimas, dificultando el acceso a la información verídica.
El envío de un correo con noticias impactantes sobre la enfermedad tiende a viralizarse rápidamente, generando falsa alarma, daños emocionales y pérdidas económicas entre las personas. Por suerte, tienen características que permiten diferenciarlas de una noticia fidedigna.

El CSIRT recomienda:

- **Siempre revisar la fuente de la información.** Toda noticia o información verídica tendrá de respaldo una investigación o citará fuentes.

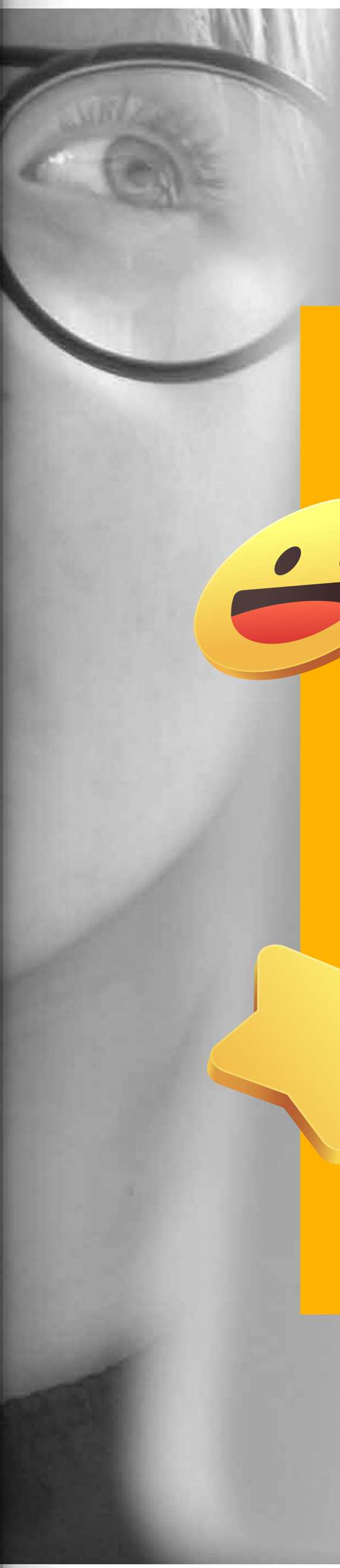
- **Revisar los errores gramaticales y de redacción.** Si algo dice provenir de una entidad seria y está en un lenguaje coloquial para referirse a la crisis o si tiene errores gramaticales u ortográficos significativos, tómalo inmediatamente como falso.

- **No hay noticias exclusivas por correo.** Las noticias reales se reproducen en diferentes medios públicos. Una simple búsqueda por más detalles en otros portales debería llevarnos a más información sobre el tema.

- **No reveles Información personal o financiera.** Si lo piensas bien, no tiene sentido que un correo sobre el coronavirus te pidan información personal y bancaria.

- **Ser escépticos al navegar por internet**, especialmente si los consejos o información vienen de fuentes que no son las oficiales, la cura del Coronavirus no te llegara por correo.

Los gobiernos y organizaciones de salud están realizando esfuerzos para protegernos y debemos confiar en la información que nos reportan. Son los medios de comunicación formales, por contraparte, quienes deben examinar en profundidad esa información. Con esos elementos podemos llegar a un grado de certeza en medio de esta pandemia.



PADRES EMPODERADOS

Internet segura para niños:

El desafío cibernético de la cuarentena

En el mundo, más de 1.500 millones de estudiantes han sido afectados con el cierre parcial o total de los establecimientos educacionales a causa de la propagación del Coronavirus. Como consecuencia, la mayoría de los menores deben continuar sus estudios en línea, lo que les permite estar más tiempo conectados a Internet. ¿Sabes qué hacen tus hijos durante todo ese tiempo?

De la noche a la mañana, el encierro en los hogares se ha vuelto la norma para contener el Coronavirus. La mayoría no tuvo mucho tiempo para planificarse y han tenido que adaptarse a una rutina donde los espacios físicos son limitados. Para las familias, en especial con niños, combinar el trabajo con la supervisión de los hijos y la mantención del hogar, requiere de mucho tiempo, esfuerzo y paciencia. Si a eso sumamos la preocupación por el virus, el desafío puede ser abrumador. Para muchos, especialmente para los padres, la solución a muchos aspectos de esta crisis ha sido el internet. Su uso se ha vuelto una alternativa para seguir con los trabajos, pero también es la posibilidad de que los hijos puedan continuar sus estudios.

