

Alerta de seguridad cibernética	8FFR21-00893-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2021
Última revisión	11 de Enero de 2021

## 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 loC 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 loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude 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 fraude, 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.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de una página fraudulenta que intenta suplantar al Banco Estado, lo que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

## Indicadores de compromiso

### URL sitio falso

<http://axentisgroup.com/rudy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html>

### Certificado Digital

Fecha Válido	26-01-2021
Fecha Término	26-04-2021
Emitido	Let's Encrypt R3

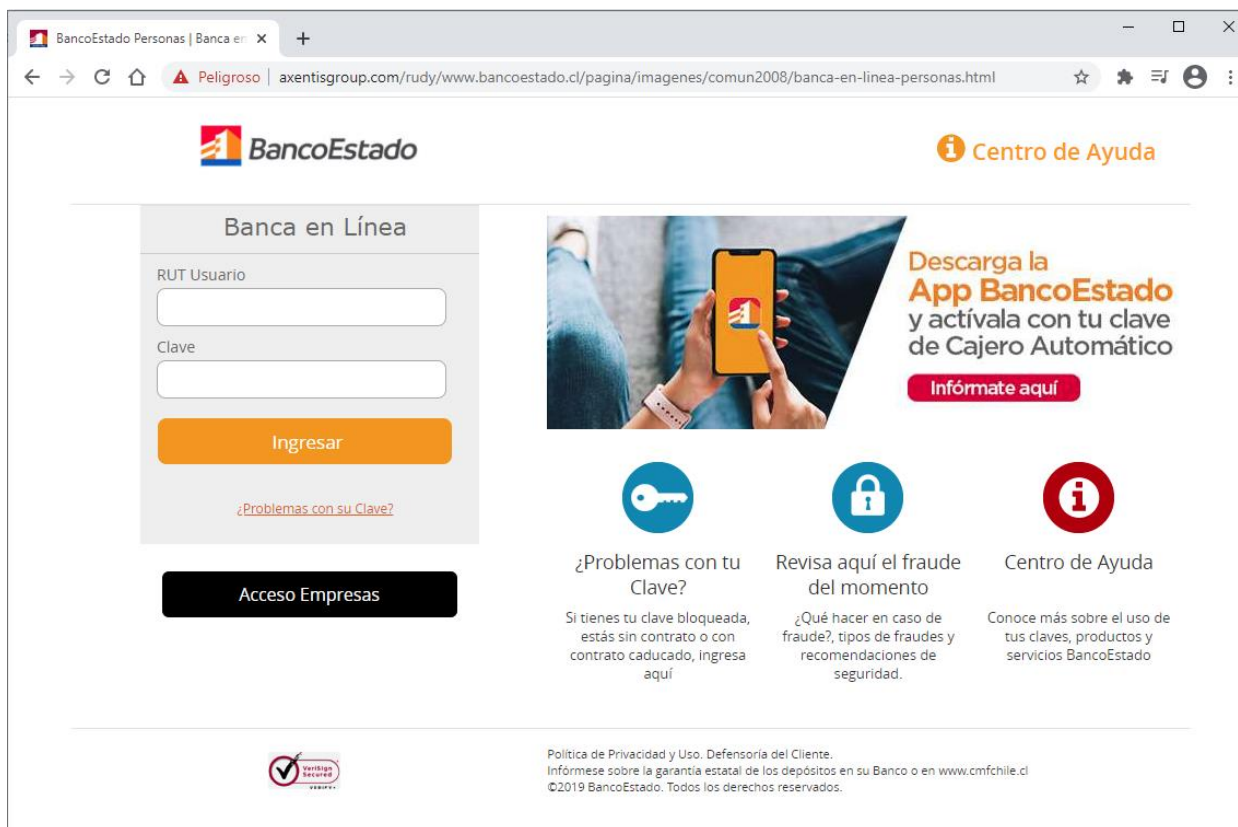
### Datos Alojamiento

IP	[185.98.131.140]
Número de Sistema Autónomo (AS)	16347
Etiqueta del Sistema Autónomo	ADISTA SAS
País	FR
Registrador	RIPE

### Datos del Dominio

Nombre de Dominio	axentisgroup[.]com
Creado	23-10-2008
Expira	23-10-2021
Información del Registrador	ENOM, INC.
ID IANA	48
Correo Electrónico	abuse@namecheap.com
Name Server	ns2027.registrosdns.com ns2028.registrosdns.com

## Imagen del sitio



The screenshot shows the 'Banca en Línea' page of BancoEstado. The browser address bar shows the URL: [axentisgroup.com/rudy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html](http://axentisgroup.com/rudy/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html). The page features the BancoEstado logo, a 'Centro de Ayuda' link, and a login form with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is a 'Acceso Empresas' button. To the right, there is a promotional banner for the 'App BancoEstado' with a 'Descarga la App BancoEstado y actívala con tu clave de Cajero Automático' message and an 'Infórmate aquí' button. Below the banner are three circular icons: a key, a padlock, and an information icon. Each icon has a corresponding heading and text: '¿Problemas con tu Clave?' (Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí), 'Revisa aquí el fraude del momento' (¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad), and 'Centro de Ayuda' (Conoce más sobre el uso de tus claves, productos y servicios BancoEstado). At the bottom, there is a 'Verifica Seguro' logo and a footer with the text: 'Política de Privacidad y Uso. Defensoría del Cliente. Infórmese sobre la garantía estatal de los depósitos en su Banco o en [www.cmfchile.cl](http://www.cmfchile.cl) ©2019 BancoEstado. Todos los derechos reservados.'

## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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 sean los oficiales.