

# INFORME DE GESTIÓN MENSUAL SEPTIEMBRE 2022



## ACERCA DE ESTE INFORME

---

En el siguiente documento resumimos la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno, dependiente del Ministerio del Interior y Seguridad Pública.

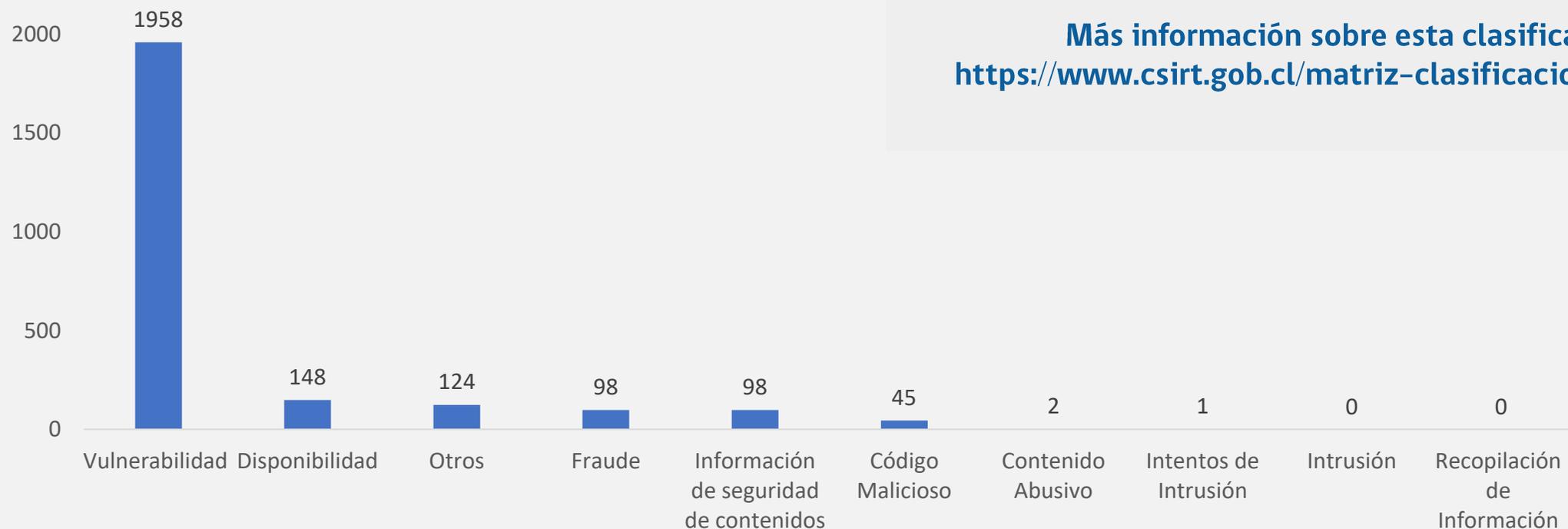
Es la gestión realizada durante septiembre de 2022, que comprende los tickets que procesamos, incluyendo el detalle de los tipos de incidentes reportados y datos como el porcentaje de tickets que se reportaron al sector público y privado.

Además, este informe mensual da cuenta de las alertas sobre campañas de phishing, malware, creación de sitios fraudulentos, vulnerabilidades y ataques de fuerza bruta informados mediante los canales digitales del CSIRT de Gobierno a la ciudadanía.

Para lograr informar oportunamente y las distintas amenazas a los que están expuestas las personas, el CSIRT de Gobierno recibe la invaluable colaboración de personas e instituciones que notifican estos incidentes en cuanto los descubren. A todos ellos, les entregamos nuestros más sinceros agradecimientos. Esperamos seguir contando con su apoyo.

## TIPO DE INCIDENTE

Ante las diversas amenazas y peligros que abundan en el ciberespacio, el CSIRT de Gobierno notifica a instituciones públicas y privadas de aquellos riesgos que considera más probables de afectar a sus sistemas. Es así como este mes generamos **2.073** tickets, un **19%** menos que en agosto. Estos tickets de agosto corresponden a las siguientes categorías, definidas según el tipo de incidente de seguridad informática al que corresponden, y ordenadas según su frecuencia.



