



# Planes de contingencia y gestión de crisis en México



# Panorama

6 de julio de 2020 – CONDUSEF

## EL ECONOMISTA

### Anonymous hackea el portal de Condusef y amaga con derribar el sitio web de Banxico

Los fallos obedecerían a hackeos de parte del grupo Anonymous México, en reclamos contra el presidente Andrés Manuel López Obrador respecto a la transparencia en instituciones del gobierno federal.

Redacción  
06 de julio de 2020, 18:47



7 de julio de 2020 – Banco de México

## EL FINANCIERO

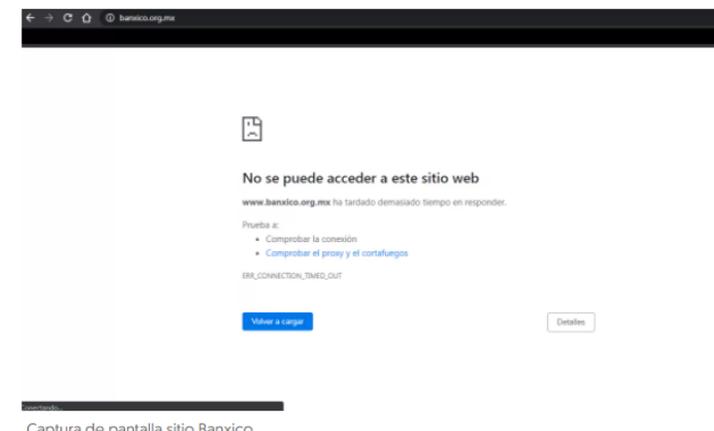
ECONOMÍA MERCADO

ECONOMÍA

### Banxico confirma intento de hackeo a su sitio web

Esto se da luego de que el lunes se cayera también la página de Condusef, luego de un presunto hackeo.

REDACCIÓN 07/07/2020 Actualización 07/07/2020 - 16:25



Fuente CONDUSEF: <https://www.economista.com.mx/politica/Anonymous-hackea-el-portal-de-Condusef-y-amaga-con-derribar-el-sitio-web-de-Banxico-durante-la-mananera-de-AMLO-20200706-0088.html>

Fuente Banco de México: <https://www.elfinanciero.com.mx/economia/se-cae-sitio-de-banxico-anonymous-mexico-se-adjudica-hackeo>



# Panorama

5 de septiembre de 2020 – Banco Estado (Chile)

**FayerWayer.** MÓVILES VIDEOJUEGOS CIENCIA INTERNET HARDWARE ENTRETENIMIENTO **Wayer** MANUALES



**Banco Estado: Ataque Cibernético es causado por poderoso Ransomware**  
07 SEPTIEMBRE 2020

La plataforma bancaria sufrió un ataque informático que obligó a cerrar sucursales y causó intermitencia en los servicios digitales.  por **MARTÍN CALDERÓN**

COMPARTIDOS    

Cientos de chilenos se quedaron hoy lunes sin poder realizar trámites bancarios. Banco Estado, la otrora banca estatal nacional, sufrió un ataque informático durante la semana pasada.

La vulnerabilidad, que se presume habría ocurrido en equipos dentro de una sucursal y no en su plataforma digital, obligó al cierre de sucursales durante hoy lunes. El propio banco confirmó a través de su cuenta de Twitter dicho cierre y ha presentado diversas intermitencias en su plataforma digital durante los últimos tres días.

El ciberataque, según confirman diversas fuentes públicas y privadas, se trataría de un malware del tipo "ransomware", llamado "Sodinokibi" o "Revil". Este software especializado es el que se presume habría entrado a alguno de los equipos de Banco Estado.

**BancoEstado** @BancoEstado

Información importante sobre nuestra red de atención

**INFORMACIÓN DE PRENSA**

Queremos informar que debido a la acción de terceros a través de un software malicioso, nuestras sucursales no estarán operativas y permanecerán cerradas hoy. Estamos haciendo todos los esfuerzos para poner en funcionamiento algunas sucursales durante la jornada. En nuestros canales oficiales estaremos informando cualquier novedad.

