Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

03 de mayo 2021

Índice

Índice de Ilustraciones

Índice de Tablas

1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de abril de 2021. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets.

El informe también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso del mes de abril y también muestra la proporción de aquellos que quedan por terminar.

Asimismo, en este documento se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.

Este reporte mensual muestra, además, el origen o procedencia de la información que procesa CSIRT –si es interna o externa- y presenta en términos porcentuales el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

Adicionalmente, también se entrega un desagregado con el detalle que permite conocer la participación –en cantidades y en términos porcentuales- de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.

Finalmente, se presenta información proveniente de la plataforma MISP[1] que contiene la cantidad de posibles IoCs[2] o –Índices de Compromiso- que se hayan detectado. Esta información es relevante para CSIRT dado que se utiliza como punto de partida para validar correlaciones con todas nuestras plataformas de análisis. En el informe se expone una tabla donde se puede enumerar la cantidad de IoCs detectados en el presente mes, los cuales se presentan diferenciados en base a direcciones IP[3] o a URL[4].

[1] MISP es una sigla en idioma inglés que significa Malware Information Sharing Platform o "Plataforma para compartir información de Malware y amenazas".
[2] IOC es una sigla en idioma inglés que significa "Índice de compromiso", y se refiere a la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones.
[3] IP es una sigla en idioma inglés que significa "Internet Protocol" y corresponde a un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone).
[4] Es una sigla en idioma inglés que significa Uniform Resource Locator o "Localizador Uniforme de Recursos". Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados. Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen un URL cuando se publican en Internet. Estos localizadores permiten crear hipervínculos. De esta forma, el URL, por lo tanto, es el conjunto de caracteres que posibilita la asignación de una dirección exclusiva a un recurso que se encuentra disponible en el espacio virtual. En otras palabras, el URL es una dirección de Internet que, al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario.

2. Alcances del Informe

La información que se muestra en el presente informe proviene de la gestión de CSIRT en el marco del proceso de notificación a entidades, instituciones y/u organismos afectados. Esa información se produce como consecuencia de las actividades desarrolladas por el equipo 24/7 en un período de tiempo mensual. A continuación, se enumera resumidamente esas actividades:

- Gestión de tickets generados, efectuando seguimiento y validando las acciones que se tomaron con el ticket enviado al organismo gubernamental afectado.

- Reporte de vulnerabilidades de aquellos tickets precedentes una vez validado que la falla de seguridad se encuentre aún presente.

- Generación de análisis y reporte de vulnerabilidades detectadas dentro de la RCE[5] (falta cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, Phishing, deface, etc…).

- Seguimiento a los tickets reportados (contacto mediante llamada telefónica y/o correo electrónico) para validar qué acciones ha tomado la entidad reportada con la información de la vulnerabilidad detectada.

- Análisis y monitoreo de un listado de -6.200 sitios aproximadamente- los cuales corresponden a portales gubernamentales, a los que se ha validado su estatus utilizando las plataformas Splunk, Pingdom y PRTG.

- Monitoreo de los dispositivos de las instituciones que se encuentran conectadas dentro de la RCE.

- Generación de ticket para notificar a la entidad y/u organismo afectado, ante la identificación de cualquier eventualidad sucedida con los dispositivos y sitios que se encuentran dentro del alcance de monitoreo de CSIRT.

[5] RCE significa Red de Conectividad del Estado

3. Tipos de Tickets

En la siguiente tabla se expone las categorías, o tipos de tickets, que son generados por el equipo CSIRT. La información se presenta ordenada, de mayor a menor, respecto a la cantidad de tickets que se generó por cada tipología. Los cuales se agrupan según la matriz de clasificación de incidentes de ENISA, (Agencia de la Unión Europea para la Ciberseguridad) en 10 categorías relacionadas a incidentes de seguridad informática y acciones preventivas y operacionales, programadas de las instituciones que resultan en la interrupción parcial de un servicio. Más abajo se muestra un gráfico que refleja esta misma información, pero como una distribución en términos porcentuales de lo que representa la participación de cada tipo de ticket dentro del total de la demanda de trabajo que recibe y procesa CSIRT.

