Informe Mensual de Servicio

Periodo Junio 2025

Elaborado por Fernando Matus H.

Santiago, 09 de Julio de 2025

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
Junio	**1**	**84**	**0**	**84**	**100.0%**
Mayo	0	83	0	83	100.0%
Abril	1	83	0	83	100.0%
Marzo	0	82	0	82	100.0%
Febrero	4	82	0	82	100.0%
Enero	3	78	0	78	100.0%

Vulnerabilidades abiertas durante el mes de Junio 2025

Durante el período se reportaron las siguientes vulnerabilidades:

ID OWL Security	Fecha Reporte	Severidad	Categoría	Resumen	Estado
3074	16-06-2025	informativa	Configuración	Se encuentran disponibles archivos de bucket AWS mediante enlace exacto	Corregido

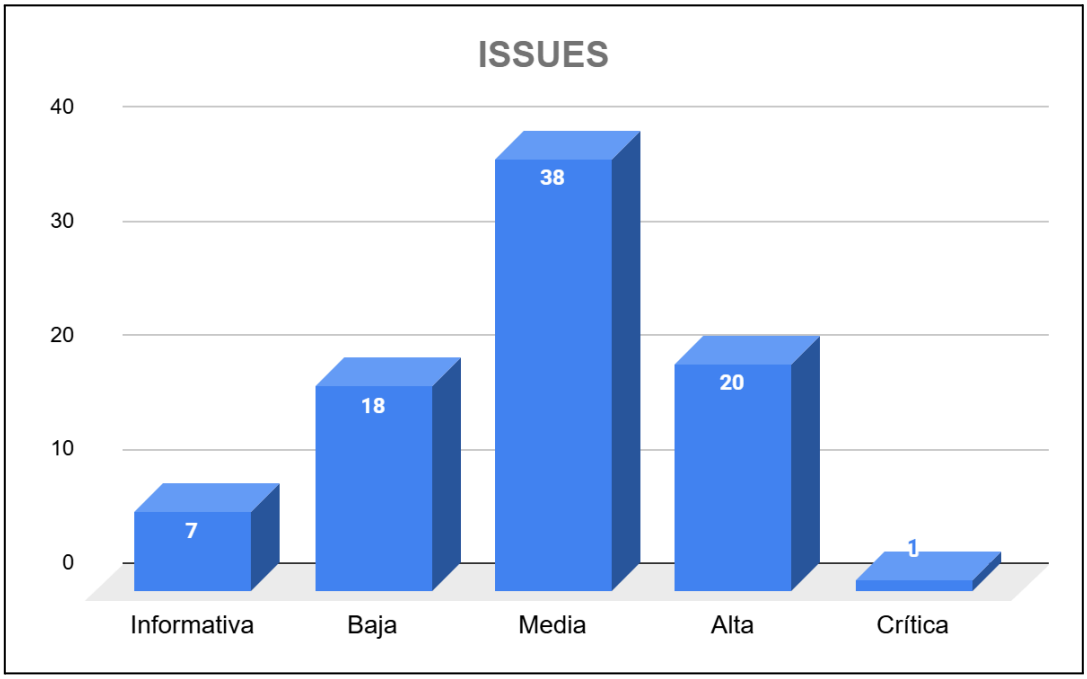