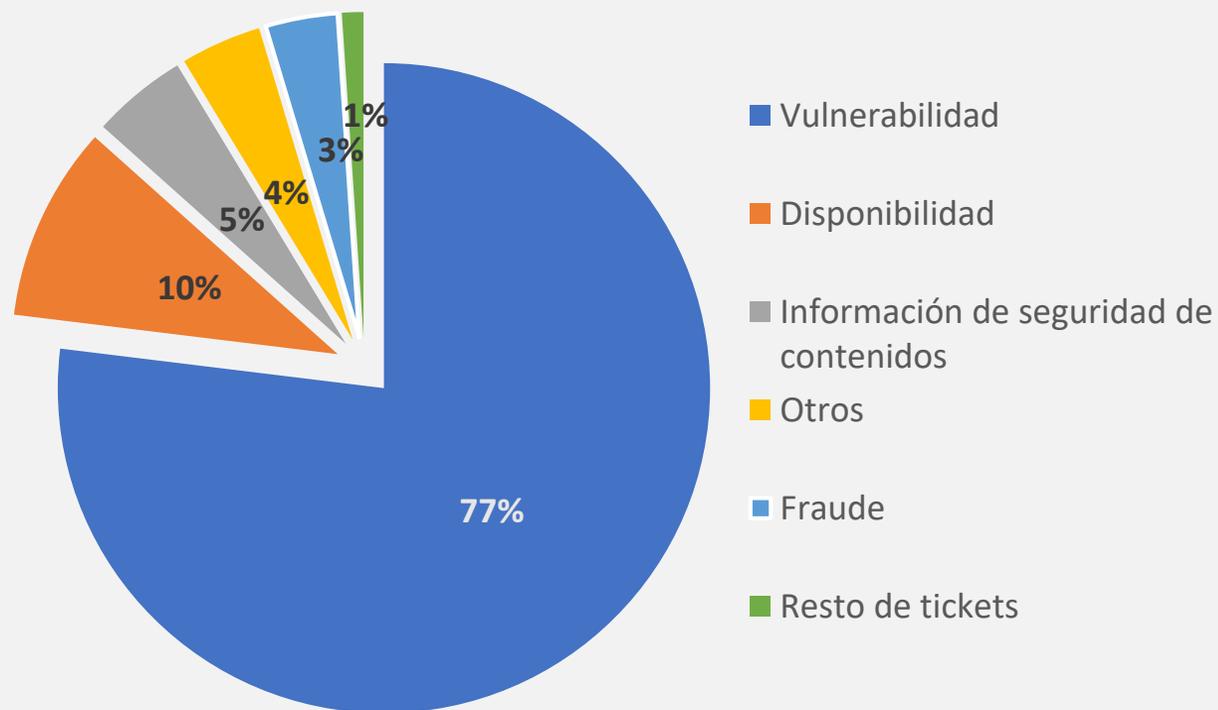
Estos tickets los ordenamos en categorías definidas por ENISA (Agencia de Ciberseguridad de la Unión Europea) según el tipo de incidente de seguridad informática al que corresponden.

**Más información sobre esta clasificación:**  
<https://www.csirt.gob.cl/matriz-clasificacion-incidentes>

## TIPO DE INCIDENTE

La enorme mayoría de los incidentes corresponde a la categoría **Vulnerabilidad**

El CSIRT de Gobierno reitera su llamado a actualizar cuánto antes sea posible sus software, ya que así se parchan dichas vulnerabilidades, que corresponden a deficiencias de seguridad, las que pueden ser explotadas por ciberdelincuentes.



# EMITIDOS A INSTITUCIONES PÚBLICAS Y PRIVADAS

Nuestra vinculación con el sector privado es fundamental para contribuir a mantener un ciberespacio más seguro, además de proteger los sistemas e información de todos los chilenos. Y para lograr esa vinculación, el intercambio de información y buenas prácticas juegan un rol fundamental. Por esto, adquirimos el compromiso de alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas.

