PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 20 de marzo de 2024

069-2024-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

El nuevo ataque 'Loop DoS' afecta a cientos de miles de sistemas 4
Vulnerabilidad en la base de datos relacional Firebird 5
Vulnerabilidades en Google ChromeOS 6
Vulnerabilidad en la herramienta Jupyter Server Proxy 7
Vulnerabilidades en IBM InfoSphere Information Server 8
Vulnerabilidad en Mitel InAttend y CMG 9
Nueva campaña de Phishing que suplanta la identidad del Banco de Crédito del Perú (BCP) 10
Índice alfabético 12

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069	Fecha: 20-03-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El nuevo ataque 'Loop DoS' afecta a cientos de miles de sistemas		
Tipo de Ataque	Denegación de servicio DoS	Abreviatura	DoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. ANTECEDENTES:

Se ha descubierto que un novedoso vector de ataque de denegación de servicio (DoS) se dirige a protocolos de capa de aplicación basados en el Protocolo de datagramas de usuario (UDP), poniendo en riesgo a cientos de miles de hosts.

2. DETALLES:

Conocidos como ataques Loop DoS, estos métodos consisten en emparejar "servidores de dichos protocolos de forma que se desencadene una comunicación perpetua entre ellos", según los investigadores del CISPA Helmholtz-Center for Information Security.

Debido a su diseño inherente, UDP es un protocolo sin conexión que no verifica las direcciones IP de origen, por lo que es propenso a la suplantación de IP.

Por lo tanto, cuando los atacantes falsifican varios paquetes UDP para incluir la dirección IP de la víctima, el servidor de destino responde a la víctima (a diferencia del actor de la amenaza), creando un ataque de denegación de servicio (DoS) reflejado.

El último estudio encontró que ciertas implementaciones del protocolo UDP, como DNS, NTP, TFTP, Active Users, Daytime, Echo, Chargen, QOTD y Time, pueden usarse como armas para crear un bucle de ataque que se perpetúa a sí mismo.

"Empareja dos servicios de red de tal manera que siguen respondiendo indefinidamente a los mensajes del otro", dijeron los investigadores. "Al hacerlo, crean grandes volúmenes de tráfico que resultan en una denegación de servicio para los sistemas o redes involucradas. Una vez que se inyecta un disparador y el bucle se pone en movimiento, ni siquiera los atacantes pueden detener el ataque".

En pocas palabras, dados dos servidores de aplicaciones que ejecutan una versión vulnerable del protocolo, un actor de amenazas puede iniciar la comunicación con el primer servidor falsificando la dirección del segundo servidor, lo que hace que el primer servidor responda a la víctima (es decir, el segundo servidor) con un mensaje de error.

La víctima, a su vez, también mostrará un comportamiento similar, enviando otro mensaje de error al primer servidor, agotando efectivamente los recursos de cada uno y haciendo que cualquiera de los servicios no responda.

"Si un error como entrada crea un error como salida, y un segundo sistema se comporta igual, estos dos sistemas seguirán enviando mensajes de error de un lado a otro indefinidamente", explicaron Yepeng Pan y Christian Rossow.

3. RECOMENDACIONES:

- Mantener medidas para filtrar el tráfico falsificado.
- Configurar filtros en el router para controlar el acceso y el tráfico de paquetes.
- Instalar y mantener actualizados los últimos parches de seguridad de su software.
- Utilizar soluciones de seguridad integrales con protección en tiempo real y que te permita detectar y bloquear malware.

Fuente de Información:	• hxxps://thehackernews.com/2024/03/new-loop-dos-attack-impacts-hundreds-of.html • hxxps://hackarizona.org/es/cientos-de-miles-de-sistemas-afectados-por-un-nuevo-ataque-loop-dos/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069	Fecha: 20-03-2024
		Página: 5 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en la base de datos relacional Firebird		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo asignación de recursos sin límites ni estrangulamiento en la base de datos relacional Firebird. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario sin privilegios con acceso mínimo a un servidor, escribir una declaración con una longitud "CHAR" larga, lo que provocaría que el servidor falle debido a la corrupción de la pila.

