Informe Mensual de Servicio

Periodo Julio 2026

Elaborado por Julio Morey A.

Santiago, 10 de Agosto de 2026

Estimada

Ana Lucía Cáceres.

Khipu

Presente

Resumen del Servicio

El Servicio Owl Security de Ciberseguridad Preventiva contempla la vigilancia y detección de vulnerabilidades en servidores de la Red Corporativa y en los Portales Web.

El alcance del Servicio considera:

- Detección de Riesgos y Vulnerabilidades a través de mecanismos de Hacking Ético y Pentesting.
- Reporte de los hallazgos en Plataforma Owl Security.
- Seguimiento y Apoyo en el proceso de Corrección.
- Certificación de las soluciones implementadas.

Resumen de Hallazgos del Periodo

Durante el período se ha detectado y reportado lo siguiente:

Mes	Nuevas	Acumuladas	En Corrección	Resueltas	Proporción Resueltas
Julio	**0**	**89**	**0**	**89**	**100.0%**
Junio	1	89	0	89	100.0%
Mayo	0	88	0	88	100.0%
Abril	1	88	0	88	100.0%
Marzo	0	87	0	87	100.0%
Febrero	0	87	0	87	100.0%

Vulnerabilidades abiertas durante el mes de Julio 2026

Durante el período no se reportaron vulnerabilidades.

