Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

19-11-2021 | Año 3 | N°124

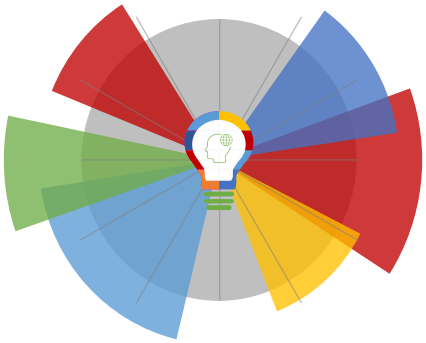
Boletín de Seguridad Cibernética

Semana del 12 al 18 de noviembre de 2021

La semana en cifras

Hash
42
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
9
URL
Asociadas a sitios fraudulentos y campañas de phishing y malware.



Parches
22
para vulnerabilidades
Las mitigaciones son útiles en productos de Citrix, Palo Alto, Intel y Google.

IP
20
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Phishing

CSIRT advierte phishing por una supuesta cuenta bloqueada	
Alerta de seguridad cibernética	8FPH21-00445-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Noviembre de 2021
Última revisión	05 de Noviembre de 2021
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3mHt5Sm?l=www.bancoripley.cl http://piccalugabros[.]it/gestione/inc/enviar02.php?l=2051603265 https://bit.ly/2ZVdSo8?l=www.bancoripley.cl https://stage.stratandtest.ovh/activacion/cuenta-wrbz/	
URL sitio falso	
http://www-bancoripley.cl.fashionbudmagazine[.]com/login	
IP	
[103.92.235.87]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00445-01/	
https://www.csirt.gob.cl/media/2021/11/8FPH21-00445-01.pdf	

Sitios fraudulentos

CSIRT advierte suplantación de página web del Banco Santander	
Alerta de seguridad cibernética	8FFR21-01019-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Noviembre de 2021
Última revisión	15 de Noviembre de 2021
Indicadores de compromiso	
URL redirección	
http://fzbgpcc.cluster051.hosting.ovh[.]net/?email=email	
URL sitio falso	
https://tycconstrucciones[.]cl/1636988179/personas/index.asp	
IP	
[138.117.149.176]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01019-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01019-01.pdf	

CSIRT informa suplantación de sitio web de tiendas Bata	
Alerta de seguridad cibernética	8FFR21-01020-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2021
Última revisión	18 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.batofertas[.]online/	
IP	
[167.160.17.175]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01020-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01020-01.pdf	

CSIRT advierte página falsa para recargar tarjeta Bip!	
Alerta de seguridad cibernética	8FFR21-01021-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2021
Última revisión	18 de Noviembre de 2021
Indicadores de compromiso	
URL sitio falso	
http://recarlabidesdecasita[.]com/recargar/	
IP	
[3.121.141.147]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01021-01/	
https://www.csirt.gob.cl/media/2021/11/8FFR21-01021-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades en productos de Citrix	
Alerta de seguridad cibernética	9VSA21-00520-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2021
Última revisión	12 de Noviembre de 2021
CVE	
CVE-2021-22955 CVE-2021-22956	
Fabricante	
Citrix	
Productos afectados	
Citrix ADC and Citrix Gateway 13.1-4.43 and later releases Citrix ADC and Citrix Gateway 13.0-83.27 and later releases of 13.0 Citrix ADC and Citrix Gateway 12.1-63.22 and later releases of 12.1 Citrix ADC and NetScaler Gateway 11.1-65.23 and later releases of 11.1 Citrix ADC 12.1-FIPS 12.1-55.257 and later releases of 12.1-FIPS Citrix SD-WAN WANOP Edition 11.4.2 and later releases of 11.4 Citrix SD-WAN WANOP Edition 10.2.9c and later releases of 10.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00520-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00520-01.pdf	

CSIRT alerta de vulnerabilidad zero day en Palo Alto Networks PAN-OS	
Alerta de seguridad cibernética	9VSA21-00521-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2021
Última revisión	12 de Noviembre de 2021
CVE	
CVE 2021-3064	
Fabricante	
Palo Alto Networks	
Productos afectados	
PAN-OS 8.1 anteriores a 8.1.17	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00521-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00521-01.pdf	