2. DETALLES:

Firebird es un sistema de gestión de bases de datos relacionales de código abierto. Es un servidor SQL potente y confiable que ofrece características avanzadas y de alto rendimiento.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-41038 de tipo asignación de recursos sin límites ni estrangulamiento en las versiones 4.0.0 a 4.0.3 y la versión 5.0 beta1 de Firebird, se deben a una falla del servidor cuando un usuario usa una forma específica de declaración SET BIND. Cualquier usuario sin privilegios con acceso mínimo a un servidor puede escribir una declaración con una longitud "CHAR" larga, lo que provoca que el servidor falle debido a la corrupción de la pila.

A. Productos afectados:

- Servidor SQL Firebird, versiones 4.0.0 a 4.0.3 y la versión 5.0 beta1.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 4.0.4.2981 y 5.0.0.117 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://firebirdsql.org/en/snapshot-builds/ • hxxps://github.com/FirebirdSQL/firebird/security/advisories/GHSA-6fv8-8rwr-9692

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069**	**Fecha: 20-03-2024** **Página: 6 de 12**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Google ChromeOS		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo autorización faltante y error de validación de entrada en Google ChromeOS. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario local ejecutar código arbitrario con privilegios elevados, un atacante remoto no autenticado podría eludir el proceso de autenticación y obtener control total sobre el sistema creando una cuenta administrativa.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-0204 de tipo autorización faltante existe debido a la falta de comprobaciones de autorización relacionadas con el archivo InitialAccountSetup.xhtml junto con un problema de normalización de ruta. Un atacante remoto no autenticado puede eludir el proceso de autenticación y obtener control total sobre el sistema creando una cuenta administrativa.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-6040 de tipo error de validación de entrada, existe debido a un error no especificado dentro del kernel de Linux. Un usuario local puede ejecutar código arbitrario con privilegios elevados.

A. Productos afectados:

- Chrome OS: anterior a 120.0.6099.301.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://chromerereleases.googleblog.com/2024/03/long-term-support-channel-update-for_11.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069**	**Fecha: 20-03-2024**
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en la herramienta Jupyter Server Proxy		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo falta de autenticación para funciones críticas en la herramienta Jupyter Server Proxy. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir el proceso de autenticación y ejecutar código arbitrario en el sistema vulnerable.

2. DETALLES:

Jupyter Server Proxy es una herramienta que permite acceder a otros servicios web desde un entorno de Jupyter Notebook o JupyterLab. Con esta extensión, puedes integrar aplicaciones web, como dashboards interactivos, aplicaciones de visualización de datos o incluso servidores completos, dentro de tu flujo de trabajo de Jupyter.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-28179 de tipo falta de autenticación para funciones críticas, existe debido a que falta una verificación de autenticación en jupyter-server-proxy. Un atacante remoto puede acceder a cualquier punto final de websocket configurado para ser accesible y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Jupyter Server Proxy: 3.2.0 - 4.1.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://github.com/jupyterhub/jupyter-server-proxy/security/advisories/GHSA-w3vc-fx9p-wp4v

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069	Fecha: 20-03-2024
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en IBM InfoSphere Information Server		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo error de validación de entrada, inyección de comandos del sistema operativo e inyección de código en IBM InfoSphere Information Server. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

IBM InfoSphere Information Server es una plataforma de integración de datos de clase empresarial que proporciona capacidades para recopilar, integrar, transformar y entregar datos de manera confiable y segura en toda la empresa. Esta plataforma ayuda a las organizaciones a gestionar eficazmente sus datos, garantizando la calidad, la integridad y la disponibilidad de la información.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-4886 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario. Un usuario remoto que puede crear o actualizar objetos de ingreso puede usar directivas para evitar la desinfección del campo ***spec.rules[].http.paths[].path*** de un objeto de Ingress (en el grupo networking.k8s.io o API de extensiones) para obtener las credenciales del controlador ingress-nginx.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5043 de tipo inyección de comandos del sistema operativo, existe debido a una validación de entrada incorrecta en la anotación ***nginx.ingress.kubernetes.io/configuration-snippet***. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación, ejecutar comandos arbitrarios del sistema operativo y obtener las credenciales del controlador ingress-nginx.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5044 de tipo inyección de código, existe debido a una validación de entrada incorrecta en la anotación ***nginx.ingress.kubernetes.io/permanent-redirect*** en un objeto Ingress. Un usuario remoto puede enviar una solicitud especialmente diseñada, inyectar comandos arbitrarios y obtener las credenciales del controlador ingress-nginx.

A. Productos afectados:

- IBM InfoSphere Information Server: anterior a 11.7.1.4 Service pack 2.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7116638

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069**	**Fecha: 20-03-2024**
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Mitel InAttend y CMG		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo error de validación de entrada en Mitel InAttend y CMG. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos arbitrarios en el sistema de destino.