En este punto, probablemente muy relevante para los padres, debemos considerar que existen diversas herramientas para intentar darle continuidad a los estudios para los jóvenes y niños. Es así, como el Ministerio de Educación cuenta con una plataforma digital gratuita para que los estudiantes puedan acceder a material pedagógico complementario para profundizar el contenido de las distintas materias, como matemáticas, física, lenguaje, ciencias, entre otras.

Los contenidos se suben semanalmente y podrás descargar el material y textos escolares. Sólo debes ingresar a www.aprendoenlinea.mineduc.cl
Por otra parte, la Unesco ofreció un listado de aplicaciones y plataformas educativas para ayudar a toda la comunidad escolar a propiciar el aprendizaje de los alumnos. Algunas de ellas son:

Blackboard
CenturyTech
ClassDojo
Edmodo
EkStep
Google Classroom
Seesaw

No se pueden negar los beneficios de la tecnología. Sin embargo, el estar largos períodos de tiempo conectados tiene sus riesgo, quizás imperceptibles a la vista de los padres, pero que tampoco debemos ignorar. Contenido inapropiado o falso, ciberbullying (abuso sostenido entre escolares a través de las redes sociales), robo de información y grooming (acoso y abuso sexual online), son algunas de las amenazas que están en internet.
Si eres papá o mamá, aquí te ofrecemos un kit de recomendaciones para que tomes el control en esta desafiante realidad y permitir que tus hijos estén conectados y seguros en línea.

LAS SOLUCIONES ESTÁN EN TI

Para tomar el control y sortear exitosamente las amenazas cibernéticas, lo primero es estar informados. Las redes sociales son unas de las plataformas más peligrosas para los jóvenes, ya que el ciberbullying está muy presente, por lo tanto el reto es conocer un poco más sobre las tecnologías y aplicaciones que usan tus hijos y sus amistades.
Este paso implica iniciar una conversación con ellos para que te cuenten qué ven en internet, cuáles son sus juegos favoritos e interesarte por sus gustos. Pero también es una oportunidad para decirles que pueden acudir a ti en busca de ayuda si tienen alguna inquietud. Quizá ellos puedan tener más conocimiento de las tecnologías que tú, pero tú tienes más experiencia en la vida para guiarlos.

Por eso, si la conversación prospera, aprovecha de establecer ciertos límites sobre los tiempos y lugares para usar los dispositivos. Para esto, el Equipo de Respuesta Ante Incidentes de Seguridad Informática, CSIRT, elaboró una propuesta de "Acuerdo Familiar", para que padres e hijos puedan convenir en el uso de las redes sociales e internet de forma segura. Puedes descargarlo en **https://www.csirt.gob.cl/recomendaciones/acuerdo-familiar/** en la sección de recomendaciones.

Otra solución es utilizar herramientas de control parental que permitan tener un registro de las actividades que realizan tus hijos en los dispositivos móviles o plataformas de streaming. Existen varias aplicaciones disponibles para Apple y Android, las que de acuerdo al plan que se contrate o la aplicación que se descargue es posible bloquear sitios web o aplicaciones, definir el tiempo que podrán estar conectados e incluso recibir alertas.

Otra alternativa es ingresar a:
www.net-aware.org.uk ("Netaware") que clasifica los juegos y apps aportando a los padres una calificación del riesgo de cada una de ellas.