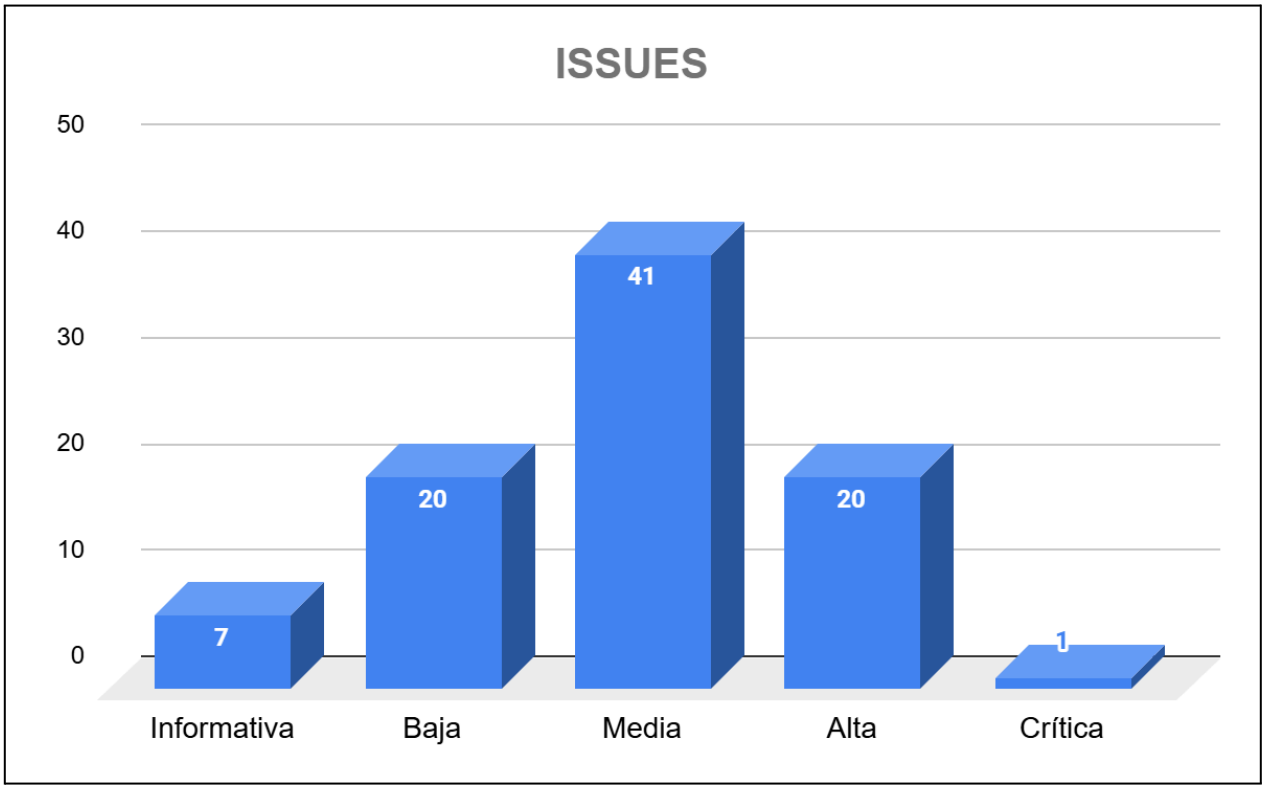
Vulnerabilidades según severidad

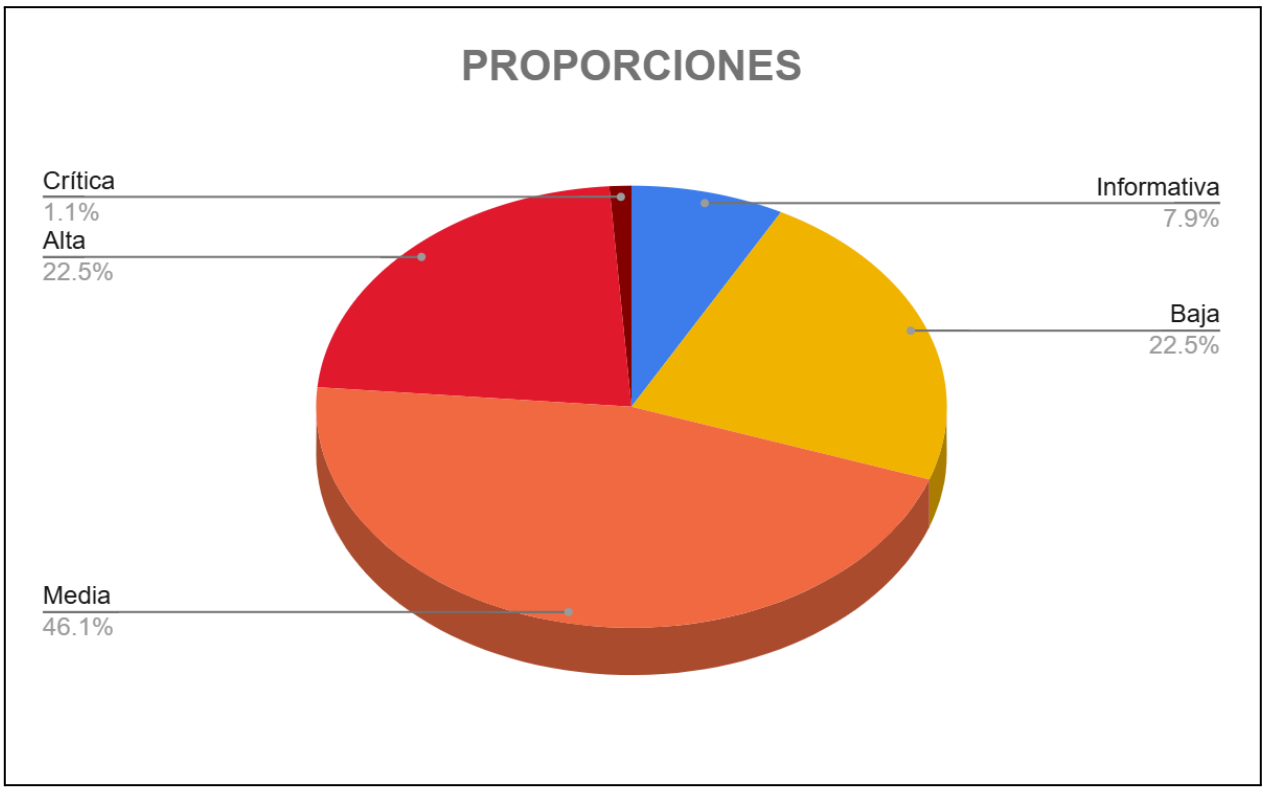
Se consideran cinco niveles de Severidad, según el nivel de Riesgo expuesto, esto es, la relación entre la Probabilidad (o facilidad) de explotación y el impacto potencial, tanto en lo tecnológico como sobre el negocio.

Esta información es sometida a una Matriz de Riesgo y se obtiene lo siguiente:

Severidad	En corrección	Resueltas	Total	Proporción sobre el total
Informativa	0	7	7	7.9%
Baja	0	20	20	22.5%
Media	0	41	41	46.1%
Alta	0	20	20	22.5%
Crítica	0	1	1	1.1%
Total	0	89	89	100.0%

Gráfico según severidades





Las Severidades corresponden al Riesgo potencial de que una vulnerabilidad sea explotada. Para calcularla se toman como referencia dos indicadores:

A. La probabilidad de que sea explotada, considerando tanto el nivel de exposición como la facilidad.
B. El impacto potencial de daño que puede tener un ataque exitoso, tanto en lo técnico como sobre el negocio, y sobre los principios de Integridad, Confidencialidad y Disponibilidad de datos y servicios.

Los valores que puede asumir la severidad son:

- **Crítica**, el riesgo es elevado y la criticidad llega a su máximo ya que el impacto sobre los datos, la estabilidad y la disponibilidad de los Servicios está gravemente comprometida
- **Alta**, el riesgo es evidente y elevado, la posibilidad de explotación son claras, bien documentadas y se debe actuar de forma acelerada en su superación.

