Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

01-10-2021 | Año 3 | N°117

Boletín de Seguridad Cibernética

Semana del 24 de 30 de septiembre de 2021

La semana en cifras

Hash

27

SHA

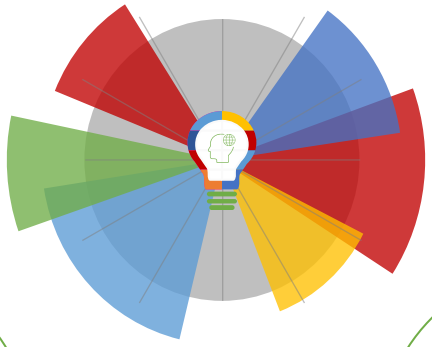
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

0

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

41

para vulnerabilidades

Las mitigaciones son útiles en productos de Google, Microsoft, Dell y Cisco.

IP

27

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

IoC Malware

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

Recomendamos 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.

No.	Hash de archivos maliciosos	Tipo de malware	Documento web
1	ce54e81125eb44ed53dec51f69f439d692ec3fcbfa99be82886163b5c869e74b	VBS/Agent.RHB!tr	2CMV21-00223-01
2	d923ce5dbb6597b2273301a0b0dc647fca4f991ed56077ab79c27255236b9161	HTML/Agent.AQX!tr	2CMV21-00223-01
3	595d62cc2f9ed1adb5942bbc6c00c1b5e57e005117d9242c7c2ddd40ae86cbe8	HTML/Agent.AQX!tr	2CMV21-00223-01
4	c6ffb2a4f4431bf21036e943929bdfc08b7fd294078b58a12ee620185e02bdd1	HTML/Agent.AQX!tr	2CMV21-00223-01
5	cc191eee507fc53308ddb782e027ad7f06067dafb3f0e29817e1e851bb6dc404	W32/Netsky.R@mm	2CMV21-00223-01
6	8650d63541ab6adedffccf52b48bac6bea614b40b01bce5714a517cb58285233	Riskware/POC_Iframe_CID	2CMV21-00223-01
7	9d501718380963810ff2c744984ae0b469acf79310208e54be06e89a4c274f43	HTML/Phish.D96E!tr	2CMV21-00223-01
8	52143f691973b6e77f05a76d9d3acfe7c542160eaddc25f30a98d34924321a7a	Trojan.Zmutzy.812	2CMV21-00223-01
9	e9112eae7f2de93d8e9722b06dc89ae78af80ff54bf8ff9466280c9be6181566	MSIL/GenKryptik.FLEG!tr	2CMV21-00223-01
10	d93c8bb2a190934c96aae21f1e9a471cf13ed75a62ac339a307eaa6e00c6d70c	MSIL/GenKryptik.FLEG!tr	2CMV21-00223-01
11	3fc3b61b78ef7b3133ae4350a591a56ee0cc7a0f0bdf6eaf40ea01f3c485dd04	MSOffice/Scam.2ED7!tr	2CMV21-00223-01
12	135dedf906bbb8eef7aef3b5966f1b933e65725cef80e653031481feb7351d62	RTF/CVE_2017_11882.C!exploit	2CMV21-00223-01
13	bec0f15ead1deb0d8761ae7c3946c5aa2547245b081fc5d2a9a84449f9c69fdf	MSOffice/Agent.GV!tr	2CMV21-00223-01
14	d5e3e06abfafe1c34fe40609293e5c68124c8386fe176be8e4a9606ea7f1f6ba	Malicious_Behavior.SB	2CMV21-00223-01
15	80076f3efa0ef7d925aea98f2dacc44218901df78131aa757fa17308d1b0c6ac	W32/Renamer.BQT!tr	2CMV21-00223-01
16	94ccac8926a3631f24f90fdee44dba55012a296b1bd918ae206a1ca63290bd19	W32/PossibleThreat	2CMV21-00223-01
17	4bec198c3b9044d9048d64b8f4910b1ece28a112a8574bbb3bde90c813c86375	W32/PossibleThreat	2CMV21-00223-01