- **Si autorizas a que tus hijos tengan alguna red social, lo recomendable es abrir juntos el perfil, configurar las opciones de privacidad, negociar el tipo de contenido que subirán y crear una contraseña segura.**
- **Si sabes que tu hijo sufre de ciberbullying, lo primero que debes hacer es contenerlo emocio nalmente, jamás culparlo. Lo mejor es asesorar se y buscar ayuda en el colegio para que lo guíen en cómo debe actuar.**
- **Si tu hijo juega en línea asegúrate de hablar para que nunca entreguen información perso nal, ni tampoco su ubicación.**
- **Instala un analizador de antimalware móvil acreditado y mantén actualizado el antivirus.**

COOPERACIÓN
internacional

CSIRT tiene la responsabilidad de ejecutar los acuerdos de cooperación suscritos por el Estado de Chile en materia de seguridad cibernética. Esta acción se realiza a través de herramientas para compartir indicadores de compromisos, el perfeccionamiento de profesionales o el intercambio de conocimiento sobre los modelos tecnológicos implementados en los diferentes países. Esta primera edición de Ciber Sucesos dedica esta columna al intercambio entre los Equipos de Respuesta de Israel y Chile, y su futuro.

Yigal Unna
Director General de la Dirección Nacional de Ciberseguridad de Israel (INCD)

Anteriormente sirvió como jefe ejecutivo de la unidad de tecnologías de Ciberseguridad del INCD. Tiene tres décadas de experiencia en el aparato de seguridad de Israel, ocupando diversas posiciones en el sistema de ciberinteligencia ,operaciones, investigación y desarrollo, junto con el desarrollo de políticas.

La cibernética como motor de crecimiento. Donde la necesidad se encuentra con la oportunidad.

Yigal Unna, Director General, Dirección Nacional Cibernética de Israel

Se espera que la industria cibernética israelí rompa más récords este año, en términos de inversiones de capital y datos de exportación. Los informes finales de 2019 aún no se publican, sin embargo, demostrarán que más de 540 compañías cibernéticas son responsables de 6.5 mil millones de dólares de exportación, y recibirán más de 1.5 mil millones de dólares en inversiones. Además, los nuevos datos de la encuesta global de "Cyber Security Ventures" clasifican a Israel como el segundo a nivel mundial en el número de compañías cibernéticas más exitosas, justo después de los Estados Unidos.

Según esta encuesta, 18 compañías cibernéticas israelíes se encuentran entre las primeras 150 compañías cibernéticas más prometedoras del mundo. Estos hechos colocan a Israel como uno de los 5 principales países líderes en la promoción de soluciones de seguridad cibernética y ponen énfasis en la importancia de la participación del gobierno en el desarrollo y fomento de esta valiosa industria. Con el fin de comprender mejor el interés nacional aquí, deberíamos explorar más a fondo las características de la cibernética.

La cibernética tiene tanto un aspecto de seguridad nacional como civil. En su aspecto cívico-social, la seguridad cibernética ha evolucionado en paralelo al progreso tecnológico que afecta cada vez más nuestra vida cotidiana; La inteligencia artificial (IA), está cambiando las reglas del juego en cibernética, y cuanto más se expande el progreso y la dependencia tecnológica, la amenaza cibernética evoluciona y la necesidad de soluciones avanzadas de seguridad se profundizan; La necesidad de dar seguridad al Internet de las cosas (IOT),con autos inteligentes y otras aplicaciones de inteligencia artificial duplicarán la demanda mundial de soluciones de regulación y seguridad en la próxima década.

De hecho, esta es una oportunidad para que cualquier economía desarrolle e implemente soluciones que los pongan en un nivel más alto de seguridad, haciéndolos más competitivos, y la industria cibernética israelí tiene mucho que ofrecer a ese respecto.

Cuando observamos el ámbito internacional desde una perspectiva de Seguridad Nacional, notamos que el Dominio Cibernético se está utilizando como un medio atractivo, disponible y relativamente barato para lograr los objetivos de los Estados y Organizaciones dedicadas a generar terror en la sociedad.

La cibernética es un dominio bipolar en el sentido de que su poder tecnológico se basa tanto en el sector público como en el sector privado. Por un lado, la I + D, la experiencia y los recursos fluyen de la comunidad de Seguridad y Defensa, pero por otro lado también provienen del sector industrial privado. Ambos sectores son atractivos y dependen uno del otro a largo plazo.

Este puzzle de características demuestra la necesidad de una industria cibernética fuerte y próspera por el bien de la seguridad nacional y la economía. La cibernética es un motor de crecimiento, y un componente esencial en la diplomacia moderna y la disuasión nacional, además de ser la piedra angular para la resistencia de la Infraestructura crítica nacional que permite la prosperidad y la operación continua de los negocios.