Vulnerabilidades según severidad

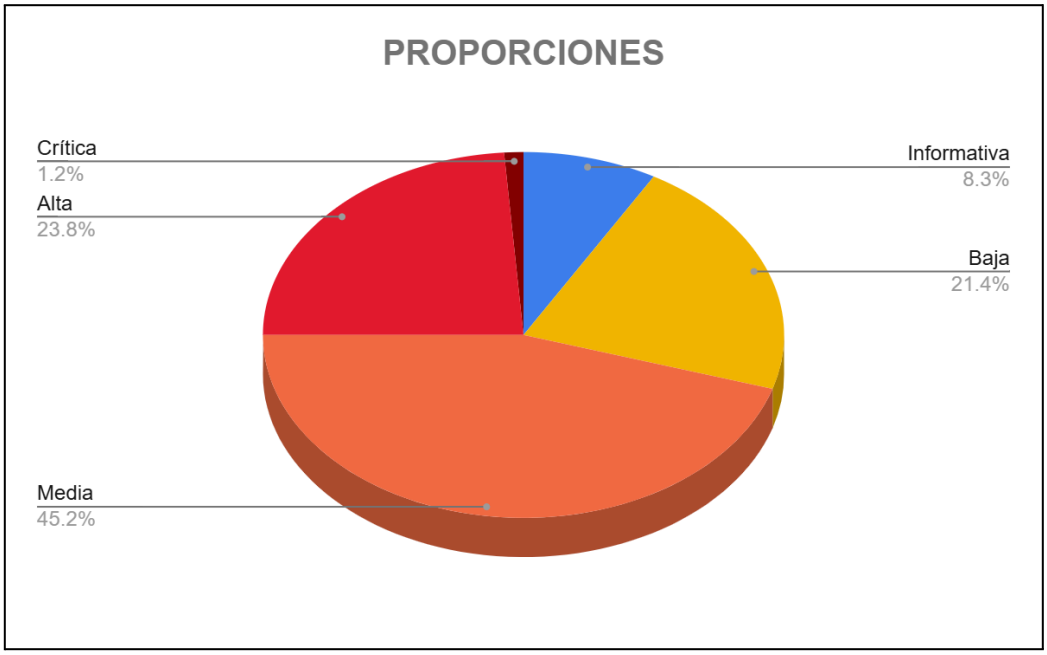
Se consideran cuatro niveles de Severidad, según el nivel de Riesgo expuesto, esto es, la relación entre la Probabilidad (o facilidad) de explotación y el impacto potencial, tanto en lo tecnológico como sobre el negocio.

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	8.3%
Baja	0	18	18	21.4%
Media	0	38	38	45.2%
Alta	0	20	20	23.8%
Crítica	0	1	1	1.2%
Total	0	84	84	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.

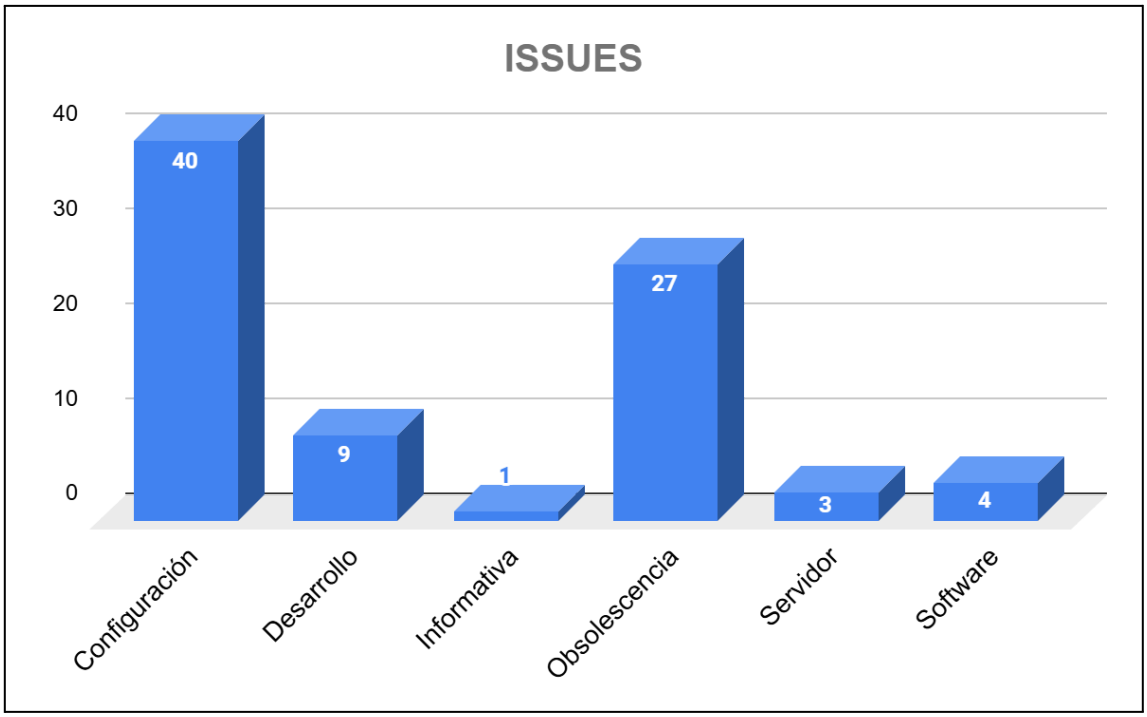
- **Informativa**, que no tienen ningún impacto potencial, pero reviste una buena práctica o recomendación del fabricante del equipo o software involucrado.

