CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 247

semana del 22 al 27 de marzo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

1

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

2

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

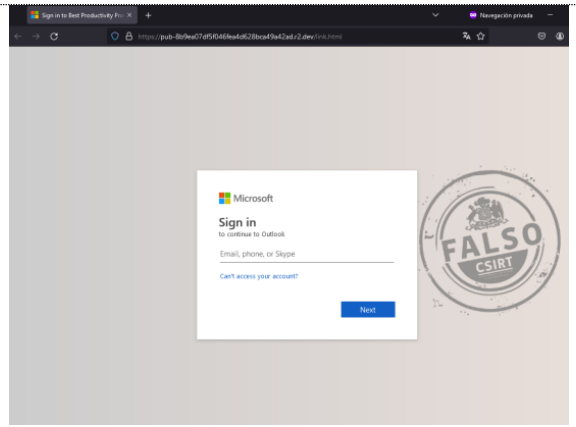
1

Las mitigaciones son útiles en productos de Apple.

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos



CSIRT alerta de nuevo sitio fraudulento que suplanta a Microsoft	
Código de alerta	8FFR24-01674-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 marzo, 2024
Última revisión	25 marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://pub-8b9ea07df5f046fea4d628bca49a42ad.r2[.]dev/link.html	
URL de redirección	
https://t[.]co/7y3BBFk0do	
Dirección IP sitio falso	
[104.18.3.35]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01674-01/	

2. Vulnerabilidades

CSIRT comparte información de nueva vulnerabilidad parchada por Apple	
Código de alerta	9VSA24-00991-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 marzo, 2024
Última revisión	26 marzo, 2024
CVE	
CVE-2024-1580	
Fabricante	
Apple	
Productos afectados	
iOS, iPadOS, Safari, visionOS y macOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00991-01/	

4. Noticias y concientización

Gobierno promulga nueva Ley Marco de Ciberseguridad

Este 26 de marzo, en el Palacio de La Moneda, el Presidente de la República, Gabriel Boric Font, promulgó la nueva Ley Marco de Ciberseguridad, normativa que permitirá robustecer al país en materia de seguridad digital y que crea la Agencia Nacional de Ciberseguridad (ANCI).

La nota completa aquí: https://ciberseguridad.gob.cl/noticias/presidente-boric-promulga-nueva-ley-marco-de-ciberseguridad/.

"Chile se convierte en el primer país de Latinoamérica y el Caribe en tener una Agencia Nacional de Ciberseguridad y un marco regulatorio de vanguardia en este campo. Esta política va a impulsar el desarrollo de la industria de la ciberseguridad en Chile, lo que también es una oportunidad de empleos y de inversión". Estas fueron las palabras el Presidente Boric durante la ceremonia de promulgación de la Ley Marco de Ciberseguridad, que se llevó a cabo el martes 26 de marzo.

Esta actividad marca un hito importante para la ciberseguridad en nuestro país, ya que gracias a la Ley y a la Política Nacional de Ciberseguridad será posible robustecer la seguridad digital de los chilenos. La nueva Ley establece la institucionalidad, los principios y la normativa general que permitirán estructurar, regular y

coordinar las acciones de ciberseguridad de los organismos del Estado, además de instaurar los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad, tanto para el sector público como privado.

La ceremonia, realizada en el Salón Montt Varas del Palacio de La Moneda, contó con la participación de los ministros del Interior y Seguridad Pública, Carolina Tohá; de Relaciones Exteriores, Alberto van Klaveren; de Defensa, Maya Fernández; de Hacienda, Mario Marcel; de la Secretaría General de la Presidencia, Álvaro Elizalde; de Justicia, Luis Cordero; de Ciencias, Tecnología, Conocimiento e Innovación, Aisén Etcheverry; de Transportes y Telecomunicaciones, Juan Carlos Muñoz; y de Energía, Diego Pardow.

La Ministra del Interior y Seguridad Pública, Carolina Tohá, subrayó que "lo que hoy día sucede es fruto de un proceso virtuoso y prolongado que en Chile hemos tenido para enfrentar seriamente los riesgos ligados a la ciberseguridad y los desafíos que ello plantea para el país". La Ministra Tohá recordó que aunque han pasado gobiernos de distintas tendencias políticas, en esta materia se ha avanzado con acuerdos transversales.

ANCI: una agencia autónoma y con verdaderas facultades

La nueva ley establece una nueva gobernanza de ciberseguridad para el país, al crear la Agencia Nacional de Ciberseguridad (ANCI), organismo con facultades regulatorias, fiscalizadoras y sancionatorias, tanto para los organismos públicos como privados.