Las características especiales del Dominio Cibernético requieren una perspectiva novedosa, diferente a otros campos tecnológicos.

La Dirección Nacional de Cibernética de Israel-INCD tiene como objetivo asegurar que la industria tenga los recursos necesarios, como mano de obra calificada, infraestructuras de I + D y demás, para continuar floreciendo. Los gobiernos deben esforzarse por conectar mejor los activos, recursos y conocimientos relevantes del sector público, el sector privado y la Academia, a fin de maximizar el uso de todo su potencial.

Según la encuesta de IVC, a la economía israelí le faltan unos 800 hombres y mujeres en el área cibernética. Estoy seguro de que Chile e Israel están compartiendo una brecha similar en Recursos Humanos. El INCD está trabajando para cumplir con los programas de desarrollo de capacidades en cibernética y tuvimos la suerte de recibir a ciberprofesionales del CSIRT del Gobierno chileno en un curso internacional que tuvo lugar recientemente en nuestro CERT nacional. Constantemente buscamos tecnologías emergentes y nuevas bases como 5G, IA, seguridad cibernética de aviación, seguros cibernéticos, seguridad cibernética de salud, puertos, seguridad en la nube y más, explorando formas de mejorar e integrar la seguridad cibernética.

La Inteligencia Artificial introduce un crecimiento exponencial de las amenazas y se hace eco de la necesidad de enfrentarlas con urgencia. Nuevas capacidades de ataque, mayor tasa de ataques por automatización y la experimentación de nuevos vectores de ataque son solo algunas de las amenazas en evolución. Sin embargo, el uso de IA es la clave para enfrentar estas amenazas.

La nueva tecnología permite una identificación más rápida de anomalías, conecta los puntos y ensambla rápidamente el panorama general, permitiendo sistemas más protegidos y seguros.

El ambiente de amenaza es común en muchos países, e Israel como Chile enfrentan ataques similares. Seguimos comprometidos a trabajar juntos para compartir información y mejores prácticas y tácticas para asegurar nuestras Naciones. Altos funcionarios chilenos visitaron Israel para discutir y promover la cooperación, e Israel se compromete a cooperar con Chile para mantener y mejorar la Seguridad Cibernética en beneficio de las personas y economías. Esto no solo por necesidad, también implica la oportunidad de un futuro mejor donde la economía y la seguridad se apoyan mutuamente.

TELE
TRABAJO

Trabajadores lejos, conectadas de forma cibersegura

En muy poco tiempo y prácticamente sin previo aviso, algunas organizaciones debieron adaptarse a una nueva forma de trabajar y cambiar diversos aspectos: desde acomodar el nuevo lugar de trabajo hasta la forma de hacer reuniones. Y si bien el teletrabajo impacta positivamente en la continuidad del empleo, también hay algunos riesgos cibernéticos que se deben tener en cuenta.

En noviembre de 2018, de acuerdo a un estudio encargado por el Ministerio del Trabajo a Cadem, el 81% de las personas estaban dispuestas a trabajar desde su casa, y quién iba a pensar que un virus sería el responsable de que un importante porcentaje de la población hoy esté realizando teletrabajo.

En este sentido, la tecnología cumple un rol importante para estar conectados y poder lograr realizar las funciones de la mejor manera posible y sin riesgos. Los peligros en el ciberespacio son variados y están relacionados con el entorno en que te desempeñas, es decir, si usas tu computador personal y no cuentas con antivirus o no mantienes el software actualizado, hay mayor probabilidad de infectar el dispositivo y como consecuencia la red interna de la organización.

Así también, existen otras amenazas, como: acceso accidental a información sensible por parte de familiares o amigos que estén en el mismo domicilio o menor control de descarga de programas o archivos con malware, que provengan de campañas de phishing.

Para prevenir estos riesgos y lograr mantener una continuidad laboral segura es importante seguir las políticas y cumplir los protocolos establecidos por la organización donde te desempeñas. Complementariamente, te entregamos algunos consejos que ayudarán a las empresas y a funcionarios a estar más ciberseguros.