Tickets	Privado	Público	Total
Vulnerabilidad	95	1.500	1.595
Disponibilidad	15	186	201
Información de seguridad de contenidos	86	12	98
Otros	64	19	83
Fraude	67	7	74
Código Malicioso	15	3	18
Intentos de Intrusión	1	1	2
Intrusión	2	-	2
Contenido Abusivo	-	-	-
Recopilación de Información	-	-	-
<b>Total</b>	<b>345</b>	<b>1.728</b>	<b>2.073</b>

**Públicas**

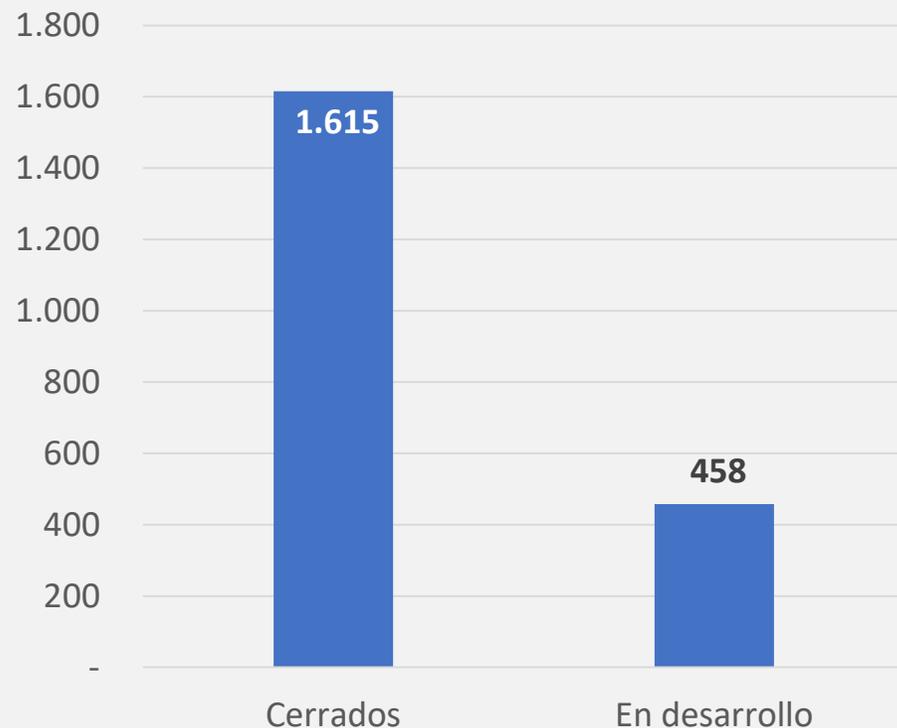
**83%**

**Privadas**

**17%**

## PROCESAMIENTO DE TICKETS

Este mes, el 78% de los tickets generados en el período logró ser cerrado exitosamente (contra un 69% en agosto), mientras el resto seguirá siendo procesado en octubre.



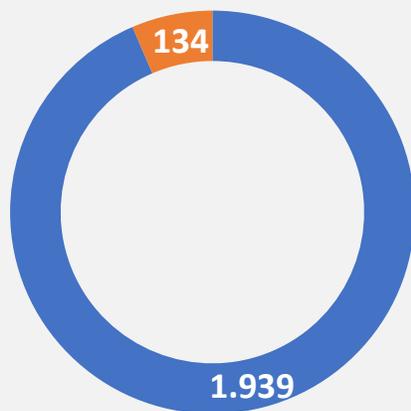
Recordamos lo esencial de obtener retroalimentación de las gestiones que se realizan en función del hallazgo encontrado.

Los invitamos a seguir cerrando brechas de seguridad para tener un Estado más ciberseguro

<https://www.csirt.gob.cl>

## PROCEDENCIA DE TICKETS

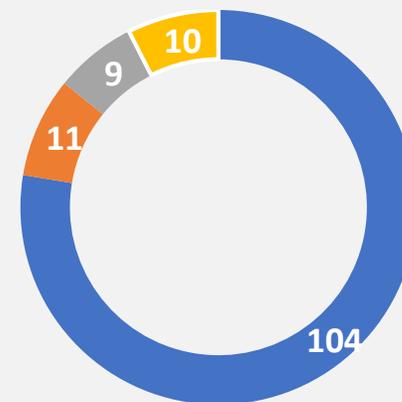
Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno que corresponde al **94%**, fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante software utilizado por el CSIRT.



■ Servicios Internos ■ Servicios Externos

Fono  
CSIRT:  
1510

Por otro lado, los tickets de origen externo (un **6%**), se originan por colaboradores vinculados al CSIRT vía contractual o se generan a través de reportes ciudadanos a través nuestro call center y por formulario web (**77%** de los tickets externos), alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.



■ Formulario web ■ Email ■ Call center ■ Otros

# BOLETINES DE SEGURIDAD CIBERNÉTICA, SEPTIEMBRE 2022

Aquí pueden revisar los boletines que comparte el CSIRT de Gobierno cada semana, con las principales alertas, vulnerabilidades y campañas que realizamos en el período.

