

---

## **Alerta de Seguridad Informática (8FPH-00045-001)**

**Nivel de Riesgo: Alto**

**Tipo: Phishing**

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

### **Notificación**

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

---

### **Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco BCI.

El correo trata de persuadir a los clientes del Banco indicándoles que su cuenta se encuentra suspendida temporalmente, ya que su correo se encuentra registrado erróneamente, persuadiendo a los usuarios que deben normalizar la situación a través del enlace indicado en el correo, enlace que redirige a un sitio, supuestamente, del Banco BCI.

“Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño”

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

## Indicadores de compromisos

### Url's:

- [http://zgdgs\[.\]pl/-/https://www2.bci\[.\]cl/?cliente=](http://zgdgs[.]pl/-/https://www2.bci[.]cl/?cliente=)
- [http://atualizacionbci\[.\]com/elegir\[.\]php](http://atualizacionbci[.]com/elegir[.]php)
- [http://atualizacionbci\[.\]com/psn/acs\[.\]php](http://atualizacionbci[.]com/psn/acs[.]php)
- [http://atualizacionbci\[.\]com/emp/acs\[.\]php](http://atualizacionbci[.]com/emp/acs[.]php)

### Smtip Host

- node7911-env-5[.]cloud[.]unispace[.]io (203.26.broadband16.iol.cz [90.183.26.203])
- node7909-env-4[.]cloud[.]unispace[.]io (202.26.broadband16.iol.cz [90.183.26.202])
- node7913-env-6[.]cloud[.]unispace[.]io (204.26.broadband16.iol.cz [90.183.26.204])
- node7915-env-8[.]cloud-de[.]unispace[.]io (ip246.ip-51-89-44.eu [51.89.44.246])
- node7919-env-10[.]cloud-de[.]unispace[.]io (ip252.ip-51-89-44.eu [51.89.44.252])
- 

### Sender

- apache@node7911-env-5[.]cloud[.]unispace[.]io
- apache@node7909-env-4[.]cloud[.]unispace[.]io
- apache@node7913-env-6[.]cloud[.]unispace[.]io
- apache@node7915-env-8[.]cloud-de[.]unispace[.]io
- apache@node7919-env-10[.]cloud-de[.]unispace[.]io

**Subject:**

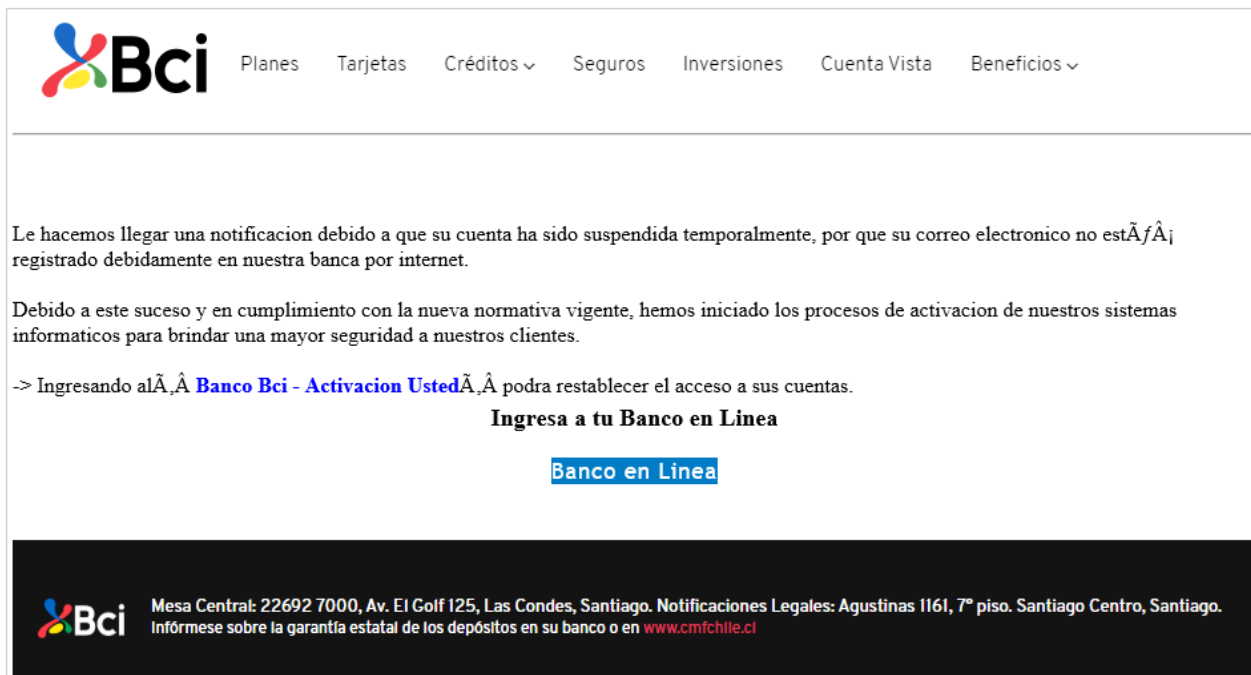
- Infoemail BCI - Importante - Servicio de Transferencias Bloqueado

**Imagen Phishing correo**



info\_email30485872@info30485872bci.cl

✓ Infoemail BCI - Importante - Servicio de Transferencias Bloqueado - ( 971363918144 )



The screenshot shows a phishing email from BCI. At the top left is the BCI logo. To its right is a navigation menu with links: Planes, Tarjetas, Créditos (with a dropdown arrow), Seguros, Inversiones, Cuenta Vista, and Beneficios (with a dropdown arrow). The main body of the email contains the following text:

Le hacemos llegar una notificación debido a que su cuenta ha sido suspendida temporalmente, por que su correo electrónico no está registrado debidamente en nuestra banca por internet.

Debido a este suceso y en cumplimiento con la nueva normativa vigente, hemos iniciado los procesos de activación de nuestros sistemas informáticos para brindar una mayor seguridad a nuestros clientes.


-> Ingresando al [Banco Bci - Activación Usted](#) podrá restablecer el acceso a sus cuentas.

**Ingresar a tu Banco en Línea**

[Banco en Línea](#)

At the bottom of the email, there is a black footer bar containing the BCI logo and the following text: Mesa Central: 22692 7000, Av. El Golf 125, Las Condes, Santiago. Notificaciones Legales: Agustinas 1161, 7° piso. Santiago Centro, Santiago. Infórmese sobre la garantía estatal de los depósitos en su banco o en [www.cmfc Chile.cl](http://www.cmfc Chile.cl)

## Imagen Sitio Web

 [atualizacionbci.com/elegir.php](http://atualizacionbci.com/elegir.php)



**Acceso Persona.**

**Acceso Empresa.**

**Inicie sesión en su cuenta en línea.**

Seleccione el tipo de acceso que desea.

atualizacionbci.com/emp/acs.php



## Acceso a cuenta - Empresa.

Ingrese los datos requeridos para continuar.  
Ingrese su número RUT y Clave.

RUT.

Su clave de acceso.

**Inicia Sesión**

atualizacionbci.com/psn/acs.php



## Acceso a cuenta - Persona.

Ingrese los datos requeridos para continuar.

Ingrese su número RUT y Clave.

Su número de RUT.

Su clave de acceso.


**Inicia Sesión**

## Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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 que sean los oficiales

## Contactos

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

 + (562) 24863850

 @CSIRTGOB

 <https://www.linkedin.com/company/csirt-gob>