N°	Tipos de ticket	Código	Total
1	Vulnerabilidad	9V00	886
2	Recopilación de Información	3R00	225
5	Información de seguridad de contenidos	7S00	153
6	Operaciones Ciberseguridad CSIRT	19OC	110
4	Fraude	8F00	84
3	Código Malicioso	2C00	43
9	Contenido Abusivo	1A00	35
8	Intrusión	5I00	23
10	Intentos de Intrusión	4I00	13
7	Disponibilidad	6D00	0
	Total		1572

Tabla 1 - Total Tipos de Tickets

Ilustración 1 - Tipos de tickets

En la siguiente tabla se muestran la tendencia y los cambios en el ranking que experimentan los tipos de tickets generados por CSIRT en el mes de abril, respecto a marzo de 2020.

Como se aprecia en la tabla, los tickets de las categorías de, vulnerabilidad, operaciones de ciberseguridad CSIRT, código malicioso y disponibilidad decrecen en su tendencia (hay menos números de tickets), mientras que las restantes cinco categorías experimentan una tendencia creciente al comparar el mes de abril con el pasado mes de marzo.

	Marzo	Abril	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▼	➡
2	Operaciones Ciberseguridad Csirt	Recopilación de Información	▲	⬆
3	Recopilación de Información	Información de seguridad de contenidos	▲	⬆
4	Código Malicioso	Operaciones Ciberseguridad CSIRT	▼	⬇
5	Información de seguridad de contenidos	Fraude	▲	⬆
6	Fraude	Código Malicioso	▼	⬇
7	Intrusión	Contenido Abusivo	▲	⬆
8	Contenido Abusivo	Intrusión	➡	⬇
9	Disponibilidad	Intentos de Intrusión	▲	⬆
10	Intentos de Intrusión	Disponibilidad	▼	⬇

Tabla 2 - Ranking de Alertas Recibidas

4. Tipos de Ticket Públicos y Privados

En la siguiente tabla se presenta el desagregado de los tickets que fueron reportados a instituciones públicas o privadas, por las distintas categorías presentadas.

Tickets	Privado	Público	Total
Vulnerabilidad	40	846	886
Recopilación de Información	45	180	225
Información de seguridad de contenidos	134	19	153
Operaciones Ciberseguridad CSIRT	90	20	110
Fraude	74	10	84
Código Malicioso	10	33	43
Contenido Abusivo	18	17	35
Intrusión	2	21	23
Intentos de Intrusión	7	6	13
Disponibilidad	0	0	0
Total	420	1152	1572

Tabla 3 - Tickets a Instituciones Públicas y Privadas

En el siguiente gráfico expone el porcentaje de participación que tiene cada destino de los tickets que son enviados a instituciones públicas o privadas.

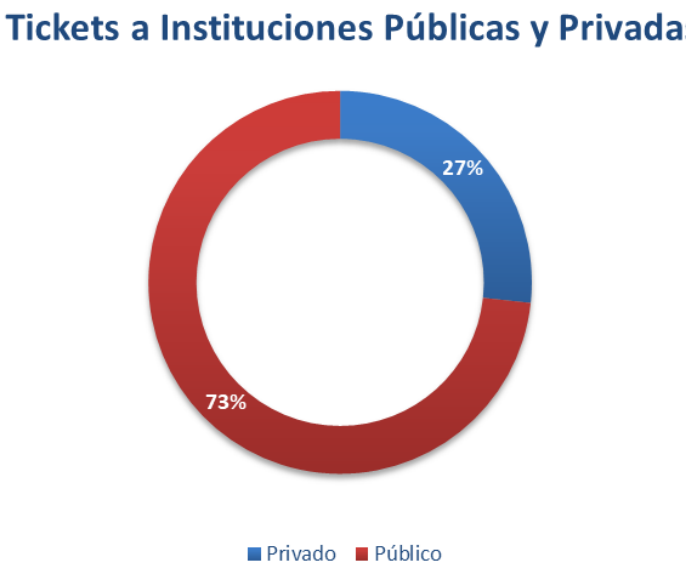


Ilustración 2–- Tickets a Instituciones Públicas y Privadas

5. Estado de Ticket Procesados en el Presente Mes

En la siguiente tabla y gráfico de distribución se muestra el estado de los tickets procesados en el mes de abril de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1.961 unidades. De este total, 866 tickets fueron cerrados exitosamente, lo que representa un 44% de eficacia, mientras que 1.095 tickets 56% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	895
Cerrados	677
Total general	1572