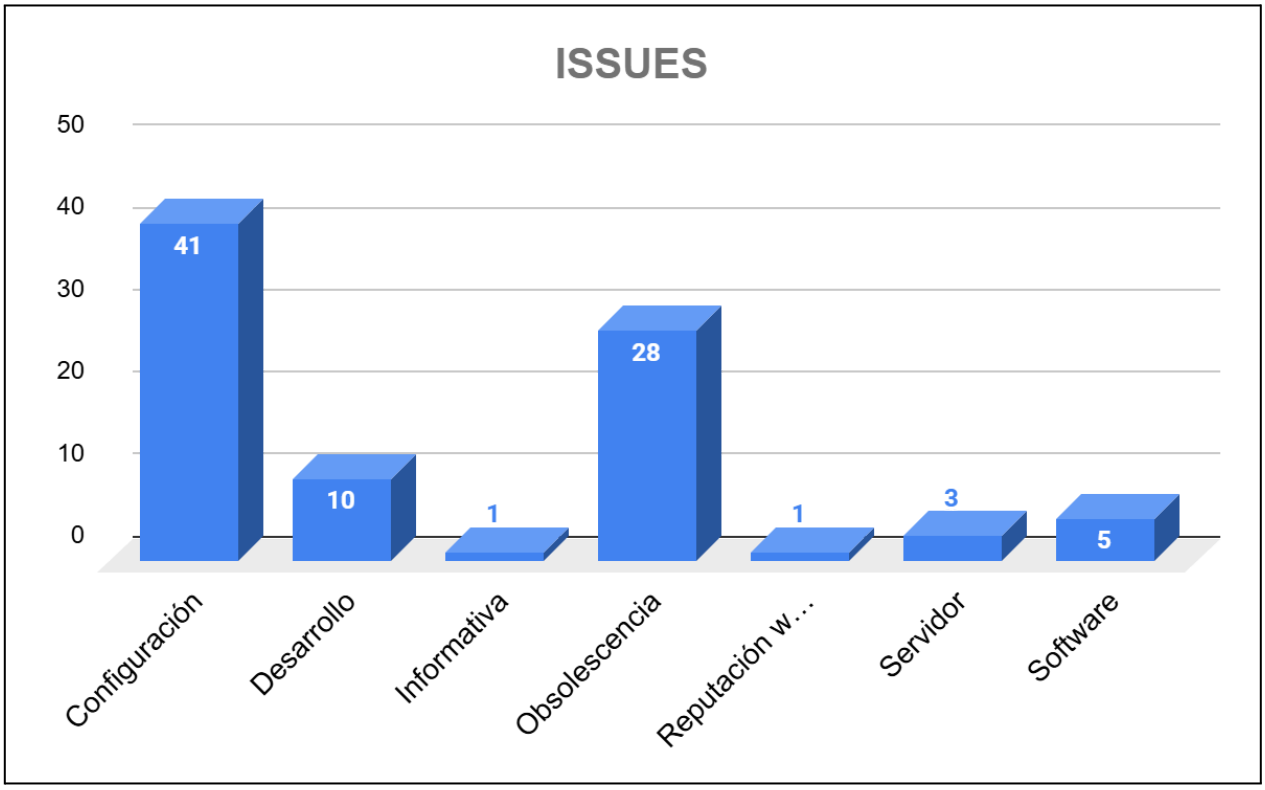
- **Media**, el riesgo se incrementa, la posibilidad de explotación indica que esta vulnerabilidad debe ser tomada con agilidad en resolver.
- **Baja**, que el riesgo es menor, ya sea porque las probabilidades de explotación son remotas, porque está identificada la vulnerabilidad, pero aún no se conoce una manera real y efectiva de explotarla, o porque el impacto potencial es de poca significación y fácil recuperación.
- **Informativa**, que no tienen ningún impacto potencial, pero reviste una buena práctica o recomendación del fabricante del equipo o software involucrado.