Boletín de Seguridad Cibernética n°165 – 26 de agosto al 1 de sept.: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-165>

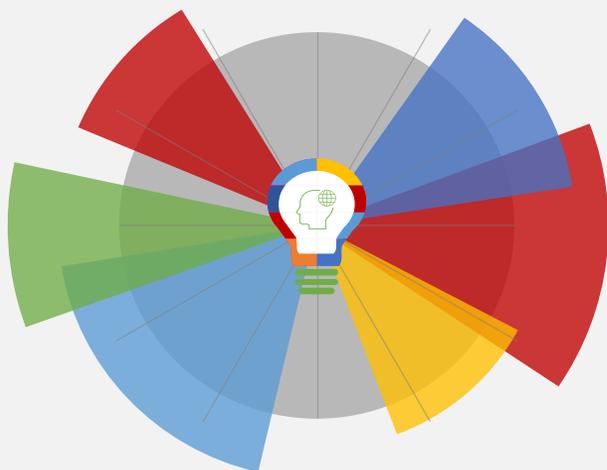
Boletín de Seguridad Cibernética n°166 – 2 al 8 de septiembre: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-166/>

Boletín de Seguridad Cibernética n°167 – 9 al 15 de septiembre: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-167/>

Boletín de Seguridad Cibernética n°168 – 15 al 22 de septiembre: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-168/>

Boletín de Seguridad Cibernética n°169 – 23 al 29 de septiembre: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-169/>

Boletín de Seguridad Cibernética n°170 – 30 sept. al 6 de octubre: <https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-170/>



Indicadores	B 165	B 166	B 167	B 168	B 169	B 170
CVE	1	2	65	1	58	48
IP	11	12	4	11	11	11
Hash	20	10	7	20	22	19
URL	9	5	6	9	10	12

# CAMPAÑAS DE CONCIENTIZACION

## Ciberconsejos para descargar apps seguras

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-descargar-apps-seguras/attachment/1-31/>

## Ciberdiccionario Volumen 16

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-16/>

## Ciberdiccionario Volumen 17

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-17/>



### En el mundo existen...

Más de cinco millones de apps disponibles para descarga. Sin embargo, algunas están creadas con fines maliciosos, como espionaje, acoso, suplantación de identidad, robo de datos, contraseñas e incluso información bancaria.



## Ciberdiccionario

**Command and Control (C&C):** El equipo de un ciberdelincuente que controla a otros distancia de forma no autorizada. Desde estos servidores C&C, los atacantes pueden ejecutar acciones en los equipos de sus víctimas, como robar información confidencial, incluso manejar una red de equipos infectados (conocida como botnet).

## Ciberdiccionario

### 4. SUPLANTACIÓN DE IDENTIDAD:

Es el uso malicioso de la imagen de personas, marcas o instituciones por parte de terceros. La suplantación de identidad es utilizada con distintos fines, ya sea para cometer actos ilícitos o con el objetivo de acosar a una persona en particular. En ambos casos es considerado un delito.

# CAMPAÑAS DE CONCIENTIZACION

## Ciberconsejos | Cómo proteger nuestro correo institucional

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-correo-institucional/>

### *Buenas prácticas* PARA EL USO DEL *Correo institucional*



El correo electrónico permite guardar información, registrarse en sitios web, contratar servicios, etc., por ende se ha vuelto un gran atractivo para los delincuentes.

¿Cuáles son los riesgos?

#### SUPLANTACIÓN



Si un tercero ingresa a tu correo, puede usurpar tu identidad, enviar mail y utilizarla para cometer estafas y/o enviar campañas de phishing y malware.