Algunas de las atribuciones de la ANCI son el asesorar al Presidente en la elaboración de políticas, planes y programas de acción, establecer protocolos y estándares obligatorios tanto para instituciones públicas como privadas, administrar el Registro Nacional de Incidentes, calificar los servicios esenciales y establecer los operadores de importancia vital, requerir información sobre incidentes o antecedentes para prevenir su ocurrencia y promover la educación en ciberseguridad.

Nace también el Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática (CSIRT) Nacional, que dependerá de la ANCI y que entre sus funciones específicas se incluye responder ante ciberataques o incidentes de ciberseguridad relevantes, coordinar a los nuevos CSIRT que se crearán para las distintas ramas del Estado, incluyendo el CSIRT de la Defensa Nacional, colaborar con entidades extranjeras en el intercambio de información, entregar asesoría técnica para la implementación y realización de acciones que permitan una mayor ciberseguridad en las instituciones del Estado, incluyendo capacitaciones y entrenamientos, solicitud de información sobre incidentes y vulnerabilidades, difusión de alertas y elaboración de criterios técnicos para la categorización de incidentes o vulnerabilidades exentas de notificación.

Además, la ley crea el CSIRT de la Defensa Nacional, que dependerá del Estado Mayor Conjunto, y que tiene atribuciones similares al CSIRT Nacional pero en el ámbito de la Defensa. La ley establece la necesidad de ambos CSIRT de colaborar en la protección tanto de las personas como de los "servicios esenciales" del país.

La ley también protege la seguridad de los servicios esenciales, no importando si estos son administrados por el Estado, empresas públicas o privadas, y define los criterios para que la ANCI establezca a los Operadores de Importancia Vital (OIV), con el objetivo de instituir deberes y multas en caso de no cumplirlas.

Entre estas obligaciones de los OIV están la implementación de un sistema de gestión para garantizar la seguridad de la información y la continuidad operativa, el mantenimiento de registros, la realización de planes de continuidad operacional y ciberseguridad, la ejecución de simulacros, ejercicios y análisis de los sistemas informáticos, la adopción de medidas para mitigar el impacto de los incidentes, la comunicación con los afectados, la capacitación y educación continua a trabajadores y colaboradores, y la designación de un delegado para ser el punto de contacto con la ANCI.

Una política nacional organizada alrededor de cinco ejes

En la oportunidad también se presentó la nueva Política Nacional de Ciberseguridad para los años 2023-2028, la que posee los siguientes cinco ejes principales:

1. Infraestructura resiliente: El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos.

2. Derechos de las personas: El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas necesarias para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente.

3. Cultura de ciberseguridad: Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas.

4. Coordinación nacional e internacional: El Estado creará una gobernanza pública para coordinar las acciones necesarias en ciberseguridad. Los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en esta área. En el ámbito internacional, el Estado se coordinará con países, organismos, instituciones y otros actores internacionales para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio.

5. Fomento a la industria y la investigación científica: El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Para ello, fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país.

Con esta nueva Ley Marco y la Política Nacional, el país se pone a la vanguardia de Latinoamérica y el Caribe en términos de política pública sobre ciberseguridad.

Ciberguía por el Día Internacional del Backup

Cada 31 de marzo se celebra el Día Internacional del Backup, y en el CSIRT decidimos compartir nuestra ciberguía para realizar respaldos en algunas plataformas, y así recordar a la comunidad de ciberseguridad sobre la importancia y necesidad de realizar respaldos regularmente y mantenerlos seguros.

La guía completa: ciberseguridad.gob.cl/ciberconsejos/ciberguia-por-el-dia-internacional-del-backup

5. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

5. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Rodrigo Muñoz Emparán
- Alejandro Madero
- Vicente Antonio Maureira Oliva
- Dennis Edgardo Astorga Naduris
- Mauricio Andrés Alarcón jara
- Francisco Jiménez Alcántara
- Pablo Ignacio Pizarro Cortínez
- Hugo Cárcamo Fincheira
- Luis Andres Egaña Valle
- Fernando Enrique Gonzalez Rojas
- Eliu Alonso Figueroa Albarran
- Manuel Alejandro Mejías Sánchez
- Andrés Felipe Barrientos cisternas
- Héctor Prieto Tabilo
- Romel Rivas
- Felipe Agustín Flores Yañez
- Paula García
- Juan Manuel Herrera Acevedo

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.03.28 17:02:04 -03'00'