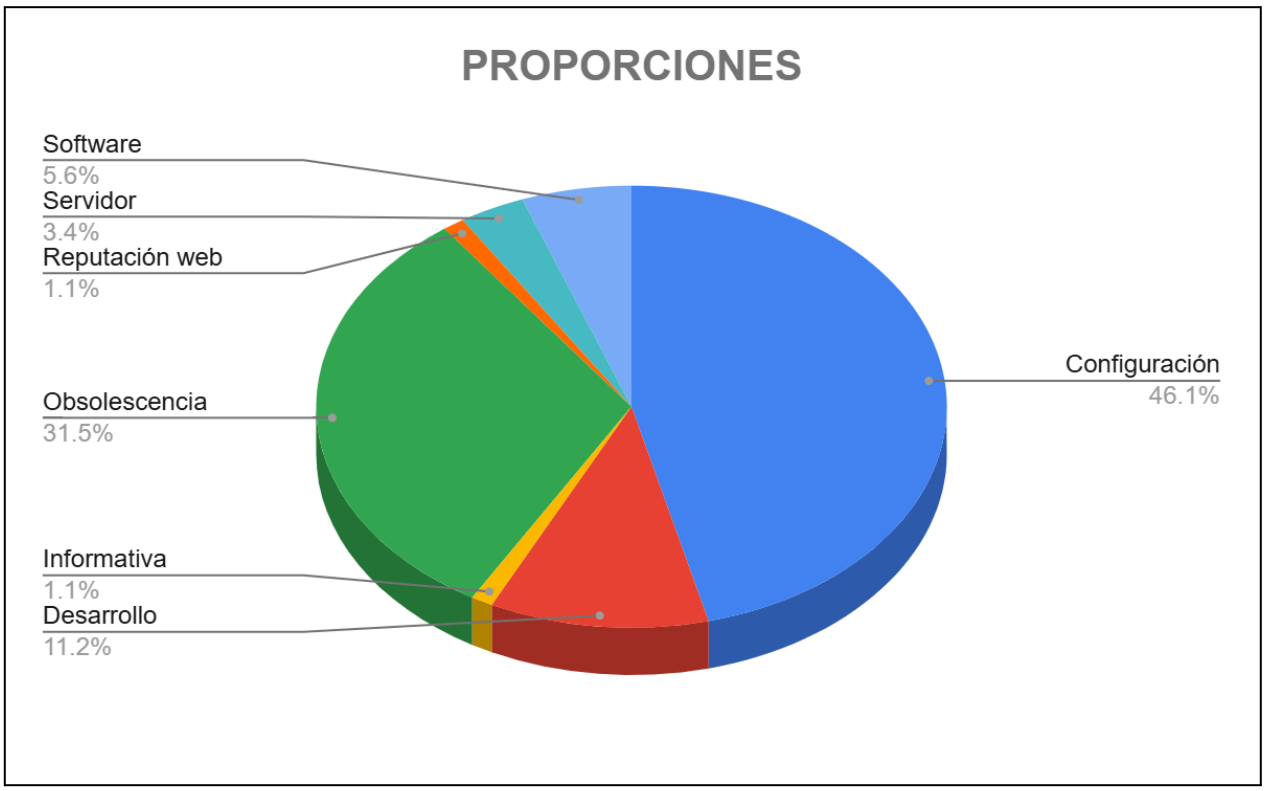
Vulnerabilidad según Categoría

Dependiendo del ámbito tecnológico impactado, se define un conjunto de categorías que permiten clasificar las vulnerabilidades detectadas.

Categoría	En corrección	Resueltas	Total	Proporción sobre el total
Configuración	0	41	41	46.1%
Desarrollo	0	10	10	11.2%
Informativa	0	1	1	1.1%
Obsolescencia	0	28	28	31.5%
Reputación web	0	1	1	1.1%
Servidor	0	3	3	3.4%
Software	0	5	5	5.6%
Total	0	89	89	100%

Gráfico según Categorías





Las categorías posibles son:

- **Servidor:** cuando la vulnerabilidad detectada corresponde a un servicio propiamente tal del sistema operativo instalado. A diferencia de Configuración, esta categoría se utiliza para identificar los aspectos que forman parte natural del sistema y que requieren de una definición global para obtener un alto nivel de seguridad.
- **Configuración:** se utiliza para aquellas vulnerabilidades que se solucionan con una configuración sobre algún sistema o servicio. A diferencia de Servidor, esta categoría abarca aspectos que van más allá del sistema base y, por ejemplo, puede estar relacionada con aplicación de buenas prácticas al momento de definir los parámetros que rigen el funcionamiento seguro de algún componente. Su alcance es particular y está focalizado.

- **Desarrollo:** indica que el riesgo está presente en alguna práctica relacionada con la codificación de software y por lo tanto, es requerido algún tipo de desarrollo para solucionarla.
- **Obsolescencia:** hace referencia a sistemas, aplicaciones o cualquier componente que esté declaradamente fuera de soporte por parte de su fabricante.
- **Reputación Web:** indica que algunos elementos podrían ser utilizados para dañar el nombre de la compañía o que existen listas negras donde está registrado como vulnerable o spam.
- **Sistema:** se refiere a riesgos y vulnerabilidades asociadas al sistema operativo o a alguno de sus componentes fundamentales.
- **Software:** implica un riesgo en algún software o biblioteca que es usado por el sistema, otras aplicaciones o usuarios.

Seguridad de Aplicaciones Móviles

Esta sección presenta los resultados de un conjunto de análisis estático sobre las aplicaciones móviles que reflejan las prácticas recomendadas en la industria.

Aplicación: Khipu 7.5.36

Sitio de la aplicación:

- https://play.google.com/store/apps/details?id=com.khipu.android&hl=es_CL

Esquema de firmas

Los esquemas de firmas presentes en la aplicación corresponden a v1, v2 y v3, que son los esquemas de firmas más utilizados, según se puede apreciar en la evidencia siguiente:

```
Verifies
Verified using v1 scheme (JAR signing): true
Verified using v2 scheme (APK Signature Scheme v2): true
Verified using v3 scheme (APK Signature Scheme v3): true
Verified using v3.1 scheme (APK Signature Scheme v3.1): false
Verified using v4 scheme (APK Signature Scheme v4): false
Verified for SourceStamp: true
Number of signers: 1
Source Stamp Timestamp: 1784325706
```

Estos esquemas entregan un conjunto de niveles de seguridad y han sido incorporados en las distintas versiones de Android, según la distribución siguiente:

Esquema de firma	Introducción	Características	Beneficios	Limitaciones
V1 JAR	Primeras versiones de android	Verificación de integridad y autenticidad básica, Se basa en el esquema de firma JAR tradicional utilizado en Java	Compatibilidad con versiones antiguas de Android	No cubre toda la estructura del APK, susceptible a ataques de repetición
V2 APK	Introducido en Android 7.0 (Nougat)	Proporciona una verificación de la integridad de todo el archivo APK en lugar de solo los archivos individuales dentro del archivo	Mayor seguridad, verificación más rápida	No permite actualización de claves sin reempaquetar el APK
V3 APK	Introducido en Android 9.0 (Pie)	Añade soporte para rotación de claves, permitiendo a los	Flexibilidad, soporte para	Requiere Android 9.0 (Pie) o superior

		desarrolladores cambiar sus claves de firma sin necesidad de lanzar una nueva aplicación	futuras versiones de Android	
V3.1	Introducido en Android 11	Corrección de vulnerabilidades en V3	Mejora de seguridad, compatibilidad hacia atrás	Requiere dispositivos con soporte para V3.1
V4 APK	Introducido en Android 11	Añade soporte para firmas a nivel de archivo para una instalación incremental	Instalaciones más rápidas	Necesita archivo adicional, compatibilidad limitada

Si alguno de los permisos habilitados no fuese necesario para el funcionamiento de la aplicación, se recomienda retirarlo.