Si eres trabajador **TEN EN CUENTA:**

- Evitar conectarse a internet desde una wifi pública a la red institucional.
- Desconfiar de los correos electrónicos que recibes, especialmente aquellos relacionados con el Coronavirus. Las estafas por phishing han aumentado desde que llegó la pandemia a nuestro país, así que sé crítico con la información que recibes.
- Revisar las políticas de seguridad de información interna del lugar donde trabajas, como el uso de los dispositivos móviles, los equipos personales o la política de escritorio limpio.
- Si usas un equipo compartido en tu casa, lo ideal sería que puedas crear un perfil nuevo específico para trabajar, con el fin de evitar que otras personas accedan a tu información.
- Mantener actualizado el antivirus, software y sistemas operativos.
- Recuerda siempre respaldar tu información.

A LAS EMPRESAS LES **RECOMENDAMOS:**

- **Utilizar una conexión VPN**, ya que permite establecer una conexión remota segura (encriptada) a la red institucional. En caso de necesitar múltiples VPN, se aconsejan conexiones VPN personalizadas sólo para tomar control remoto del equipo asignado al interior de la institución y utilizar los permisos de acceso ya asignados a dicho equipo.

- **Establecer medidas para evitar el acceso** de forma fortuita a información institucional por otros usuarios del equipo del funcionario, como familiares o amigos.

- **Utilizar equipos institucionales con los resguardos** de seguridad correspondientes: antivirus reconocido y actualizado, sistema operativo licenciado y con sus parches al día, y aplicaciones licenciadas y actualizadas.

- **Contratar servicios de videoconferencia con niveles** de seguridad alto para la sustitución de reuniones presenciales.

- **Establecer una definición del trabajo permitido**: clasificación de información, sistemas y servicios internos a los que está autoriza el teletrabajador.

- **Aplicar la lógica de respaldo de la información** en este nuevo escenario.

- **Establecer medidas de seguridad como doble factor** de autenticación tanto en el correo institucional como en las plataformas que se utilizan para trabajar.

- **Verificar los accesos a sistema o plataformas** según el rol que posea cada trabajador.

- **Revisar la política de seguridad para la conexión** de forma segura de externos.

- **Establecer la revocación de autoridad y derechos de acceso** y la devolución de los equipos cuando concluyen las actividades de trabajo a distancia.

Que el teletrabajo se realice bajo un ambiente Ciberseguro,es responsabilidad de todos.

COMUNIDAD
HACKERS

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
LÍDER EN INGENIERÍA, CIENCIA Y TECNOLOGÍA

CSIRT QUIERE ESTIMULAR A LOS NUEVOS TALENTOS QUE SE ESTÁN FORMANDO EN LAS UNIVERSIDADES CHILENAS EN MATERIA DE SEGURIDAD INFORMÁTICA, PARA INVOLUCRARLOS EN EL PROGRESO CIBERNÉTICO DEL PAÍS Y FOMENTAR UN ECOSISTEMA DE SEGURIDAD ENTRE EL ESTADO Y LA SOCIEDAD. ESTA COLUMNA ESTÁ DEDICADA A DESTACAR A LOS HACKERS CHILENOS Y SUS EMPRENDIMIENTOS EN EL ÁMBITO DE LA CIBERSEGURIDAD.

En la actualidad, la ciberseguridad tiene un rol relevante. Tanto es así, que paulatinamente en las universidades han ido surgiendo equipos de estudiantes apasionados por la cultura hacker, quienes buscan potenciar sus habilidades en materias de seguridad informática, mediante entrenamientos y desafíos para el desarrollo de la ciberseguridad, integrando principios éticos.