18	a0f83ac12ac70862e8d23f203dfacab3cb6b7db722caaf54a0316c9c036c67d4	MSOffice/CVE_2017_11882.DMP	2CMV21-00223-01
19	333ea88cba349ca95118c5a3ea4e4f2f16cd403a933a1ee805d0763f629e07f5	HTML/Phishing.BTV!tr	2CMV21-00223-01
20	d2328ee77375a61ce495f4ad6a18d4766588cd0d97cb17cc20eb6618ffe3ae96	PossibleThreat	2CMV21-00223-01
21	c103b226304f25770133cc9f080bbb43c3a790eeaf542f581ecbdf37aff33b5e	HTML/Agent.AQX!tr	2CMV21-00223-01
22	dfa4598a66fb4267bb2c51bf9e2dba6bc3c022cb2ad9838a6da7ff0f69077afc	W32/Agensla.FLEH!tr.pws	2CMV21-00223-01
23	378e722690fc135e245b37d280aece03cad76ad95da7ac4af06293bb27bfd823	W32/Agensla.FLEH!tr.pws	2CMV21-00223-01
24	dc7bc675429ac837433812650657f4e2712eaa1a9ed0ee15323c50c38a45930c	W32/Agensla.FLEH!tr.pws	2CMV21-00223-01
25	f4a4a7d84f937fdaa9808d529e4541ae6ef330e77ed8bd42fc776ff088fa22fb	MSIL/Tiny.BGM!tr.dldr	2CMV21-00223-01
26	4128ef1454b3c622904e02a72036174abcc26605d7204248f260441ab57efa4c	HTML/Redirect.1258!tr	2CMV21-00223-01
27	de723989633a408ec0940236e4ae0a52d6fde55ba881d18aaf3366a28e3e2975	MSIL/GenKryptik.FLDA!tr	2CMV21-00223-01

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.

No.	IP	Etiqueta de sistema autónomo	Documento web
1	46.183.223.82	DataClub S.A.	2CMV21-00223-01
2	172.96.11.222	UNREAL-SERVERS	2CMV21-00223-01
3	88.30.17.247	Telefonica De Espana	2CMV21-00223-01
4	192.119.110.154	HOSTWINDS	2CMV21-00223-01
5	217.31.95.26	Hostserver GmbH	2CMV21-00223-01
6	45.137.22.143	RootLayer Web Services Ltd.	2CMV21-00223-01
7	45.137.22.48	RootLayer Web Services Ltd.	2CMV21-00223-01
8	23.94.152.203	AS-COLOCROSSING	2CMV21-00223-01
9	23.94.152.201	AS-COLOCROSSING	2CMV21-00223-01
10	45.144.225.128	Delis LLC	2CMV21-00223-01
11	84.38.130.219	DataClub S.A	2CMV21-00223-01
12	67.207.82.148	DIGITALOCEAN-ASN	2CMV21-00223-01
13	103.133.110.171	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00223-01
14	185.222.57.172	RootLayer Web Services Ltd	2CMV21-00223-01

Nombres de archivos con malware:

N°	Archivo Malware	
1	bank details.XLXs.img	2CMV21-00223-01
2	DEPARTAMENTO_INTERNACIONAL_DE_MOLOTERÃ..docx	2CMV21-00223-01
3	dhlshipping.html	2CMV21-00223-01
4	Doc1.pdf.rar	2CMV21-00223-01
5	Document.zip	2CMV21-00223-01
6	ðŸ“£_â,¬68__763__ID_2sVRGlvUKdyuCm540l3p8SdseMqgI6.html	2CMV21-00223-01
7	IN00987656.pdf.exe	2CMV21-00223-01
8	message18002.zip	2CMV21-00223-01
9	NEW PRODUCT DETAILS.doc	2CMV21-00223-01
10	New_Order_PO#960780_MT_Quote-MT.gz	2CMV21-00223-01
11	Nuevo pedido # 86-55113,pdf.iso	2CMV21-00223-01
12	OBL PN210700369.doc	2CMV21-00223-01
13	Proforma Invoice-Bank Advice (PAID) Attached.pdf.zip	2CMV21-00223-01
14	Quotation 200113893.pdf.img	2CMV21-00223-01
15	QUOTATION INVOICE.html	2CMV21-00223-01
16	REVISED ORDER.zip	2CMV21-00223-01
17	RFQ indent.xlsx	2CMV21-00223-01
18	Sept-PO-34482.html	2CMV21-00223-01
19	Spare Parts KITO.XLXs.img	2CMV21-00223-01
20	URGENT ORDER CURRENT LOUVOLITE PROJECT.doc	2CMV21-00223-01