Niveles de API

El nivel de API en Android se refiere a una versión particular del conjunto de Interfaces de Programación de Aplicaciones (APIs) que el sistema operativo Android pone a disposición de los desarrolladores. Cada versión de Android tiene un nivel de API asociado y cada aplicación desarrollada tiene un nivel mínimo de API definido y un nivel de API objetivo, es decir, optimizado para la versión especificada.

- **El nivel mínimo de API**: sirve para indicar qué dispositivos pueden instalar y ejecutar la aplicación; mientras más bajo el nivel, mayor es la base de dispositivos y de usuarios en el mercado que pueden utilizar la aplicación.
- **El nivel objetivo de API**: especifica la versión de Android para la que la aplicación está diseñada y optimizada. Esto también incluye aspectos de seguridad como la gestión de permisos y la compatibilidad de mecanismos de seguridad a futuro.

Definir adecuadamente los niveles de API permite a los desarrolladores maximizar el alcance de su aplicación mientras aprovechan las mejoras y nuevas funcionalidades de las versiones más recientes de Android.
Los niveles de API de la aplicación son:

```
<uses-sdk
    android:minSdkVersion="21"
    android:targetSdkVersion="35" />
```

API mínima: nivel 21. Lanzada para la versión Android 5.0 (Lollipop) en noviembre de 2014 y finalizando el soporte de seguridad en marzo de 2018.
API objetivo: nivel 35. Lanzada para la versión de Android 15 (Vanilla Ice Cream) en septiembre de 2024 y posee soporte de seguridad vigente.

Permisos de la aplicación

La aplicación tiene configurado acceso a un total de 18 permisos, que son detallados en la tabla siguiente:

Nº	Permiso	Descripción
1	android.permission.AUTHENTICATE_ACCOUNTS	Permite que una aplicación utilice las capacidades de autenticación de cuentas del Administrador de cuentas, incluida la creación de cuentas, así como la obtención y configuración de sus contraseñas.
2	android.permission.CAMERA	Permite que la aplicación tome fotografías y videos con la cámara. Esto permite que la aplicación recopile imágenes que la cámara está viendo en cualquier momento.
3	android.permission.GET_ACCOUNTS	Permite acceder a la lista de cuentas en el Servicio de Cuentas.
4	android.permission.READ_CONTACTS	Permite que una aplicación lea todos los datos de contacto (dirección) almacenados en su teléfono. Las aplicaciones maliciosas pueden utilizar esto para enviar sus datos a otras personas.
5	android.permission.READ_EXTERNAL_STORAGE	Permite que una aplicación lea desde un almacenamiento externo.
6	android.permission.SYSTEM_ALERT_WINDOW	Permite que una aplicación muestre ventanas de alerta del sistema. Las aplicaciones maliciosas

		pueden apoderarse de toda la pantalla del teléfono.
7	android.permission.WRITE_EXTERNAL_STORAGE	Permite que una aplicación escriba en un almacenamiento externo.
8	android.permission.ACCESS_NETWORK_STATE	Permite que una aplicación vea el estado de todas las redes.
9	android.permission.INTERNET	Permite que una aplicación cree sockets de red.
10	android.permission.READ_SYNC_STATS	Permite que una aplicación lea las estadísticas de sincronización; p.ej. el historial de sincronizaciones que se han producido.
11	android.permission.USE_FINGERPRINT	Permite el uso de huellas dactilares.
12	android.permission.VIBRATE	Permite que la aplicación controle el vibrador.
13	android.permission.WAKE_LOCK	Permite que una aplicación evite que el teléfono entre en modo de suspensión.
14	android.permission.WRITE_SYNC_SETTINGS	Permite que una aplicación modifique la configuración de sincronización, como por ejemplo si la sincronización está habilitada para Contactos.
15	com.google.android.c2dm.permission.RECEIVE	Permite que una aplicación reciba notificaciones automáticas desde la nube.
16	com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	Un permiso personalizado definido por Google.
17	com.google.android.gms.permission.AD_ID	Esta aplicación utiliza un ID de publicidad de Google y posiblemente pueda publicar anuncios.
18	com.khipu.android.permission.C2D_MESSAGE	Permiso desconocido de referencia de Android

Si alguno de los permisos habilitados no fuese necesario para el funcionamiento de la aplicación, se recomienda retirarlo.

Correos electrónicos

Se encontraron los siguientes correos electrónicos dentro del código de la aplicación:

1. support@khipu.com
2. soporte@khipu.com

Revisión Mensual de Seguridad Perimetral

En esta sección se presentan los resultados de un conjunto de análisis rutinarios que representan aspectos básicos de buenas prácticas.