CSIRT alerta de vulnerabilidad en procesadores Intel	
Alerta de seguridad cibernética	9VSA21-00522-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2021
Última revisión	16 de Noviembre de 2021
CVE	
CVE-2021-0146	
Fabricante	
Intel	
Productos afectados	
Intel Pentium Processor J Series, N Series Intel Celeron Processor J Series, N Series Intel Atom Processor A Series Intel Atom Processor E3900 Series Intel Pentium Processor N Series Intel Celeron Processor N Series Intel Atom Processor E3900 Series Intel Pentium Processor Silver Series/ J&N Series Intel Pentium Processor Silver Series/ J&N Series – Refresh Intel Atom Processor C3000	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00522-01/	
https://www.csirt.gob.cl/media/2021/11/9VSA21-00522-01.pdf	

CSIRT alerta de vulnerabilidades en Google Chrome		
Alerta de seguridad cibernética	9VSA21-00523-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	16 de Noviembre de 2021	
Última revisión	16 de Noviembre de 2021	
CVE		
CVE-2021-38007	CVE-2021-38018	CVE-2021-38012
CVE-2021-38015	CVE-2021-38017	CVE-2021-38011
CVE-2021-38022	CVE-2021-38016	CVE-2021-38010
CVE-2021-38021	CVE-2021-38014	CVE-2021-38005
CVE-2021-38020	CVE-2021-38008	CVE-2021-38006
CVE-2021-38019	CVE-2021-38013	CVE-2021-38009
Fabricante		
Google		
Productos afectados		
Google Chrome: 7.0.517.41 a 95.0.4638.69		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00523-01/		
https://www.csirt.gob.cl/media/2021/11/9VSA21-00523-01.pdf		

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el equipo del CSIRT de Gobierno.

El CSIRT de Gobierno recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

HASH	Tipo Malware	Documento web
02756fefc515abf4212112a695e53cbc8f4b5f41b0ad7cb89ac2f8ae9f6467dc	W32/Injector	2CMV21-00248-01
8d31e522102744c714db644fd0572e337f6a69e72f3c3a4bb0deab211e9a12df	W32/Injector	2CMV21-00248-01
6d2bdf46d0def71bfd20c1565c28d456b744ed597ccb661a76912437b7e5718f	W32/Injector	2CMV21-00248-01
d784a286f15841718897e2b41ff05138c808e29374b6743b4cff1018306ce19a	Malicious_Behavior	2CMV21-00248-01
0214dfe1fb35f770e5228e06ec8ce40b4888aead8b0bd174701cd6c11ab56c34	MSExcel/CVE_2017_11882	2CMV21-00248-01
af19d80d5b368fca57c6fb523707081ae257147e25099acfb1e9b5164a96358d	W32/Netsky	2CMV21-00248-01
ec56ce552dc1fa7f917ece126ac825398401ae69bb7a398d668a0dc5ba2aff27	Riskware/POC_Iframe_CID	2CMV21-00248-01
97c75e51be09a805863be9dcd00091d699cb0889b00f4dd2f3ad4c7675f4b0fb	Malicious_Behavior	2CMV21-00248-01
c7d1bffffd4d49d89f571e0ffeb0244762997f7225e8c83253a7cfd4671a1e0c	PossibleThreat	2CMV21-00248-01
1816f032e9ca7c5a5cc879eb65c90a28f3adf2967d62220ba6d91e430dcd30e8	PossibleThreat	2CMV21-00248-01
e504ea9972d1d846493e010f2da6a2605baac04c019703ee0349d100a7484cfd	PossibleThreat	2CMV21-00248-01
727ef4fae330cf2a766efb213409b8c5c890bd519aec84b868ba96f72ad60fa4	PossibleThreat	2CMV21-00248-01
db6ccff08e4e2ddcfbf551356526edf49d781144644d136ff3c85a9d648727cc	PossibleThreat	2CMV21-00248-01
cfd5d0741ef7aaeb7c8b77d4880d0fb6284b2bd2ce3b5714a309b5cb9222b0f8	PossibleThreat	2CMV21-00248-01
8decda6f2414fa2d6e20448da0195da436d243a9f26c66d390848d87aa4cac75	Malicious_Behavior	2CMV21-00248-01
ce74a421212ea6db55404fc4a177a3607144bc82ecfb1c671125225e5940bfa7	MSIL/Kryptik	2CMV21-00248-01
0b9db3a994fa26161104fe79a7735b647d59ef603be4a662a565c30c7515282a	MSIL/Kryptik	2CMV21-00248-01
2fc085bdecf691e22544ecf82b31882a8918a004c1148840b760c5eb2c00f254	PossibleThreat	2CMV21-00248-01
b04e5861b2a7f6ceb725dcbc23480f5ec1e212bcdc40c1d7bdbf4d8b3a346319	W32/Injector	2CMV21-00248-01
5d99bdb224452fda2c738f2f882fe1c812afac3d98f2c9824ef6d750e9494a46	PossibleThreat	2CMV21-00248-01
c97ed76a6e99343dd526061116e677c0c6a9d589bec7e2f2f177b77e300528bc	Malicious_Behavior	2CMV21-00248-01
8a1a33421dff48b00f0a9ce79fefb8213f5dc2827f05577b0cb33e786f51f3dc	Malicious_Behavior	2CMV21-00248-01
5319fb9aa658191a80c6054ad80dec70455c01c580b7aba556c23d4b22c3be41	Malware_Generic	2CMV21-00248-01
d11d0082df53e178f0d3970cb4037ad09e2c2b3e39c85c5c9a55444b83ee0f5f	Malicious_Behavior	2CMV21-00248-01
f50d8e6b2460a7ffbeab5c0e3eac3062c5c90f6eeb47beda27d582452c86dea2	Malware_Generic	2CMV21-00248-01
66fe8dd2339e12fb3de52730d49d38f4471512c70c6b593b9d3735458a2e9b53	Malicious_Behavior	2CMV21-00248-01
6b0388de71d3779ee4192fb67f7cf338023c3e3a7bf0433ca8e31311f3301a8d	Malware_Generic	2CMV21-00248-01
5d99bdb224452fda2c738f2f882fe1c812afac3d98f2c9824ef6d750e9494a46	Malware_Generic	2CMV21-00248-01
ad100dd66a8c7a0af413d82a4babe032c90ba07f03d234feafe0eb39e97987d4	HTML/Agent.BUJ!tr	2CMV21-00248-01
8a1a33421dff48b00f0a9ce79fefb8213f5dc2827f05577b0cb33e786f51f3dc	Malware_Generic	2CMV21-00248-01
7ebc7f5a95b0d6723dd769348955a1c71c6df487b59588f55b97604961fcd1ae	W32/Malicious_Behav	2CMV21-00248-01
17a3f0a447a29ab04d4a194eb79772fe7641da5bbe8b0cf5781bf4e922f55c47	MSIL/CoinMiner	2CMV21-00249-01
1495ed8cf2d45165ddad9769a6585a70f5f2b164639dd6412c08edddd196a70d	MSIL/Kryptik	2CMV21-00249-01
93a3a49cd87bcb3d89898fb0d8dfbd448a9b02ca7e5a6fee4b3e4d0104da3d6d	MSIL/CoinMiner	2CMV21-00249-01

