



PERÚ

Presidencia  
del Consejo de Ministros

Secretaría de Gobierno  
y Transformación Digital



Siempre  
con el pueblo



# ALERTA INTEGRADA DE SEGURIDAD DIGITAL



Lima, 25 de setiembre de 2022

## ALERTA INTEGRADA DE SEGURIDAD DIGITAL



### N° 262-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.


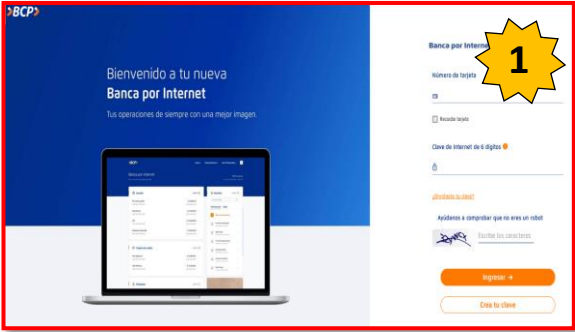

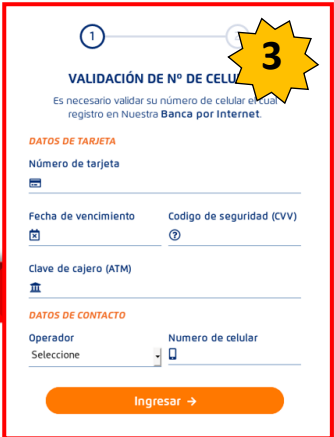

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

## Contenido

Phishing, suplantado la identidad del sitio web “Banca por Internet” del Banco de Crédito del Perú .....4

Índice alfabético .....6

		ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 262		Fecha: 25-09-2022
				Página 04 de 06
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>			
Nombre de la alerta	Phishing, suplantado la identidad del sitio web "Banca por Internet" del Banco de Crédito del Perú			
Tipo de ataque	Phishing	Abreviatura	Phishing	
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de Subfamilia	G02	
Clasificación temática familia	Fraude			
Descripción				
<p>1. A través A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio web "Banca por Internet" del Banco de Crédito del Perú (BCP), el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, clave de internet, DNI, numero de celular, fecha de vencimiento, código de seguridad y clave de cajero.</p> <p>2. <b>Detalles del proceso de Phishing</b></p> <div style="display: flex; flex-direction: column; align-items: center;"> <div style="display: flex; align-items: center; margin-bottom: 20px;"> <div style="border: 2px solid red; padding: 5px; text-align: center;">  </div> <div style="margin: 0 20px; font-size: 2em; color: red;">➔</div> <div style="border: 1px solid blue; border-radius: 15px; padding: 10px; text-align: center;"> <p><b>Imagen 1:</b></p> <p>Solicita datos bancarios como número de tarjeta y clave bancaria.</p> </div> </div> <div style="display: flex; align-items: center; margin-bottom: 20px;"> <div style="border: 2px solid red; padding: 5px; text-align: center;">  </div> <div style="margin: 0 20px; font-size: 2em; color: red;">➔</div> <div style="border: 1px solid blue; border-radius: 15px; padding: 10px; text-align: center;"> <p><b>Imagen 2:</b></p> <p>Solicita ingresar datos personales como el DNI.</p> </div> </div> <div style="display: flex; align-items: center; margin-bottom: 20px;"> <div style="border: 2px solid red; padding: 5px; text-align: center;">  </div> <div style="margin: 0 20px; font-size: 2em; color: red;">➔</div> <div style="border: 1px solid blue; border-radius: 15px; padding: 10px; text-align: center;"> <p><b>Imagen 3:</b></p> <p>Requiere validar los datos de la tarjeta como el número, fecha de vencimiento, código de seguridad, clave de cajero y el número de celular.</p> </div> </div> <div style="display: flex; align-items: center;"> <div style="border: 2px solid red; padding: 5px; text-align: center;">  </div> <div style="margin: 0 20px; font-size: 2em; color: red;">➔</div> <div style="border: 1px solid blue; border-radius: 15px; padding: 10px; text-align: center;"> <p><b>Imagen 4</b></p> <p>Luego, redirige a una ventana en la cual se menciona que el proceso de validación se ha completado con éxito.</p> </div> </div> </div>				

**3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:**

**INDICADORES DE COMPROMISO:**

- ✓ **URL:** hxxps[:]//slasher[.]pl/bczonaseguralbeta/inicia[-]sesion
- ✓ **Dominio:** slasher[.]pl
- ✓ **IP:** 5[.]252[.]229[.]113
- ✓ **Código:** 200
- ✓ **Longitud:** 6.74 KB
- ✓ **SHA-256:** d5a89e26beae0bc03ad18a0b0d1d3d75f87c32047879d25da11970cb5c4662a3

DETECTION	DETAILS	COMMUNITY
Security Vendors' Analysis ⓘ		
alphaMountain.ai	ⓘ Phishing	BitDefender ⓘ Malware
Emsisoft	ⓘ Phishing	G-Data ⓘ Malware
Heimdal Security	ⓘ Malicious	Netcraft ⓘ Malicious
Sophos	ⓘ Phishing	Webroot ⓘ Malicious

**OTRAS DETECCIONES:**

**MALICIOSO**

**https://slasher.pl/bczonasegur...**

Analizado en: 31/08/2022 15:20:54 (UTC)

Ambiente: windows 7 32 bits

Puntaje de amenaza: 100/100

Detección AV: 9% Sitio malicioso

Indicadores: 1 3 8

La red: 



↔

**malicioso**

Puntaje de amenaza: 100/100

**#suplantación de identidad**

**4. Algunas Recomendaciones:**

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta

## Índice alfabético

amenazas .....	4
antivirus .....	5
ciberdelincuentes .....	4
ciberespacio .....	4
monitoreo .....	4
Phishing .....	4
víctimas .....	4