Registros de Seguridad Correos Electrónicos

Dominio: khipu.com

El parámetro “p” indica que en caso de una autenticación fallida se aplicará la política de “Quarantine”. Esto significa que los mensajes que no superen la autenticación serán marcados y tratados como sospechosos.
Política DMARC configurada en quarantine, permite la entrega de correos falsificados a la carpeta de spam.
Riesgo: Un atacante podría enviar mensajes suplantando el dominio; usuarios que revisen spam o tengan reglas automáticas de movimiento podrían abrirlos.
Recomendación: Cambiar política DMARC p=reject tras periodo de monitoreo para evitar la entrega de correos no autenticados, dando como resultado el mensaje de correo electrónico marcado como spam.
Configuración p=quarantine es un paso intermedio que reduce el riesgo de falsos positivos mientras se ajusta la configuración y es útil cuando todavía hay terceros autorizados (ERP, marketing, partners) que envían en nombre del dominio y podrían romperse si se pusiera reject de golpe.

El parámetro “rua” indica que se encuentra configurada la dirección en donde se enviarán los reportes y la información adicional a los casos detectados.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13962
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;_dmarc.khipu.com.              IN      TXT

;; ANSWER SECTION:
_dmarc.khipu.com.       0       IN      TXT     "v=DMARC1; p=quarantine; rua=mailto:ad90959f5ad147f4
a3724e89676e771b@dmarc-reports.cloudflare.net,mailto:dmarc@khipu.com"

;; Query time: 16 msec
;; SERVER: 172.23.192.1#53(172.23.192.1) (UDP)
;; WHEN: Mon Aug 10 12:00:02 -04 2026
;; MSG SIZE  rcvd: 182
```

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

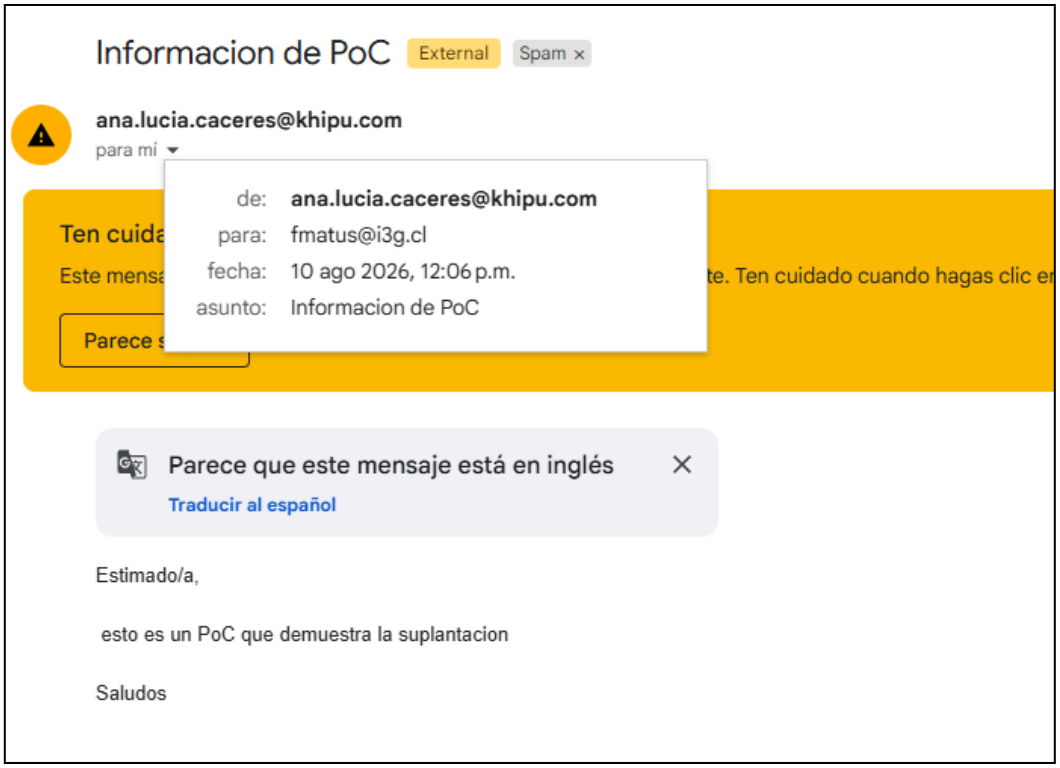
Prueba de Concepto 1

La prueba muestra que la suplantación es posible.

La prueba consistió en lo siguiente:

Usuario ana.lucia.caceres@khipu.com envió un correo electrónico a jmorey@i3g.cl suplantando el correo de Ana Lucía Cáceres.

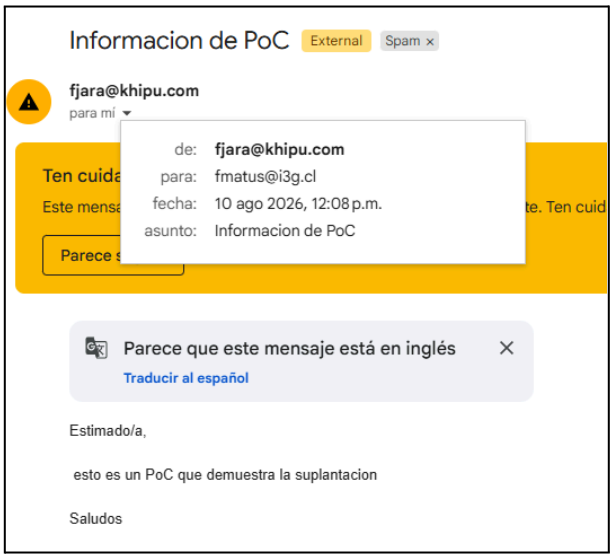
Correo fue marcado como sospechoso y enviado a spam.