Tabla 4 - Total Estado de Ticket

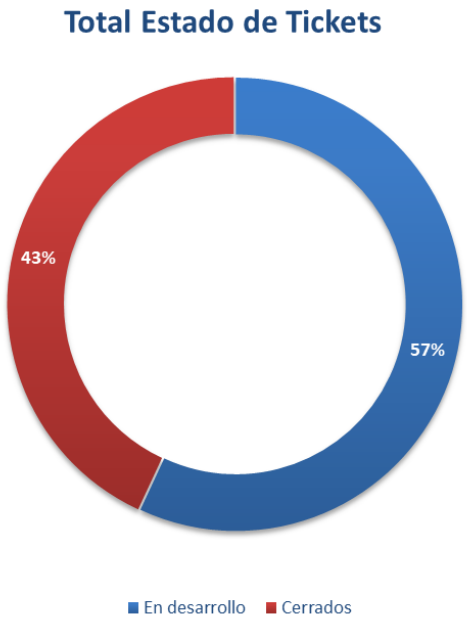


Ilustración 3 - Total Estado de Tickets

6. Procedencia de Generación de Tickets

En la siguiente tabla se presenta la composición -del origen de los tickets- que procesó CSIRT para el desarrollo de su labor durante el mes de abril de 2021.

Como se aprecia en la tabla, los tickets se pueden originar tanto interna como externamente.

Los tickets de origen internos son todos aquellos que fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante el software que utiliza CSIRT -que también considera los sensores que dan aviso o reportan- desde otros servicios públicos o de las FF.AA.

Por otro lado, los tickets de origen externo son todos aquellos que provienen de proveedores vinculados a CSIRT vía contractual o que se generan a través de call center, por formulario web, por medio de otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

Tipo de Fuente	Cantidad de Tickets
Servicios Internos	1279
Servicios Externos	293
Total Fuentes de Tickets	1572

Tabla 5 - Fuentes de Servicios (Interna y/o Externa)

Como se puede observar en el siguiente gráfico, un 81% de la demanda de trabajo que recibió CSIRT en el pasado mes de abril tiene un origen interno, mientras que el 19% restante proviene de fuentes externas.

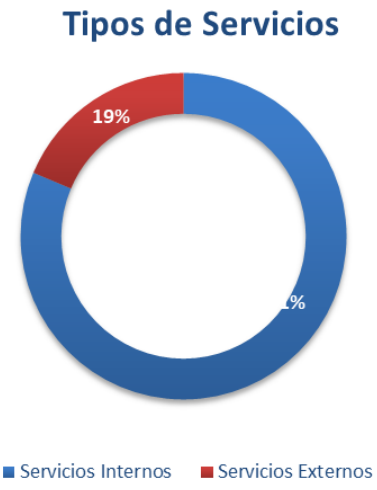


Ilustración 4- Distribución Porcentual de Origen de Tickets

7. Fuentes de Origen Externo de Tickets

En la siguiente tabla se presenta información que da cuenta de las fuentes externas que dieron origen a tickets de esa procedencia durante abril de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	183
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	110
Tickets generados por privados vía email	0
Tickets generados por privados vía call center	0
Tickets generados por información de otros CSIRT internacionales	0
Total	293

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en abril de 2021 el porcentaje mayor de tickets externos son generados por reportes entregados por "Empresas privadas sin convenio de ciberseguridad CSIRT", con un 62% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía formulario web" con un 38% de contribución.