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

No.	IP	Etiqueta de sistema autónomo	Documento web
1	142.11.199.235	HOSTWINDS	4IIA21-00041-01
2	31.130.184.68	Blue Diamond Network Co., Ltd.	4IIA21-00041-01
3	31.130.184.95	Blue Diamond Network Co., Ltd.	4IIA21-00041-01
4	31.130.184.62	Blue Diamond Network Co., Ltd.	4IIA21-00041-01
5	31130184194	Blue Diamond Network Co., Ltd.	4IIA21-00041-01
6	31.130.184.93	Blue Diamond Network Co., Ltd.	4IIA21-00041-01
7	103.167.84.88	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	4IIA21-00041-01
8	194.61.24.153	ERA LLC	4IIA21-00041-01
9	194.61.24.154	ERA LLC	4IIA21-00041-01
10	194.61.24.151	ERA LLC	4IIA21-00041-01
11	194.61.24.155	ERA LLC	4IIA21-00041-01
12	194.61.24.152	ERA LLC	4IIA21-00041-01
13	45.144.225.200	ERA LLC	4IIA21-00041-01

IP reportadas en informes anteriores y que aún se encuentran activas a la fecha de este reporte:

N°	IP	Documento web
1	5.188.206.155	4IIA21-00041-01
2	5.188.206.158	4IIA21-00041-01
3	5.188.206.98	4IIA21-00041-01
4	5.188.206.100	4IIA21-00041-01
5	5.188.206.102	4IIA21-00041-01
6	5.188.206.154	4IIA21-00041-01
7	5.188.206.101	4IIA21-00041-01
8	5.188.206.156	4IIA21-00041-01
9	5.188.206.157	4IIA21-00041-01
10	5.188.206.99	4IIA21-00041-01

Vulnerabilidades

CSIRT alerta ante vulnerabilidades críticas en productos Cisco	
Alerta de seguridad cibernética	9VSA21-00497-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2021
Última revisión	26 de septiembre de 2021
CVE	
CVE-2021-34770 CVE-2021-34727 CVE-2021-1619	
Fabricante	
Cisco	
Productos afectados	
Cisco IOS XE Software for Catalyst 9000 Family Wireless Controllers Cisco IOS XE SD-WAN Software Cisco IOS XE Software	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00497-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00497-01.pdf	

CSIRT alerta de vulnerabilidades graves en Dell EMC VxRail Appliance		
Alerta de seguridad cibernética	9VSA21-00498-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	29 de septiembre de 2021	
Última revisión	29 de septiembre de 2021	
CVE		
CVE-2021-22005 CVE-2021-22019 CVE-2021-22013 CVE-2021-22012 CVE-2021-22017 CVE-2021-22016 CVE-2021-22018	CVE-2021-22011 CVE-2021-22020 CVE-2021-22015 CVE-2021-21991 CVE-2021-22014 CVE-2021-22010	CVE-2021-22009 CVE-2021-22008 CVE-2021-22007 CVE-2021-22006 CVE-2021-21993 CVE-2021-21992
Fabricante		
Dell		
Productos afectados		
Dell EMC VxRail Appliance.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00498-01		
https://www.csirt.gob.cl/media/2021/09/9VSA21-00498-01.pdf		

CSIRT alerta de vulnerabilidad crítica en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00499-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de septiembre de 2021
Última revisión	29 de septiembre de 2021
CVE	
CVE-2021-37973	
Fabricante	
Google	
Productos afectados	
Google Chrome: 7.0.517.41 a 93.0.4577.82	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00499-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00499-01.pdf	

CSIRT alerta de vulnerabilidades graves en Microsoft Edge		
Alerta de seguridad cibernética	9VSA21-00500-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	29 de septiembre de 2021	
Última revisión	29 de septiembre de 2021	
CVE		
CVE-2021-37965	CVE-2021-37961	CVE-2021-37967
CVE-2021-37964	CVE-2021-37962	CVE-2021-37968
CVE-2021-37957	CVE-2021-37963	CVE-2021-37969
CVE-2021-37958	CVE-2021-37956	CVE-2021-37970
CVE-2021-37959	CVE-2021-37973	CVE-2021-37971
CVE-2021-37960	CVE-2021-37966	CVE-2021-37972
Fabricante		
Microsoft		
Productos afectados		
Microsoft Edge (Chromium-based): 79.0.309.71 a 93.0.961.52		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00500-01		
https://www.csirt.gob.cl/media/2021/09/9VSA21-00500-01.pdf		

Actualidad

Exitoso Segundo Simposio de Ciberseguridad para Funcionarios Públicos, realizado por el CSIRT de Gobierno, congrega a casi mil inscritos

El Segundo Simposio para Funcionarios Públicos, efectuado el 28 de septiembre y realizado íntegramente por funcionarios del CSIRT de Gobierno, dependiente del Ministerio del Interior, logró superar con creces los números de registros de su primera versión, llegando a los casi mil inscritos.