## Ciberdiccionario Volumen 18

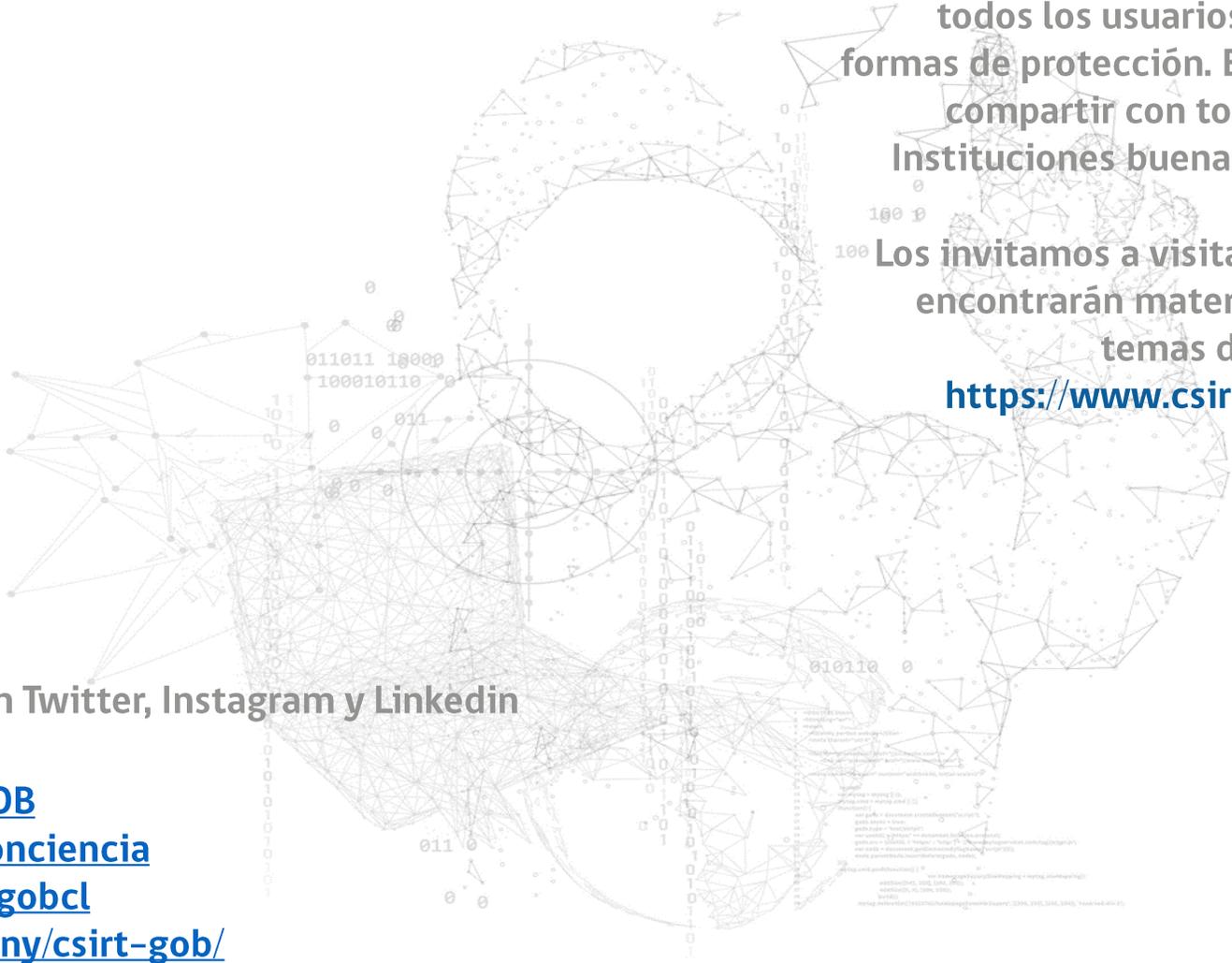
<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-18/>



### Ciber diccionario

**Archivo ejecutable:** Archivos que contienen instrucciones para el computador, como la descarga e instalación de software. Hacer clic en ellos sin conocer su procedencia es riesgoso: hay delincuentes que envían emails con ejecutables, y mensajes que convencen a su víctima de iniciarlos, resultando en su infección con software malicioso.





Para prevenir una amenaza, es fundamental que todos los usuarios conozcan los riesgos y las formas de protección. El CSIRT de Gobierno recomienda compartir con todos los trabajadores de las Instituciones buenas prácticas de ciberseguridad.

Los invitamos a visitar el sitio web del CSIRT, donde encontrarán material educativo sobre diversos temas de ciberseguridad.

<https://www.csirt.gob.cl/recomendaciones/>

Síguenos también en Twitter, Instagram y LinkedIn

[twitter.com/CSIRTOGOB](https://twitter.com/CSIRTOGOB)

[twitter.com/CSIRTConciencia](https://twitter.com/CSIRTConciencia)

[instagram.com/csirtgobcl](https://instagram.com/csirtgobcl)

[linkedin.com/company/csirt-gob/](https://linkedin.com/company/csirt-gob/)