Uno de estos equipos es 'Hacktion', un grupo de siete estudiantes de Ingeniería Civil Informática de la Universidad Técnica Federico Santa María de Valparaíso (UTFSM), compuesto por: Álex Jara, Fabián Da Silva, Víctor Torres, Carina Flores, Pablo Aravena, Rodrigo Gómez y Gabriela Sepúlveda. CSIRT estuvo con los integrantes de Hacktion para saber cómo se preparan y cuáles son sus proyectos. En esta interesante conversación nos contaron sobre "Campo de Marte", una actividad dirigida a la comunidad académica de la V Región que privilegia e incentiva los entrenamientos y ejercicios para el desarrollo de la ciberseguridad con fuertes principios éticos, y en la que este grupo de estudiantes participó en tres ediciones durante el año 2019. Los ejercicios consisten en el enfrentamiento CTF (Capture the Flag), desafíos informáticos enfocados en la seguridad, y donde se ponen a prueba los conocimientos y se aprenden nuevas técnicas. Las pruebas son de carácter formativo y de preparación. A medida que van pasando las tareas, el grupo recibe una bandera con un puntaje, mientras más alto el puntaje aumenta el nivel de complejidad.

"No fue fácil en un principio, ya que ninguno de nosotros tenía experiencia en este tipo de actividad, sin embargo logramos superar bien los desafíos y cada logro ha ido despertando nuestras ganas de seguir aprendiendo. Por esta razón, como Hacktion nos hemos propuesto para este año empezar a realizar investigaciones y crear una comunidad de ciberseguridad en la carrera de Informática de la UTFSM, con el fin de dar a conocer el área a más estudiantes".

Por su parte, la UTFSM tiene un fuerte compromiso social con el desarrollo de la ciberseguridad, por lo que dentro de sus proyectos se destacan:

- Acuerdo de cooperación con la PDI, para que los estudiantes puedan desarrollar sus memorias en materias relacionadas con el cibercrimen y crear un laboratorio de análisis de malware que sea útil para toda la comunidad.
- Desarrollar un laboratorio de ciberseguridad para que los estudiantes puedan practicar habilidades.
- Continuar con el desarrollo de charlas, talleres y entrenamientos.
- Generar contenido de formación para ser distribuido entre los colegios de la región, para fomentar las buenas prácticas del uso de Internet y la tecnologías de información.

ES IMPORTANTE RECALCAR QUE ESTE TEMA NO SE QUEDA EN TAN SOLO CREAR EQUIPOS QUE COMPITAN EN LOS DESAFÍOS MENCIONADOS, SINO QUE TAMBIÉN ES FUNDAMENTAL COMPARTIR ESTOS CONOCIMIENTOS PARA CREAR CONSCIENCIA EN LA COMUNIDAD, YA QUE UNO DE LOS MAYORES DESAFÍOS QUE TRAE CONSIGO LA TRANSFORMACIÓN DIGITAL ES LA MISIÓN DE GENERAR UN CAMBIO CULTURAL BASADO EN CIBERSEGURIDAD.

El dilema de la inscripción de los nombres de **DOMINIO.CL**

Fraude o Negocio

Registrar un nombre de dominio similar al de una Institución u organismo es un hecho que va en aumento, sin embargo el objetivo que persigue su inscripción es cuestionable. En ocasiones, sólo buscan dirigir el tráfico a otro portal, pero también hay ciberdelincuentes que lo hacen para replicar los sitios web para confundir o engañar a las personas.

Contar con un sitio web en la actualidad es una necesidad para las empresas. Con el paso de los años y la incorporación de nuevas tecnologías se han vuelto cada vez más imprescindibles para tener presencia en el mercado digital. El beneficio de esta nueva forma de posicionamiento es tanto para los clientes como para las organizaciones. Gracias a las páginas web, las personas pueden hacer trámites de forma más rápida, realizar cualquier tipo de compra, obtener información de la empresa, en fin, los beneficios abundan.

Y para lograr que los potenciales clientes lleguen al sitio esperado, lo primero que se debe hacer es contar con la marca online, registrando el nombre de dominio. Y es aquí cuando a veces comienza el conflicto, ya que en algunos casos se registran nombres similares al de una institución u organismo. Esto se conoce como "cybersquatting o ciberocupación" y es la acción de registrar de mala fe un determinado nombre de dominio que simula a uno legítimo, para posteriormente traficar con él o hacer uso con fines fraudulentos.

En este último punto, cabe destacar que la creación de los sitios fraudulentos permite a los ciberdelincuentes generar campañas de phishing, con el fin de robar credenciales, tarjetas bancarias o alojar malware en los equipos y así acceder a información de la persona o una empresa.