Hemos hecho las denuncias correspondientes y llamamos a todo a quien tenga información a hacer las denuncias.

Reiteramos nuestro llamado a utilizar nuestros canales remotos o digitales, tales como CajaVecina, Cajeros Automáticos, App y la página web.

Estamos haciendo todos nuestros esfuerzos para contener y revertir esta acción maliciosa de personas que buscan afectar la acción cotidiana de millones de chilenos que utilizan diariamente BancoEstado. Seguimos trabajando para restablecer en su totalidad los sistemas operativos afectados.

Es importante reafirmar que no ha existido afectación alguna a los fondos de nuestros clientes o al patrimonio de BancoEstado.

Lamentamos los inconvenientes que esta situación pudiese causar e invitamos a nuestros clientes a utilizar los canales digitales.

Para atender dudas o consultas, disponemos de nuestro call center 600 200 7000 o nuestras redes sociales. En nuestros canales oficiales actualizaremos esta información durante todo el día.

7:07 AM · Sep 7, 2020 · Twitter for iPhone

823 Retweets 206 Quote Tweets 774 Likes

Fuente: <https://www.fayerwayer.com/2020/09/banco-estado-hackeo-ransomware/>



# Panorama

11 de septiembre de 2020 – Adeslas (España)

**El Confidencial** Inicio sesión Suscribirse

TECNOLOGÍA CIENCIA MÓVILES EMPRENDEDORES APPS INTERNET BLOGS

**Tres semanas KO por un ciberataque: así tienen secuestrados los sistemas de Adeslas**

La compañía de salud, una de las más grandes de España, lleva desde el 11 de septiembre sin poder operar con normalidad debido a un potente ataque 'ransomware'

Sede de SeguCaixa Adeslas. (Foto: Wikimedia)

**03/10/2020 05:00** - ACTUALIZADO 05/10/2020 16:38

La primera información llegó el pasado 11 de septiembre. La aseguradora Adeslas, una de las más grandes de su sector en España, anunciaba que había sufrido un **grave ataque informático** y que tenía problemas para seguir trabajando con normalidad. En ese primer momento **no se dieron más detalles sobre el tipo de ataque** ni el calado total del mismo, pero tres semanas después, el problema sigue sin resolverse y se empiezan a esclarecer algunos puntos. Como ha confirmado la empresa, son víctimas de **uno de los temidos 'ransomware'** que ya han afectado a muchísimas otras instituciones y ahora han metido en serios problemas a esta gran empresa.

Los estragos de este ataque, centrado en bloquear toda la estructura informática, se muestran claramente con un pequeño vistazo. Se ven **en las webs de la empresa**, y se dejan notar incluso **en las redes sociales**, donde su cuenta oficial responde cada día a quejas de todo tipo de pacientes. Tal es la situación que a día de hoy **ni siquiera se puede acceder al área de cliente en la web**, casi cualquier apartado de sus páginas viene acompañado de un mensaje en el que se avisa que ahora mismo no está todo el servicio disponible y la situación interna es de lo más delicada, como comentan a este periódico fuentes conocedoras de la situación. Tanto los hospitales asociados a la aseguradora como los trabajadores llevan semanas bajo mínimos u obligados a recuperar métodos de hace años.

**Chantaje a Adif: cibercriminales amenazan con difundir 800GB de información sensible**

El grupo REvil asegura que, si la empresa pública no se atiene a sus condiciones (previamente, un rescate económico), difundirá online sus contratos y facturas, así como otros datos.

"No se puede ni encender un ordenador. Está todo fatal, no puedes ver, ni hacer radiografías, **no se puede ver a quién tienes [en agenda] y quién no**, no se puede ver quién ha venido y qué les están haciendo, el historial [médico]", explica una fuente conocedora de la situación y que convive a diario con estos

Fuente: [https://www.elconfidencial.com/tecnologia/2020-10-03/adeslas-ransomware-hackers-ciberataque-datos\\_2773032/](https://www.elconfidencial.com/tecnologia/2020-10-03/adeslas-ransomware-hackers-ciberataque-datos_2773032/)



