



## DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

Nº EXPEDIENTE: 001-072325

FECHA: 20 de septiembre de 2022

NÚMERO DE REGISTRO: REGAGE22e00041144547

NOMBRE: [REDACTED]

DN [REDACTED]

CORREO ELECTRÓNICO [REDACTED]

Le agradecemos que se ponga en contacto con el Ministerio de Ciencia e Innovación para ejercer su derecho de acceso a la información pública, consistente en:

### SOLICITUD

#### Asunto

CIBERATAQUE AL CSIC

#### Información que solicita

Por la presente solicito información al amparo de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información y Buen Gobierno. -Copia de los informes que cualquier servicio del ministerio haya podido emitir tras el ciberataque sufrido por el CSIC los días 16 y 17 de julio de 2022. -Relación de las adjudicaciones que este ministerio haya podido llevar a cabo para reforzar los sistemas de detección y blindaje a fin de evitar episodios como el citado. Ruego que se detalle nombre del adjudicatario, importe, concepto del encargo y organismo licitador.

### TRAMITACIÓN DE LA SOLICITUD

El cómputo del plazo para resolver se inicia el día 20 de septiembre de 2022, de acuerdo con lo dispuesto por el artículo 20.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

El plazo se ha ampliado por un mes más.

### RESOLUCIÓN | CONCESIÓN PARCIAL DE ACCESO A LA INFORMACIÓN

Analizada su solicitud, la Secretaría General de Investigación del Ministerio de Ciencia e Innovación resuelve **conceder parcialmente** el acceso a la información solicitada.





El artículo 14 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la Información y buen gobierno prevé que el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:

- a) La seguridad nacional.
- b) La defensa.
- c) Las relaciones exteriores.
- d) La seguridad pública.
- e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
- h) Los intereses económicos y comerciales
- i) La política económica y monetaria.
- j) El secreto profesional...

Es evidente que, frente a un ciberataque de origen extranjero, y ante el riesgo de posible reiteración en el futuro, la divulgación de la información completa de los informes internos que cualquier servicio del ministerio hubiera podido emitir, supondría un peligro cierto de divulgar incondicionadamente aspectos relativos a la seguridad informática del organismo en un ejercicio que atentaría directamente contra las previsiones reproducidas que excepcionan y limitan el derecho de acceso.

Junto a ello, resulta también de aplicación la previsión del artículo 18 de la citada Ley de transparencia que prevé que se inadmitirán a trámite, mediante resolución motivada, las solicitudes:

- b) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas.

Sin perjuicio de ello se le traslada la información más relevante al respecto.

El Consejo Superior de Investigaciones Científicas, tras detectar en la mañana del 18 de julio comportamientos anómalos en varios de sus dispositivos que presentaban indicios de haber sido infectados por un malware de tipo ransomware procedió a su aislamiento, evitando de este modo su propagación. Asimismo, siguiendo los procedimientos establecidos ante incidentes de esta naturaleza, puso inmediatamente los hechos en conocimiento del CCN (Centro Criptológico Nacional) y COCS (Centro de Observaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos).

A partir de ese momento, fueron siendo aplicadas nuevas medidas de contención dictadas por ambas entidades, entre otras:

- Aislamiento de las comunicaciones:
  - Corte de la conexión a Red SARA
  - Corte de la comunicación interna en edificios
  - Aislamiento de las sedes del CSIC para evitar posibles desplazamientos laterales.
- Cierre del acceso Web a las plataformas
- Bloqueo del acceso a través de sistemas VPN
- Aislamiento de posibles máquinas o plataformas afectadas
- Despliegue de nuevo software de seguridad con capacidad de bloqueo por comportamiento







- Inclusión de los Indicadores de Compromiso (IoC) relacionados con el incidente en los sistemas de seguridad de la entidad.
- Fortificación de los sistemas afectados.
- Restauración de los sistemas involucrados, por medio de copias de seguridad.

En paralelo, se realizaron los análisis forenses correspondientes que evidenciaron indicios de actividad maliciosa con despliegue del ransomware Kid (perteneciente al grupo Vice Society) y encriptación de datos entre la madrugada del día 16 y la mañana del 17 de julio. En este periodo, los atacantes tratan de desplegar el ransomware en el mayor número de sistemas posible; siendo detectado y parado en gran parte de los sistemas (1.146) en los que intentan el despliegue por el software de seguridad instalado.

El impacto del ciberataque ascendió a 30 servidores y menos de 10 equipos de usuario final correspondientes, tanto de los servicios centrales del CSIC como de 6 de sus 149 centros, institutos y sedes. Se produjo asimismo exfiltración de información. La información encriptada de carácter corporativo fue restaurada sin pérdida de información.

La restauración de comunicaciones y servicios se fue realizando paulatinamente, conforme se iban securizando equipos e infraestructuras. A fecha de hoy todos los centros del CSIC tienen restablecidas las comunicaciones y más de 14.000 equipos (servidores y equipos de usuario final) tienen reforzadas todas las medidas de seguridad. El CSIC, no obstante, trabaja de manera continua para el fortalecimiento de la seguridad informática.

Finalmente, y por las mismas razones expuestas, no se puede informar detalladamente del contenido de las contrataciones técnicas relacionadas con el ciberincidente. Destacándose, no obstante, por su vinculación directa con el mismo, una contratación gestionada y adjudicada por el CSIC mediante procedimiento de emergencia para el desempeño de asistencia técnica para un servicio de instalación de software de seguridad (en 6.700 equipos de usuario, servidores u otro equipamiento) de 40 diversos centros e institutos del CSIC distribuidos por todo el territorio nacional que presentaban carencia de recursos técnicos para abordar la instalación del software en todos los equipos de su sede. La empresa adjudicataria fue ECONOCOM SERVICIOS, S.A por un coste de 61.008,00€, sin IVA.

Con anterioridad a esa contratación se habían realizado distintas inversiones adicionales para el reforzamiento de la seguridad.

De acuerdo con el art.15.5 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, le recordamos que la normativa vigente en materia de protección de datos (Ley Orgánica 3/2018 y Reglamento 2016/679 del Parlamento Europeo y del Consejo) es aplicable al tratamiento de los datos personales que contiene la presente resolución.

Contra esta resolución, que pone fin a la vía administrativa, podrá interponer reclamación ante el Consejo de Transparencia y Buen Gobierno o bien recurso contencioso administrativo:

- De forma previa y potestativa, podrá interponer, en el plazo de un mes, reclamación ante el Consejo de Transparencia y Buen Gobierno, conforme con lo recogido por el art.24 de la Ley 19/2013.
- En el plazo de dos meses, podrá interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia Madrid de conformidad con lo dispuesto en la Ley 29/1998 y en la Ley 39/2015.

En ambos casos, el plazo para interponer recurso o reclamación se computará a partir del día siguiente al de la notificación de esta resolución.

LA SECRETARIA GENERAL DE INVESTIGACIÓN,

Raquel Yotti Álvarez

CSV :

DIRECCIÓN DE VALIDACIÓN : <https://sede.administracion.gob.es/pagSedeFront/servicios/consultaCSV.htm>

FIRMANTE(1) : RAQUEL YOTTI ALVAREZ | FECHA : 21/10/2022 13:41 | Sin acción específica