Pueden leer los detalles y descargar las presentaciones en www.csirt.gob.cl/noticias/exitoso-segundo-simposio-funcionarios.

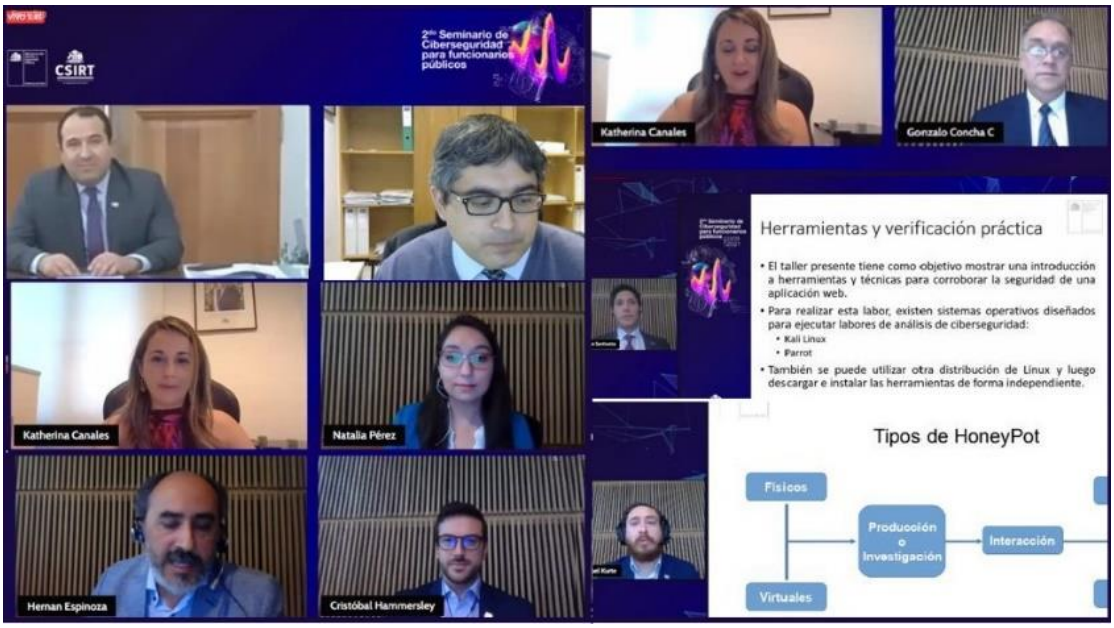
Como en su primera versión, la bienvenida estuvo a cargo del Subsecretario del Interior, desde el Palacio de La Moneda. Las charlas y talleres realizadas por los funcionarios fueron las siguientes.

CHARLAS

- Ciberseguridad en el Estado, análisis del nuevo marco normativo: Carlos Landeros, Director del CSIRT de Gobierno.
- Seguridad en sitios web: Natalia Perez, Analista CSIRT.
- Controles para mitigar amenazas en ciberseguridad: Gonzalo Concha, Analista CSIRT
- Revocación de nombres de dominio: Cristóbal Hammersley, Asesor CSIRT.

TALLERES

- Usando un SIEM (opensource): Wazuh: Hernan Espinoza, Analista CSIRT.
- Usando un Honeypot (opensource): Miguel Kurte, Analista CSIRT.
- Seguridad en sitios web, herramientas y verificación práctica: Juan Sanhueza, Analista CSIRT.



Claves de la jornada

- Se registraron para participar casi 1.000 encargados de ciberseguridad de reparticiones del Estado, empresas públicas y organizaciones privadas que tienen convenio con el CSIRT de Gobierno, contra 680 el año pasado.

- Las charlas y talleres son realizadas íntegramente por expertos pertenecientes al CSIRT de Gobierno, por lo que además de su conocimiento técnico comparten su experiencia en la práctica, monitoreando el ciberespacio nacional

- Para servir a un público lo más amplio posible, sin importar restricciones presupuestarias, los talleres utilizaron herramientas de código abierto, con uso libre, gratuito y adaptable.

- Para elegir los temas a tratar se encuestó a los encargados de ciberseguridad de los servicios públicos con los que trabaja el CSIRT de Gobierno, con tal de responder a necesidades concretas de la administración pública en materia de ciberseguridad.

- Se transmitió durante 8 horas a través de Zoom y Linkedin Live.