```
Delivered-To: fmatus@i3g.cl
Received: by 2002:a05:6a10:a051:b0:6f2:de3b:1487 with SMTP id f17csp2975394pxa; Mon, 10 Aug 2026 09:06:28 -0700 (PDT)
X-Received: by 2002:a05:6a21:38a:b0:3c3:8315:80b7 with SMTP id adf61e73a8af0-3cc1a108008mr3662870637.9.1786377988089; Mon, 10 Aug 2026 09:06:28 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1786377988; cv=none; d=google.com; s=arc-20260327; b=Yu7wFtsCXSQZlrmvtO0mUolavx2QMjg1l9MrX0ZGBHdSgz1Q/npKObiRm66OE1fOuo
f2F2Y8yPx4WqF6ZpnxepG2lWt4eby3BL+C6PokwqFEPKHqX/8Zrv+PUfjpaZKDPNW56N vQxLKpZh+xy+nj+yJYTqmAJtGB0wMqPvwKBUrLsQttLP626wCJ6RIQsVpJyVV0VN27S8
k2yVd0NoM8NPbysOyQqh5UwN54MeBQBJHfu5yzhnwaV4WT/PUDpKrEan8pVK7wL4sUSP kNWc1988keQNQe3OxQ003eK7scabpGcy/GVZYg2wa88tOwpypSPScytnPqt/z1ndUYJO WvKg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20260327; h=message-id:mime-version:date:subject:to:from; bh=TW02V9PMUSeNvGc/h5rJt6PnfP5yqD1cOhiuNQg8GZU=;
fh=EJCQ0444/1LHjGMCmDNIIJnIYqOja7JeiGxGawl0sOw=; b=R7QAplfJh43gJRmQOlGspQWq4UnGvUw1fLVPtK6S6D2s7cAIhOsjLz95LpFqke0Lx2 +k34R/cT0noASxoYceoi0tB6ppuLm4RGM9+OWnEvW7oCPLhCXWQtee7vrmwYPWGbx6XA
e9rtb8RyacYEWyZ2b8ycr37026Xw4AjM4Ihfzuzv2Ln1/2IjmlxTgnlcbmZ1ca6LuHeH J6xk3JOz3/dXqASmiYvwfZR+Zcsxiws/r1wVQz1KO+JJW2hGJ7fLOJYpt8v9h/rAd4sS
sy4aoU/jz6ca/4barfRoSJbFlkZI6GDqlmga7W9yMzNzFKZro/lp+sIH/sK8/1uGMC7A nsqA==; dara=google.com
ARC-Authentication-Results: i=1; mx.google.com; spf=none (google.com: any@mailfrom.notexist.khipu.com does not designate permitted sender hosts)
smtp.mailfrom=any@mailfrom.notexist.khipu.com; dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=QUARANTINE) header.from=khipu.com
Return-Path: <any@mailfrom.notexist.khipu.com>
Received: from helo.attack.com ([186.9.147.190]) by mx.google.com with ESMTP id 41be03b00d2f7-cbe8f1e01d8si15771414a12.94.2026.08.10.09.06.24 for <fmatus@i3g.cl>; Mon, 10 Aug 2026 09:06:28
-0700 (PDT)
Received-SPF: none (google.com: any@mailfrom.notexist.khipu.com does not designate permitted sender hosts) client-ip=186.9.147.190;
Authentication-Results: mx.google.com; spf=none (google.com: any@mailfrom.notexist.khipu.com does not designate permitted sender hosts) smtp.mailfrom=any@mailfrom.notexist.khipu.com;
dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=QUARANTINE) header.from=khipu.com
From: <ana.lucia.caceres@khipu.com>
To: <fmatus@i3g.cl>
subject: Informacion de PoC
Date: Mon, 10 Aug 2026 16:06:21 +0000
Content-Type: text/plain; charset="UTF-8"
MIME-Version: 1.0
Message-ID: <1538085644648.096e3d4e-bc38-4027-b57e-K6ND9S@message-ids.attack.com>
X-Email-Client: https://github.com/chenjj/espoofer