2. DETALLES:

Mitel InAttend, es una aplicación de administración de llamadas que se utiliza para gestionar eficientemente el enrutamiento de llamadas entrantes en un entorno empresarial; **Mitel CMG (Collaboration Management Gateway)** se trata de una solución que facilita la integración entre diferentes sistemas de comunicación y colaboración dentro de una empresa. CMG permite la interoperabilidad entre plataformas de comunicación como Microsoft Teams, Cisco Webex, Google Meet, entre otras, para mejorar la productividad y la eficiencia en el trabajo colaborativo.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-28815 de tipo error de validación de entrada, existe debido a una configuración incorrecta en el componente BluStar. Un atacante remoto puede ejecutar comandos arbitrarios en el sistema de destino.

A. Productos afectados:

- Mitel InAttend: 2.6 SP4 - 2.7.
- Mitel CMG: 8,5 SP4 - 8,6.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0003 • hxxp://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0003-001-v1.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°069	Fecha: 20-03-2024
		Página: 10 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad del Banco de Crédito del Perú (BCP)		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se identificó que los ciberdelincuentes están llevando a cabo una nueva campaña de Phishing en la que suplantan la identidad de la entidad bancaria BCP. El objetivo de esta campaña maliciosa es obtener de forma ilícita credenciales de acceso, así como información personal y bancaria de los usuarios.

2. DETALLES:

Imagen 1: Se solicita introducir las credenciales de acceso, que comprenden el número de DNI, el número de tarjeta y una clave de internet de seis dígitos.

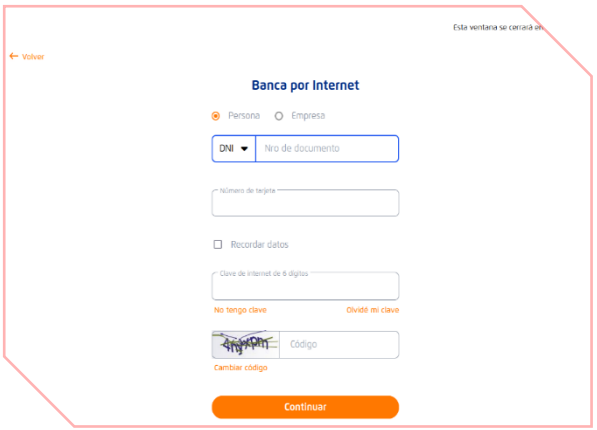


Imagen 2: Después de haber ingresado las credenciales de acceso, se necesita verificar el número de DNI para continuar.

Imagen 3: A continuación, se pide confirmar el número de teléfono celular y los datos bancarios de la tarjeta de crédito o débito.

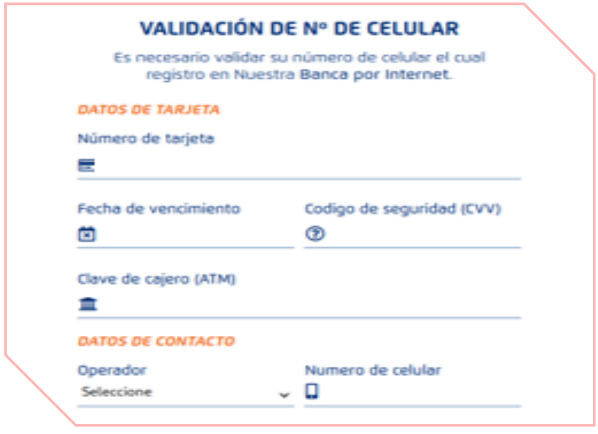
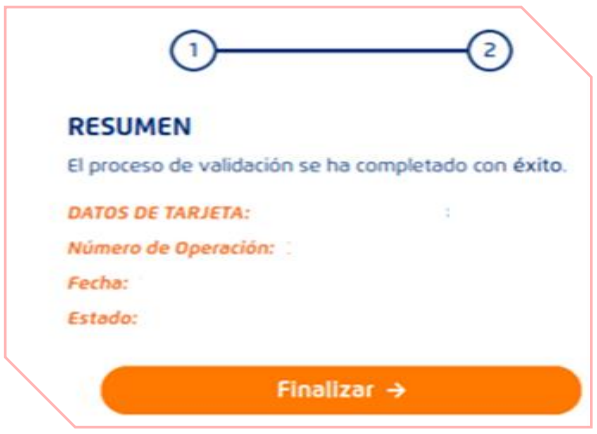
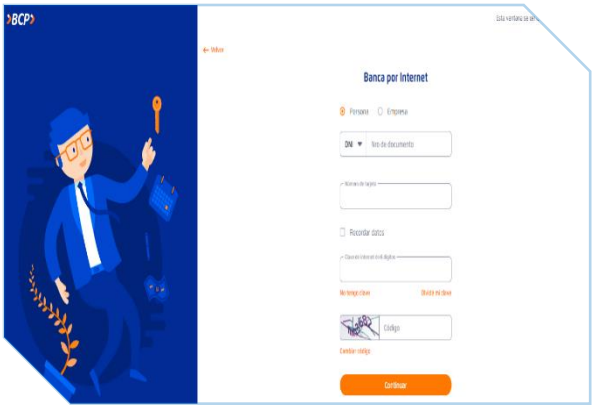