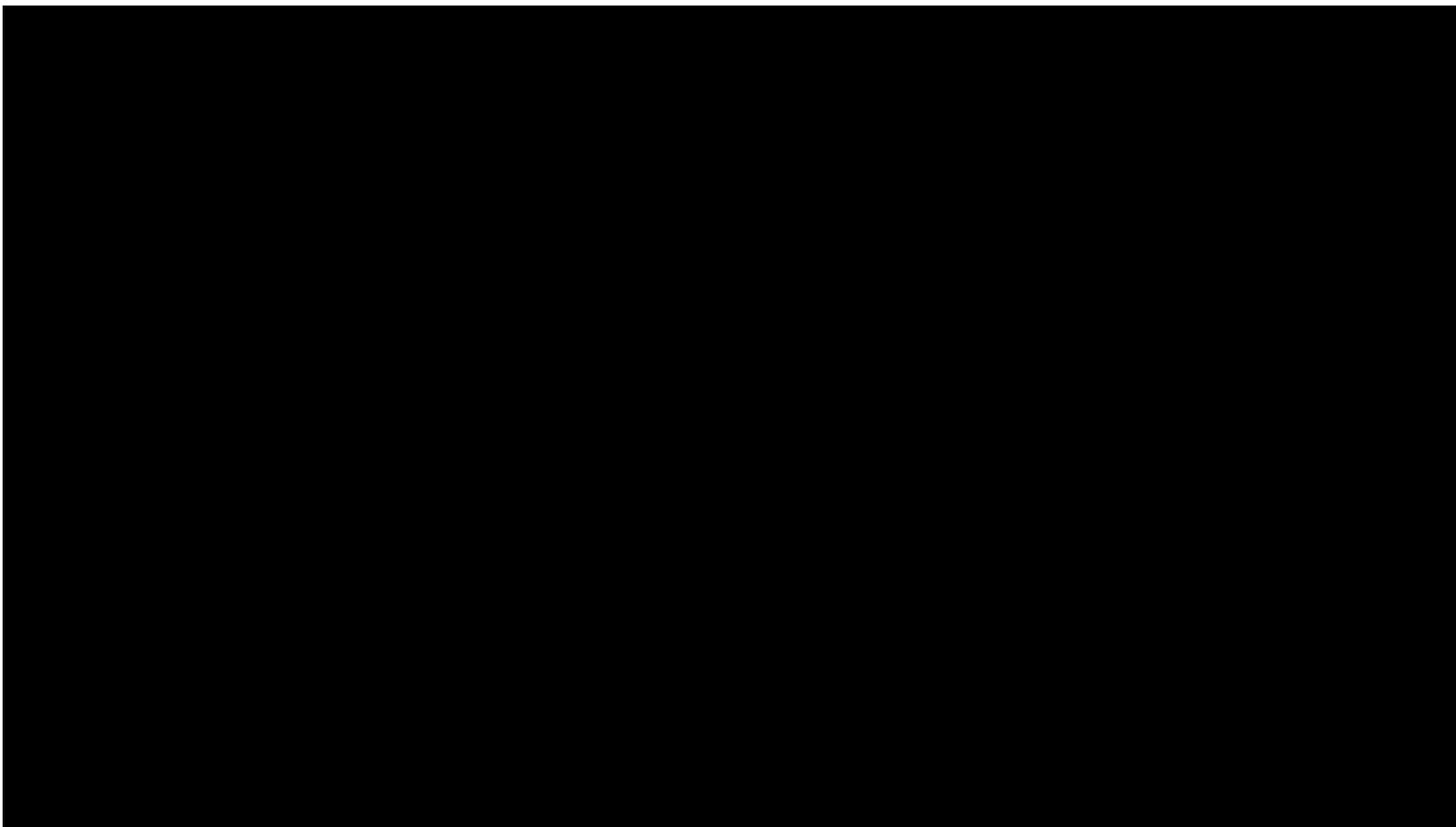
## Panorama

Los ataques han cambiado de objetivo, pasando a dirigirse contra las grandes multinacionales, instituciones financieras, instituciones de gobierno e infraestructuras esenciales, a través de sus empleados y clientes.