La propagación del Coronavirus ha propiciado también la inscripción de más de mil nombres de dominio relacionados con la enfermedad **(.NET; .COM; .ORG; .CL y .INFO),** sólo en marzo de este año, según datos recopilados por el **CSIRT y CCN CERT** de España.

¿EL OBJETIVO? En algunos casos se desconoce, otros buscan entregar información útil, mientras que un gran porcentaje de ellos sólo quieren aprovecharse de la necesidad de las personas de informarse y encontrar una explicación sobre lo que está pasando.

¿**Qué hacer** si se registra un nombre **de dominio similar al mío**?

Existe una alternativa para solicitar revocar un nombre de dominio. La Organización Mundial de Propiedad Intelectual gestionó en el 2018, 5.655 controversias de nombres de dominio en distintos países del mundo. En Chile, esto no es un tema ajeno y también contamos con una entidad que se encarga de resolver este tipo de controversias para los dominios .CL: NIC Chile.
En caso de que una persona considere que ha sido afectado por la creación de un sitio, puede iniciar un trámite llamado "procedimiento de revocación", que se resume en los siguientes pasos:

1.– Se presenta un conflicto de nombre de dominio de nivel superior geográfico (.CL)

2.– Se debe realizar la solicitud de revocación del nombre de dominio inscrito.

3.– Para llevar a cabo la revocación se debe ingresar al sitio web **www.nic.cl**

- **a)** Se ingresa a la sección de controversia.s
- **b)** Ingresar solicitud.
- **c)** Ingresar nombre de dominio que se pretende revocar y motivo de controversia.
- **d)** Ingresar datos de individualización del solicitante.

4.– Con el registro, se crea el expediente de arbitraje electrónico y comienza la etapa "tachas" (se presentan los árbitros disponibles) y el "nombramiento del árbitro" (el árbitro acepta el nombramiento)

5.– Una vez aceptado el arbitraje, se efectúa la consignación de los honorarios. Si esto no ocurre, se termina el conflicto y el dominio mantiene su consignación al actual titular.

6.– Por el contrario, si se efectúa la consignación de los honorarios se el cómputo del plazo para presentar la demanda. El plazo es de 5 días contados desde la notificación de la resolución.

7.– Presentada la demanda, la contraparte tendrá un plazo de 10 días corridos para contestar.

8.– El juez tiene 20 días corridos para resolver si mantiene el nombre de dominio a nombre de su actual titular o pasa a pertenecerle al revocante.

Plazos para revocar un nombre de dominio

LA ACCIÓN DE REVOCACIÓN TEMPRANA procede cuando se invoca por el revocante un interés preferente y el único requisito es presentar la solicitud de revocación, dentro del plazo de 30 contados desde que se registró el nombre de dominio

LA REVOCACIÓN ES TARDÍA procede cuando se solicita con posterioridad a los 30 días desde que se ha inscrito el nombre de dominio disputado, invocando una inscripción abusiva, *bajo los siguientes criterios

- Que el nombre de dominio sea idéntico o engañosamente similar.
- Que el asignatario del nombre de dominio no tenga derechos o intereses legítimos.
- Que el nombre de dominio haya sido inscrito o se utilice de mala fe.

Una forma de cuidar el ciberespacio y disminuir las amenazas radica en la importancia de que los dueños de sitios web estén atentos a la creación de portales similares a los suyos, de manera de poder realizar el proceso de revocación rápidamente y así evitar que los cibercriminales cometan más estafas.

Por esto, queremos hacer hincapié en el plazo de revocación temprana, es decir, dentro de los 30 días desde que se inscribió el nombre en NIC Chile, ya que al tener pocos días de inscripción los atacantes podrían tienen menos opción para cometer algún delito.

El CSIRT cuenta con un Manual de Resolución de Conflictos por Nombres de Dominio en .CL, al que puede consultar tanto una persona natural como jurídica. Encuéntralo y descárgalo en **https://www.csirt.gob.cl/reportes/manual-de-dominio/**

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/
CSIRT en Inglés
https://www.csirt.gob.cl/eng/

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/simposiochile/

CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

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

Colaboradores equipo CSIRT:
Natalia Perez
Carolina Covarrubias
Carlos Silva
Patricio Quezada

Diseño y diagramación: Blackbook

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