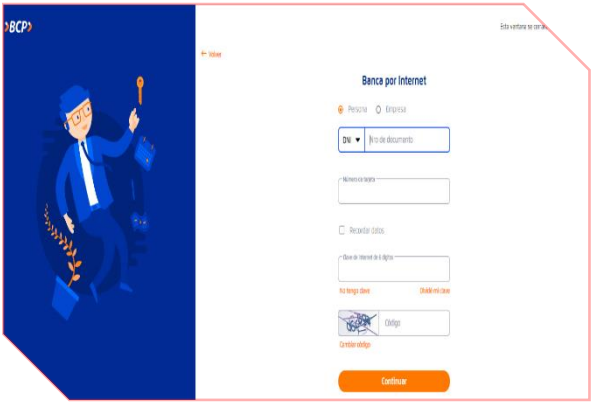
Imagen 4: Finalmente, se señala la validación de los datos ha sido exitosa; sin embargo, los datos fueron capturados por los cibercriminales.



A. Comparación entre el sitio web oficial y el sitio web falso del banco BCP:

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
hxxps://loginunico.viabcp.com/#/tarjeta-sesion	hxxps[:]//vvvvwebzonasengunra[.]com/view?cgi=Liy40Ni9kLRV9iQOV2o2





- Los dos sitios webs tienen una apariencia y estructura similar.
- La diferencia se encuentra en el dominio, ya que el sitio fraudulento no concuerda con la dirección oficial del BCP.
- Ambos sitios cuentan con el protocolo seguro de transferencia de hipertexto (HTTPS), lo que puede convencer aún más a las víctimas al acceder al sitio falso del BCP.

B. Los proveedores de seguridad informática emiten una alerta sobre el riesgo de suplantación de identidad mediante técnicas de phishing.

Análisis de proveedores de seguridad			
Avira	Suplantación de identidad	Bitdefender	Suplantación de identidad
CyRadar	Malicioso	Buscador de amenazas Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
leonico	Suplantación de identidad	búsqueda en seco	Malicioso
Sofos	Suplantación de identidad	raíz web	Malicioso

C. Indicadores de compromiso (IoC)

- URL : hXXps[:]//vvvvwebzonasengunra[.]com/view?cgi=Liy40Ni9kLRV9iQOV2o2
- Dominio : vvvvwebzonasengunra[.]com
- SHA-256 : 80c3fe2ae1062abf56456f52518bd670f9ec3917b7f85e152b347ac6b6faf880
- IP : 198[.]54[.]115[.]232

D. Referencia:

- Phishing, conocido como suplantación de identidad, es una táctica empleada por ciberdelincuentes para engañar a los usuarios y obtener información personal como contraseñas, datos de tarjetas de crédito o números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Verificar minuciosamente la URL para asegurarse de que corresponda al sitio web oficial.
- Tener en cuenta que las instituciones bancarias no solicitan la actualización de datos confidenciales en línea.
- Ingresar datos confidenciales solo desde fuentes oficiales.
- Evitar seguir instrucciones de sitios web sospechosos o de reputación dudosa.
- Mantener el antivirus actualizado sirve como primera línea de defensa contra ataques cibernéticos.
- Abstenerse de compartir la URL con amigos o familiares para evitar riesgos.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta

Índice alfabético

Denegación de servicio DoS..... 4
Explotación de vulnerabilidades conocidas..... 5, 6, 7, 8, 9
Phishing..... 10