# Ataque Watering Hole





## Herramientas mas comunes utilizadas para perpetrar delitos cibernéticos durante el COVID-19

### Ataque y explotación de las plataformas y procesos remotos

- Manipulación digital de documentos de identidad en plataformas de identificación remota.
- Aprovechamiento de credenciales comprometidas para acceder y controlar cuentas remotamente.

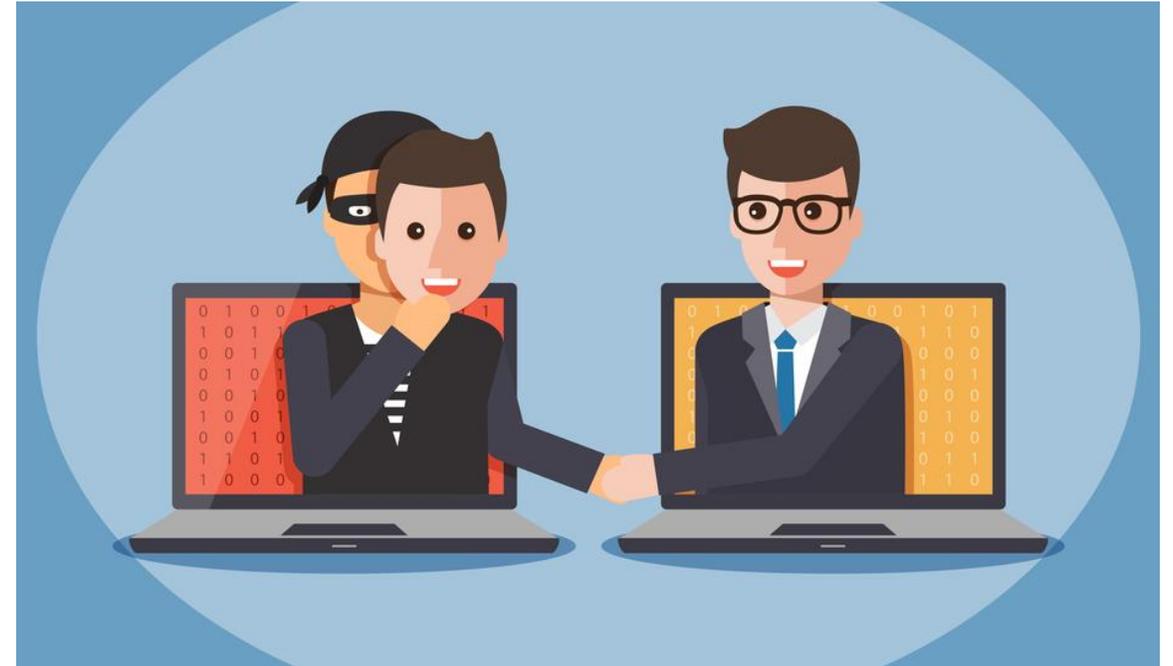




## Herramientas mas comunes utilizadas para perpetrar delitos cibernéticos durante el COVID-19

### Suplantación de la identidad, programas malignos y extorsión

- Comunicaciones a clientes o usuarios aparentemente legítimas a través de email.
- Distribución de malware a través de correos apócrifos, descargas, sitios web maliciosos o aplicaciones fraudulentas.
- Campañas en redes sociales con cuentas secuestradas de usuarios famosos.





## Herramientas mas comunes utilizadas para perpetrar delitos cibernéticos durante el COVID-19

### Compromiso de correo electrónico de negocios (BEC)

- Estafas utilizando cuentas de correo electrónico comprometidas.
- Utilizar ingeniería social para convencer a compañías para dirigir pagos a nuevas cuentas.
- Hacer uso de solicitudes urgentes como consecuencia de la pandemia.