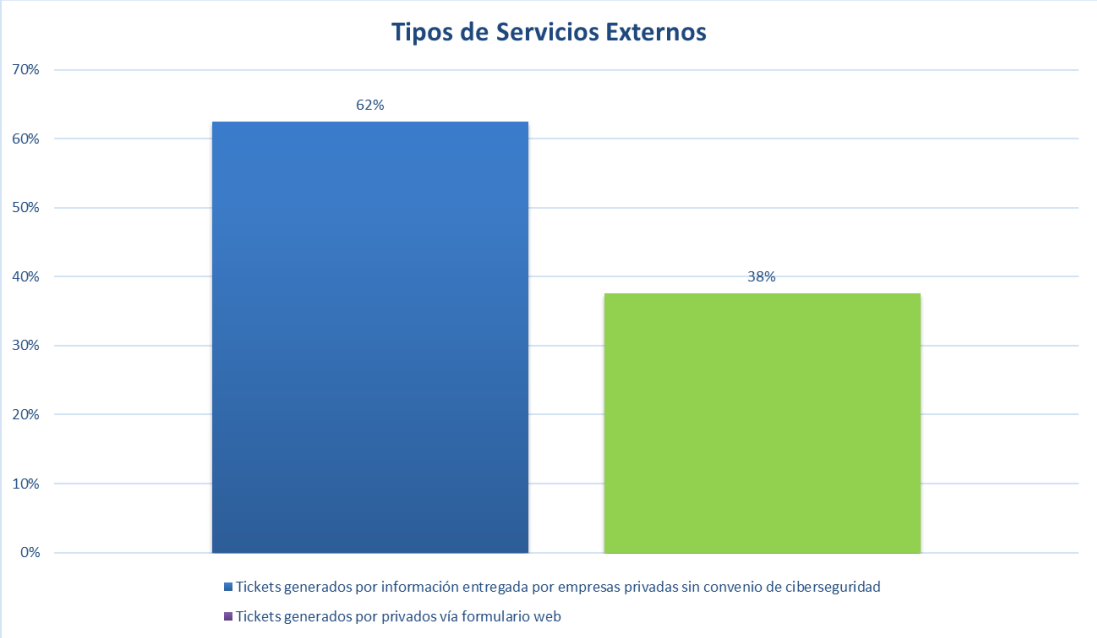
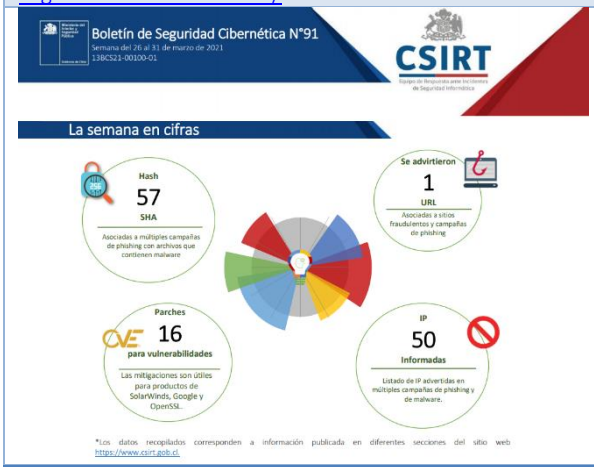
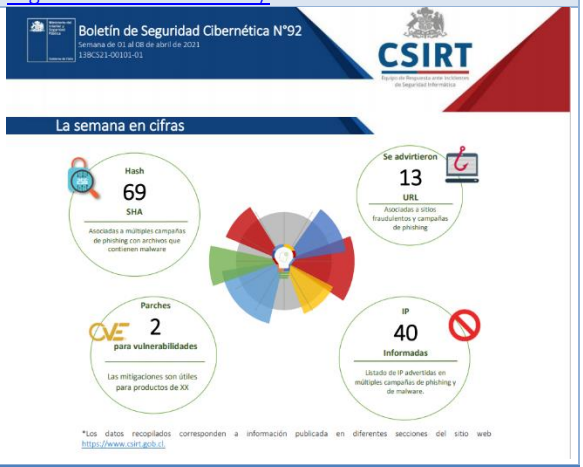
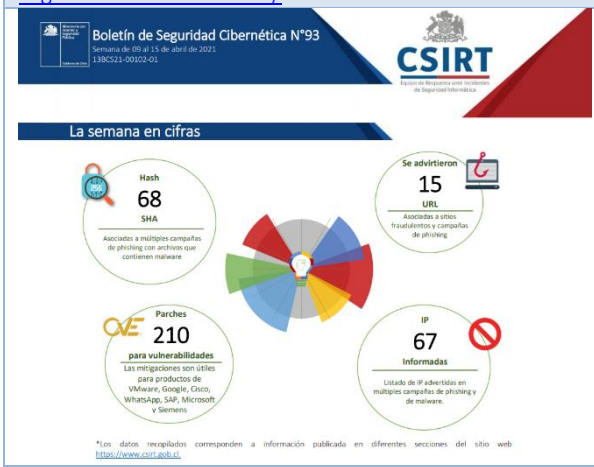
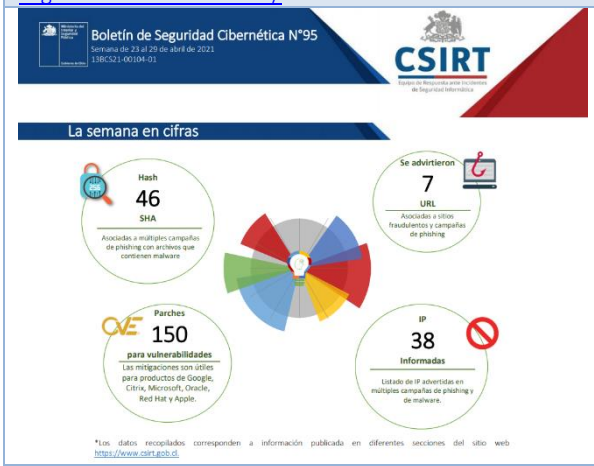


Ilustración 5- Tipos de servicios externos

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

Los enlaces que se comparten a continuación, corresponden a los boletines semanales publicados durante el mes de marzo que contienen el resumen de actividades realizadas por el CSIRT y que fueron publicadas en el sitio web www.csirt.gob.cl.