CiberSucesos No. 12 | Ciberseguridad Industrial

Tras dos meses con ediciones especiales de CiberSucesos, volvemos a nuestra programación regular con el número 12, enfocado en la ciberseguridad industrial y que cuenta con sus secciones tradicionales. Esta disciplina se ocupa de proteger tanto las tecnologías de la información (IT), el campo tradicional de la ciberseguridad, como las tecnologías de las operaciones (OT).

Pueden revisar la revista completa, aquí: https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-12-ciberseguridad-industrial/.

Quienes navegamos día a día la creciente convergencia existente entre lo virtual y lo real, con todas las ventajas e incertidumbres que plantea, debemos también tomar conciencia de que a medida de que la realidad se digitaliza, cada vez más elementos físicos y tangibles de nuestro diario vivir quedan a merced de amenazas cibernéticas que antes quedaban circunscritas a lo virtual.

Son ejemplos de la "convergencia", como se le denomina, entre IT y OT, los principales componentes de la llamada Industria 4.0, como el internet operacional de las cosas (IIoT), sistemas de control industrial (ICS), sensores inteligentes, robots, controladores lógicos programables (PLC) y los sistemas de supervisión, control y adquisición de datos (SCADA), entre otros.

Así, un actor malicioso que logre entrar a los sistemas de una industria moderna puede causar graves daños a su infraestructura física, dañando líneas de producción, pudiendo generar productos peligrosos o nocivos, e incluso hiriendo directamente a personas. Famosos son ejemplos como el ataque que, accediendo remotamente a las redes SCADA de distribución eléctrica en Ucrania dejaron a cientos de miles de personas sin luz, o el gusano Stuxnet, con el que se cree que Israel logró sabotear el programa nuclear iraní.

En definitiva, la ciberseguridad hoy debe contemplar esta integración digital e industrial, y es por eso que nuestras notas principales se dedican a explicar qué es la ciberseguridad industrial, cuáles son sus alcances y cómo protegerla. En la misma línea, la sección Tendencias explica los ataques a la cadena de suministro, una forma de infectar a múltiples organizaciones con solo acceder a una de sus proveedoras.

En el apartado de Comunidades Nacionales contamos con la experiencia de Freddy Macho, presidente del IoT Security Institute Chile (IoTSI), que se ocupa de promover la ciberseguridad industrial en nuestro país, y como parte de la Cooperación Internacional, el ejemplo que desde España supone en Centro de Ciberseguridad Industrial (CCI). Y para cerrar, en la sección Legal, delineamos las principales normas que el CSIRT de Gobierno ha impulsado de la mano de distintas superintendencias para mejorar los estándares de ciberseguridad en varias industrias del país, como la generación y distribución eléctrica, las aguas y las telecomunicaciones.

El Comando de la Semana | No. 19 Recon-NG

El Comando de la Semana revisa en esta ocasión a Recon-NG, un marco de trabajo de reconocimiento web con todas las funciones, escrito en Python, completado con módulos independientes, con interacción con la base de datos, funciones especiales integradas, ayuda interactiva y finalización de comandos. Recon-NG proporciona un entorno poderoso en el que el reconocimiento basado en código abierto se puede realizar de manera rápida y completa sobre un sitio o sistema web.

Con los comandos que compartimos semanalmente no pretendemos reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-19/.

El Control de la Semana | No. 13 Registros del Administrador y el Operador

Nuestra Ficha de Control Normativo se concentra en esta ocasión en cómo crear instrucciones, medidas y controles para un elemento esencial de la Política General de Seguridad de la Información en una organización: los Registros del Administrador y el Operador.

En el contexto de los registros de eventos (protagonistas de nuestro anterior Control de la Semana), un grupo especial lo forman aquellos relacionados con las acciones de los administradores y operadores. Por ejemplo, las conexiones del usuario «root» fallidas y exitosas en un sistema Linux.

Por eso, en el documento descargable a continuación encontrarán los detalles más importantes a tener en consideración al momento de definir nuestros controles para los Registros del Administrador y el Operador.

Pueden descargar esta nueva ficha semanal, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-13/.

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- Carlos Barrios
- Josefa Orellana Solar
- Roberto Jeria Silva
- Felipe Andrés Acosta Díaz
- Cat[.]py_01
- Fernando Enrique González Rojas
- Eduardo Riveros Roca
- Juan Benítez Ontiveros
- Claudio Enrique Jerez Sanhueza
- Andrés Antonio Sáez Rojas
- José Villa
- Francisco Javier Gutiérrez

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.01 13:05:46 -03'00'