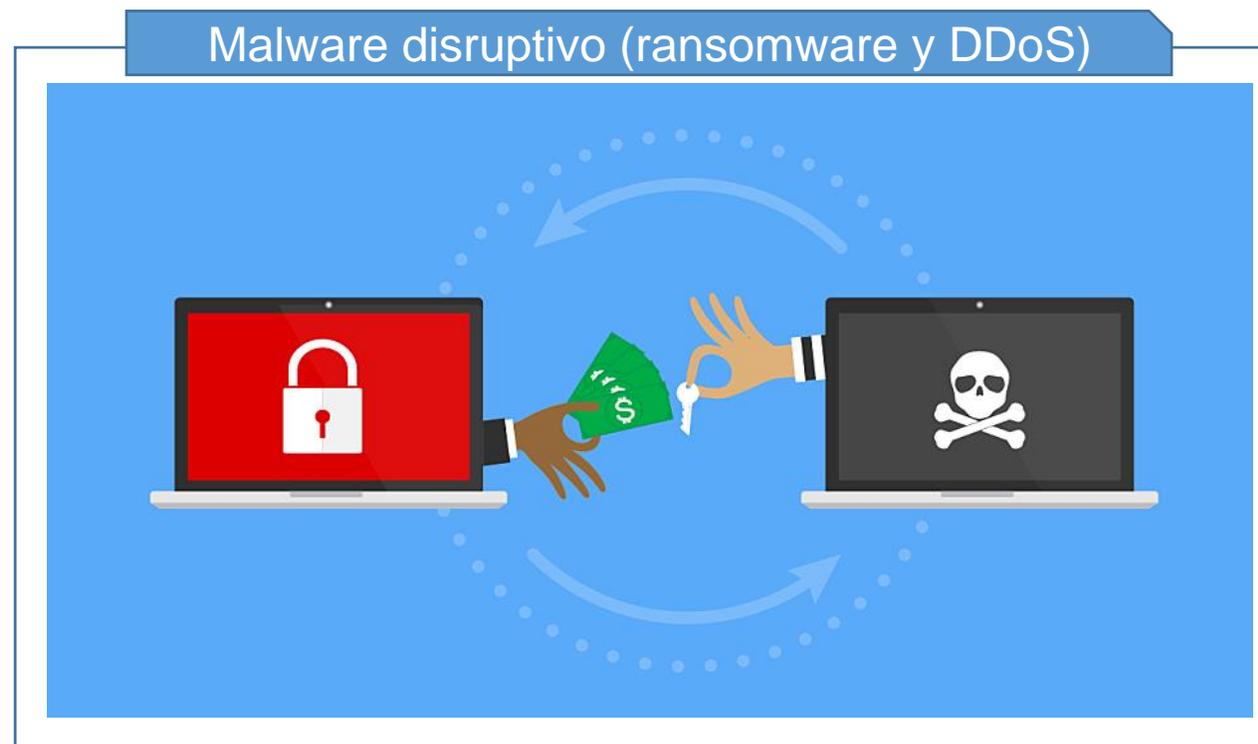
# Aspectos que han cobrado relevancia en el 2020

## Estafas por Internet y el phishing





# Aspectos que han cobrado relevancia en el 2020





# Aspectos que han cobrado relevancia en el 2020

Malware destinado a la obtención de datos





## Aspectos que han cobrado relevancia en el 2020

### Dominios maliciosos





# Aspectos que han cobrado relevancia en el 2020

## Desinformación





# Importancia de contar con un plan de continuidad

## Elementos relevantes

- Definir los escenarios que requieren un plan de continuidad
- Identificar y acordar los **procesos más críticos** y sus **tiempos máximos de inactividad**.
- Contar con **alternativas reales** que aseguren la continuidad de estos procesos.
- Tener definidos **roles y responsabilidades**.
- Saber cómo **actuar frente a los posibles escenarios de riesgo**.
- Planificar la **prueba periódica del plan**.
- Conocer los **aspectos a mejorar**, según los resultados de las pruebas.
- Ser conscientes de la importancia de **mantener actualizado el Plan**.





## Reflexiones sobre COVID-19

- La necesidad de acelerar los procesos de transformación digital
- La seguridad debe acompañarnos en todo lugar y en cada momento
- Las amenazas informáticas no están en confinamiento
- El impacto y el volumen de los ciberataques es cada vez mayor
- Los planes de contingencia deben estar actualizados y probados
- La continuidad en las operaciones debe considerar siempre la seguridad de la información
- Las crisis también traen oportunidades