Estimado/a,

 esto es un PoC que demuestra la suplantacion

Saludos
```

Prueba de Concepto 2

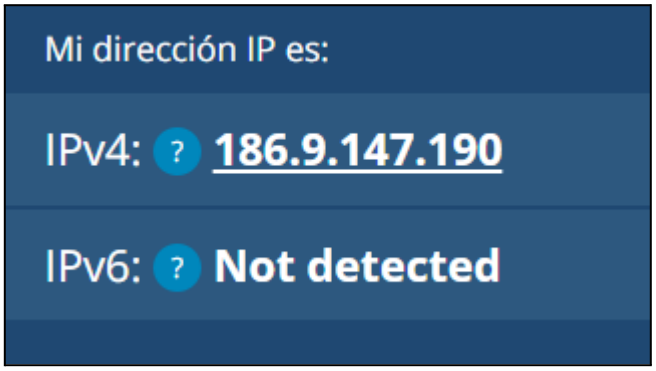
Se envía correo haciendo uso del usuario fjara@khipu.com, demostrando que es posible usar el DNS khipu.com con nombre de usuarios ilegítimos.



Todas las pruebas fueron realizadas desde la dirección IP pública **186.9.147[.]190**

Mensaje original

ID del mensaje	<1538085644648.096e3d4e-bc38-4027-b57e-BQ1QPQ@message-ids.attack.com>
Creado el:	10 de agosto de 2026 a las 12:08 p.m. (Entregado tras 6 segundos)
De:	fjara@khipu.com
Para:	fmatus@i3g.cl
Asunto:	Informacion de PoC
SPF:	NONE con el IP 186.9.147.190 Más información
DMARC:	'FAIL' Más información



El registro SPF se encuentra correctamente configurado para las IP asociadas a los servicios Google Workspace, Amazon Simple Email Service, Mailchimp, Zendesk y productos Sendinblue.

```
;; QUESTION SECTION:
;khipu.com.                     IN      TXT

;; ANSWER SECTION:
khipu.com.              0       IN      TXT     "MS=ms61610785"
khipu.com.              0       IN      TXT     "ZOOM_verify_osCsH8GBFypuixTxFnKcNY"
khipu.com.              0       IN      TXT     "anthropic-domain-verification-5s0xbe=lCE23UPgcn85Gi
q9qXo8WsLuC"
khipu.com.              0       IN      TXT     "atlassian-domain-verification=t7s7g3X/wu3DQ3aoap/Cb
16dCMLVGq0lioFxFlphkaYbQn5f1evcVda/vwwDGezh"
khipu.com.              0       IN      TXT     "brevo-code:b763e3f9ee8c696328599cb4a16831dd"
khipu.com.              0       IN      TXT     "cursor-domain-verification-2nvrgr=wxp7gSNRnOACXNBla
t3BFqATv"
khipu.com.              0       IN      TXT     "google-site-verification=OfTdiWiMkzurJ3Y2gNa7seqGbl
ftGY184qQ01xAOxQA"
khipu.com.              0       IN      TXT     "sophos-domain-verification=54e5c2f55e6a971378d78e4c
c9d5ccc1f0e7aa37b36a6492720f52e6dd383f14"
khipu.com.              0       IN      TXT     "v=spf1 include:_spf.google.com include:servers.mcsv
.net include:spf.sendinblue.com include:amazonses.com include:spf.mindfree.cloud include:50213834.sp
f03.hubspotemail.net include:mail.zendesk.com ~all"

;; Query time: 67 msec
;; SERVER: 172.23.192.1#53(172.23.192.1) (UDP)
;; WHEN: Mon Aug 10 12:11:13 -04 2026
```

Certificados Digitales

En la imagen siguiente se observa que los protocolos SSL/TLS se encuentran habilitados TLSv1.2 y TLSv1.3 lo que es considerado como seguro.

```
Connected to 104.20.23.8

Testing SSL server www.khipu.com on port 443 using SNI name www.khipu.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled
```

La fecha de caducidad del certificado está señalada en la siguiente imagen.

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.khipu.com
Altnames: DNS:*.khipu.com, DNS:khipu.com
Issuer:   Sectigo Public Server Authentication CA OV R36

Not valid before: Feb 27 00:00:00 2026 GMT
Not valid after:  Mar 30 23:59:59 2027 GMT
```

Superficie de Ataque Expuesta

Esta sección presenta una visión consolidada de los activos tecnológicos de la organización que se encuentran expuestos a Internet u otros entornos no controlados.

Subdominios

Esta tabla lista todos los subdominios identificados. Pueden corresponder a entornos de desarrollo, producción o pruebas.

Nº	Subdominios
1	account-link.khipu.com
2	app.khipu.com
3	bi.khipu.com
4	cl.khipu.com
5	design.khipu.com
6	dev.khipu.com
7	docs.khipu.com
8	hites-identity-validator.khipu.com
9	js-scl.khipu.com
10	js.khipu.com

Nº	Subdominios
11	khipu.com
12	lms.khipu.com
13	magic.khipu.com
14	prod-oci-scl.khipu.com
15	status.khipu.com
16	token-generator.khipu.com
17	vtex-callback.khipu.com
18	www.khipu.com
19	zoom.khipu.com

Servicios Activos

Subconjunto de subdominios que presentan puertos 80/443 accesibles y que responden a peticiones HTTP.

Nº	Servicios HTTP Activos
1	https://design.khipu.com
2	https://hites-identity-validator.khipu.com
3	https://lms.khipu.com
4	https://khipu.com
5	https://zoom.khipu.com
6	https://dev.khipu.com
7	https://app.khipu.com
8	https://docs.khipu.com
9	https://bi.khipu.com
10	https://js.khipu.com

Nº	Servicios HTTP Activos
11	https://magic.khipu.com
12	https://js-scl.khipu.com
13	https://vtex-callback.khipu.com
14	https://token-generator.khipu.com
15	https://account-link.khipu.com
16	https://prod-oci-scl.khipu.com
17	https://status.khipu.com
18	https://www.khipu.com
19	https://cl.khipu.com