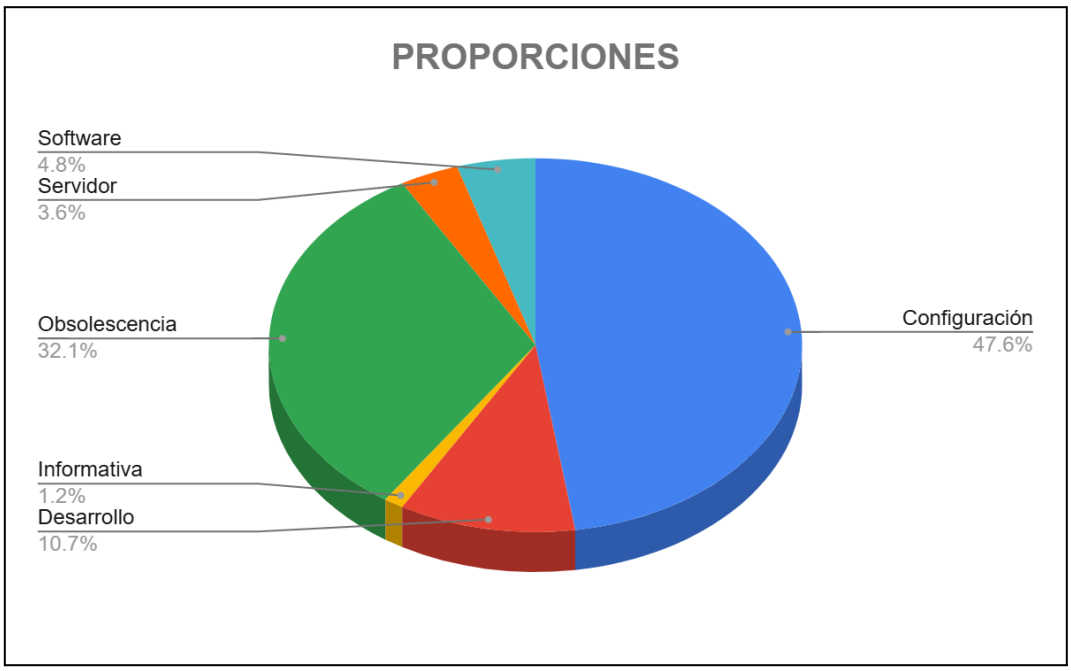
Vulnerabilidad según Categoría

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	40	40	47.6%
Desarrollo	0	9	9	10.7%
Informativa	0	1	1	1.2%
Obsolescencia	0	27	27	32.1%
Servidor	0	3	3	3.6%
Software	0	4	4	4.8%
Total	0	84	84	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

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:

```
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
```

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 desarrolladores cambiar sus	Flexibilidad, soporte para futuras	Requiere Android 9.0 (Pie) o superior

		claves de firma sin necesidad de lanzar una nueva aplicación	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="19"
    android:targetSdkVersion="33" />
```

API mínima: nivel 19. Lanzada para la versión Android 4.4 en octubre 2013, finalizado el soporte de seguridad en octubre 2015[1].

API objetivo: nivel 33. Lanzada para la versión de Android 13 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.

[1] La fecha de fin de soporte es la fecha oficial para teléfonos Google Pixel.

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 Registro DMARC se encuentra parcialmente configurado. **El parámetro "p" indica que en caso de una autenticación fallida no se ejecutará ninguna acción.** Los parámetros "rua" indican que se encuentran configuradas las direcciones en donde se enviarán los reportes e información adicional a los casos.

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46175
;; 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=none; rua=mailto:rua@dmarc.brevo.com"

;; Query time: 68 msec
;; SERVER: 172.23.192.1#53(172.23.192.1) (UDP)
;; WHEN: Tue Jul 08 19:45:08 -04 2025
;; MSG SIZE  rcvd: 111
```

	Test	Result
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✓	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 External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.