e61b55673e3c393632da298946136f6946f3aa4d6bc95ad7e8e42bdf1234c775	PossibleThreat	2CMV21-00249-01
440928f7612b8ea263648a6cad8aa4fcbbdcf4c2908e2ca3b0427a0c1ed11e4c	MSIL/Kryptik	2CMV21-00249-01
e22593115e2132bb409ff706cee9341dfbd8990c7ab61b6dae718eec0ac6d019	MSIL/GenKryptik	2CMV21-00249-01
be0d20e365851dfb49d756ff9f173bcd952bbe258badd2daf8d68a2ba024e569	MSIL/GenKryptik	2CMV21-00249-01
57fa17734750caa76f4d3fd8cd1ec9db69e54af6dd1603fd4f5a158fc15b958e	MSIL/GenKryptik	2CMV21-00249-01
d9e316e8a8e478b6e88a76153c0dfcc2f4bcbcbb631ba0516818f3f365cdad45	MSIL/GenKryptik	2CMV21-00249-01
7adcc25316101df9dab7f17a72bcede23253b09e3af4aa1e4472020b8cce8b2a	W32/Agent	2CMV21-00249-01
42db0461ac868e01c599a0aed146f50419ba7afc270a6da394900492763a94a8	W32/Agent	2CMV21-00249-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso. Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	ASN	Documento web
74.208.169.72	IONOS SE	AS 8560	2CMV21-00248-01
45.137.22.146	RootLayer Web Services Ltd.	AS 51447	2CMV21-00248-01
37.0.11.45	Delis LLC	AS 211252	2CMV21-00248-01
23.235.198.62	IMH-IAD	AS 54641	2CMV21-00248-01
193.56.29.164	Web Hosted Group Ltd	AS 210228	2CMV21-00248-01
185.222.57.202	RootLayer Web Services Ltd.	AS 51447	2CMV21-00248-01
173.231.241.38	IMH-IAD	AS 54641	2CMV21-00248-01
173.231.241.37	IMH-IAD	AS 54641	2CMV21-00248-01
159.223.92.129	DigitalOcean	AS 14061	2CMV21-00248-01
159.223.70.69	DigitalOcean	AS 14061	2CMV21-00248-01
159.223.56.212	DigitalOcean	AS 14061	2CMV21-00248-01
103.195.101.74	Reliablesite	AS 23470	2CMV21-00248-01
185.222.57.202	RootLayer Web Services Ltd.	AS 51447	2CMV21-00249-01
212.193.30.31	Des Capital B.V.	AS 213035	2CMV21-00249-01
37.0.11.45	Delis LLC	AS 211252	2CMV21-00249-01
94.130.135.43	Hetzner Online GmbH	AS 24940	2CMV21-00249-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