Boletín de Seguridad Cibernética n°91	Boletín de Seguridad Cibernética n°92
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n91/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n92/
	
Boletín de Seguridad Cibernética n°93	**Boletín de Seguridad Cibernética n°94**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n93/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n94/
	

Boletín de Seguridad Cibernética n°95	
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n95/	
	

9. Síntesis de gestión sobre concientización y buenas prácticas

Los enlaces que se comparten a continuación, corresponden a campaña de concientización y buenas prácticas publicadas por CSIRT durante el mes de marzo y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

Ciberconsejos para evitar caer en el phishing durante la Operación Renta	Estudio sobre ciberacoso y salud mental en los jóvenes | Fundación Katy Summer
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-caer-en-el-phishing-durante-la-operacion-renta/	https://www.csirt.gob.cl/recomendaciones/estudio-sobre-ciberacoso-y-salud-mental-en-los-jovenes-fundacion-katy-summer/
	

Ciberconsejos para protegernos de Emotet	Ciberconsejos | El Bitcoin y las estafas que lo rodean
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-emotet/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-el-bitcoin-y-las-estafas-que-lo-rodean/
	

Ciberconsejos para evitar caer en estafas este Día de la Madre	CiberSucesos No. 9 | La Inteligencia Artificial y la Ciberseguridad
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-caer-en-estafas-este-dia-de-la-madre/	https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-9/
	

9. Actualidad

Ministerio del Interior firma 20 convenios de ciberseguridad con organizaciones de todo el país

Para extender su alianza con los distintos sectores del quehacer nacional e implementar mejores estándares y colaborar en materia de ciberseguridad, el Ministerio del Interior firmó ayer 20 nuevos convenios de cooperación con empresas privadas y universidades, que se suman a los 53 signados durante 2020. Este hito se suma a su reciente colaboración con organismos como la Subsecretaría de Telecomunicaciones, la Superintendencia de Seguridad Social y la Superintendencia de Casinos de Juego por la implementación de circulares de ciberseguridad.

Los detalles en: https://www.csirt.gob.cl/noticias/csirt-firma-convenios-2021/.

Superintendencia de Casinos de Juego publica normativa en ciberseguridad junto al CSIRT de Gobierno

En presencia del Subsecretario del Interior, Juan Francisco Galli, la Superintendenta de Casinos de Juego (SCJ), Vivien Villagrán, firmó hoy la circular que fija los estándares y normativas para la gestión de la información e implementación de la ciberseguridad en los casinos de juego del país, iniciativa llevada a cabo junto al Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT) de Gobierno.

Se avanza un nuevo paso, así, en el trabajo que realiza el Ministerio del Interior junto a las superintendencias para entregar los lineamientos de ciberseguridad a los distintos sectores de la economía, y así proteger y cuidar la información y datos de los chilenos e instituciones.

La noticia completa, aquí: https://www.csirt.gob.cl/noticias/superintendencia-de-casinos-de-juego-publica-normativa-en-ciberseguridad-junto-al-csirt-de-gobierno/.

CSIRT de Gobierno participa de panel sobre transformación digital bancaria en Latinoamérica

El director nacional del CSIRT de Gobierno, Carlos Landeros, participó en el seminario virtual «Tendencias y desafíos de la Transformación Digital para el sector financiero en la región», organizado por la Internet Society Capítulo Colombia (ISOC) e impulsado por la Corfo, ProChile y el Ministerio de Relaciones Exteriores.

En el webinar, nuestro director compartió la experiencia del sector bancario chileno en relación con la ciberseguridad, los principales ataques sufridos en los últimos años, y la importancia de fomentar la cooperación público privada a todo nivel para responder en conjunto a las amenazas.

Este archivo puede ser encontrado en el siguiente enlace:
https://www.csirt.gob.cl/noticias/csirt-de-gobierno-participa-de-panel-sobre-transformacion-digital-bancaria-en-latinoamerica/.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.03 11:37:32 -04'00'