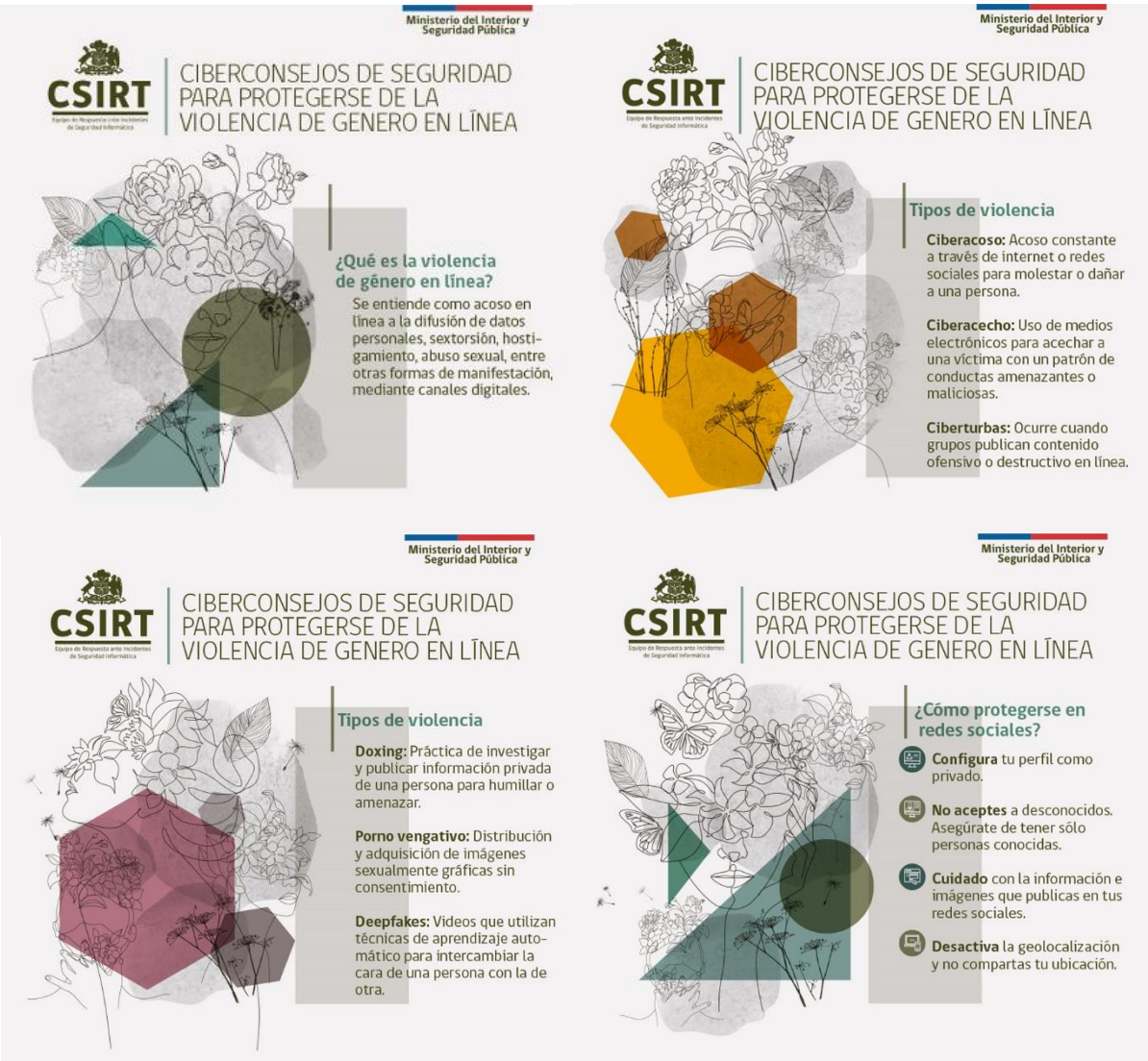
Nombres de archivos con malware	Documento web
11112021FX.cab	2CMV21-00248-01
29383773738387477474774.arj	2CMV21-00248-01
45678909876543456789.zip	2CMV21-00248-01
Advice Payment Copy.GZ	2CMV21-00248-01

Advice Payment Copy.TAR	2CMV21-00248-01
cotizaciÃ³n.pdf.img	2CMV21-00248-01
data2322.zip	2CMV21-00248-01
dKm7EEQynBnEXWy.rar	2CMV21-00248-01
invoice & packing list.rar	2CMV21-00248-01
Invoice and packing list.rar	2CMV21-00248-01
Iz150pqkbOdUArY.zip	2CMV21-00248-01
notificaciÃ³n bancaria SWift.exe.xz	2CMV21-00248-01
OFFER.zip	2CMV21-00248-01
Payment Advice 11.11.2021,pdf.html	2CMV21-00248-01
Payment confirmation(49.600).7z	2CMV21-00248-01
Payment_Advice.zip	2CMV21-00248-01
PO 210411.xlsx	2CMV21-00248-01
PO-101524309.zip	2CMV21-00248-01
PRICE DETAILS.zip	2CMV21-00248-01
Re 22-039 Quotationinstant tent shipment qty.gz	2CMV21-00248-01
remitance advice.r15	2CMV21-00248-01
SHIPPING DOCUMENT & PL.rar	2CMV21-00248-01
Swift Copy.r17	2CMV21-00248-01
Cceeoj9#234.zip	2CMV21-00249-01
cliff.kuhfeldt's CV.7z	2CMV21-00249-01
payment request documents.7z	2CMV21-00249-01
Remittance_advice.zip	2CMV21-00249-01
specs. in English.r17	2CMV21-00249-01

Actualidad

Ciberconsejos de seguridad para protegerse de la violencia de género en línea

El 25 de noviembre fue designado por las Naciones Unidas como el Día Internacional de la Eliminación de la Violencia contra la Mujer. Lamentablemente, existen diferentes formas de violencia, las que se pueden manifestar tanto de forma física como virtual. Estas son algunas recomendaciones para cuidarse en línea, las que también pueden encontrar aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-violencia-de-genero/.




Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD PARA PROTEGERSE DE LA VIOLENCIA DE GENERO EN LÍNEA
¿Cómo protegerse en redes sociales?
Evita compartir fotografías y videos de contenido sexual con desconocidos.
Bloquea al acosador e intenta cortar las vías de comunicación de inmediato.
Nunca compartas tus contra-señas, ni siquiera con tu pareja o amigos(as).
Guarda la prueba de violencia, acoso, amenaza o abuso.
Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS DE SEGURIDAD PARA PROTEGERSE DE LA VIOLENCIA DE GENERO EN LÍNEA
¡Pide ayuda si es necesario!
Si eres víctima o testigo, puedes denunciar o pedir ayuda llamando a:
Ministerio de la Mujer:
1455
Unidad de Cibercrimen de la PDI:
+562 27080 658

El Control de la Semana | No. 18 Controles de red

Vuelve el Control de la Semana con su edición número 18, centrada en los Controles de Red, o sea, las formas de mantener nuestras redes y los datos que circulan por ellas protegidos de amenazas, incluyendo conceptos útiles, recomendaciones y mejores prácticas que nuestras organizaciones deben aprender e implementar.

Todo lo encontrarán en el siguiente documento descargable:
https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-18/

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 los sitios web que se ingresen sean los oficiales.

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Sandra Odette Mansilla Reyes
- Juan Pablo Berríos Isaacs
- Christopher Pablo Rauber Oyarce
- Julio Ruedi Arretx
- Isaías Moisés Arancibia Venegas
- Fernando Peralta Echeverría
- José Ignacio Parra
- Andrea Fernández Gamarra
- Felipe Andrés Pizarro Astudillo
- Cristián Acuña
- Francisco Gutiérrez
- Andrés Orellana
- Fernando
- Sofía Margarita Gutiérrez Stipo

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.19 15:17:58 -03'00'