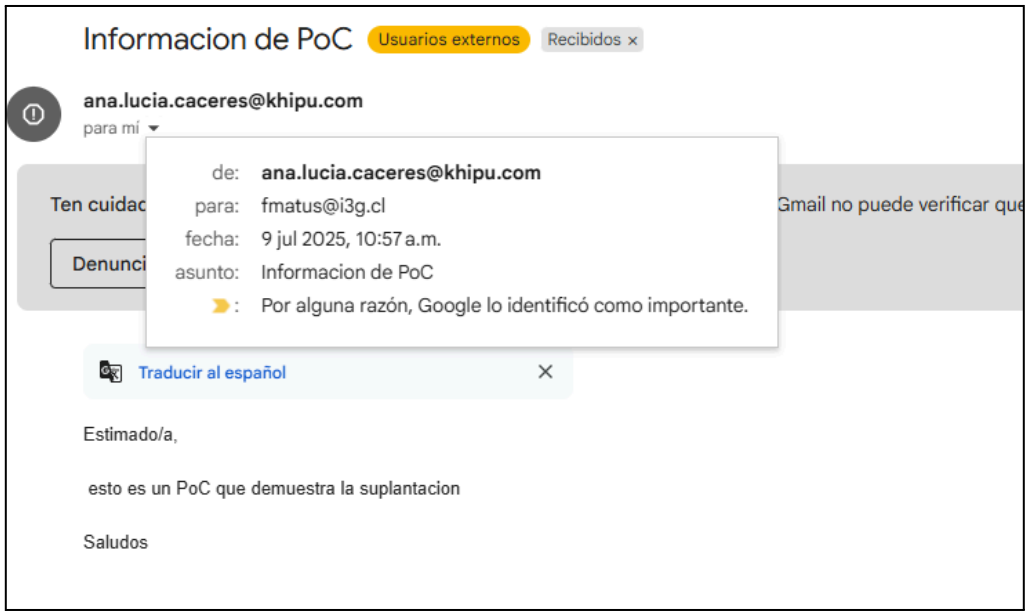
Importante: *Parámetro "p" debe ser configurado en "Quarantine" o "Idealmente Reject"*

Prueba de Concepto 1

La prueba muestra que es posible suplantar el DNS khipu.com aprovechando la configuración actual del parámetro p=none

La prueba consistió en lo siguiente:

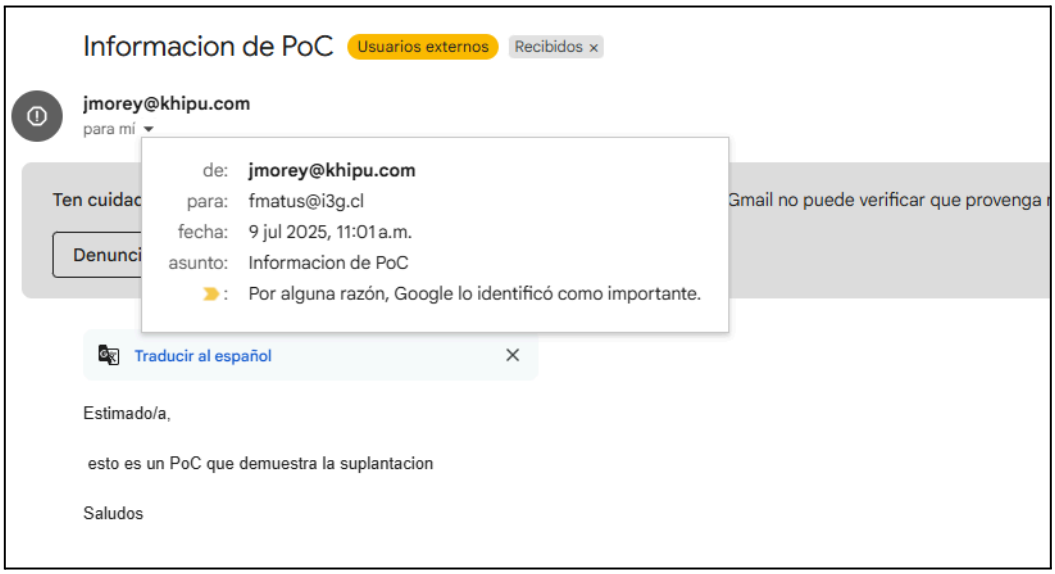
Usuario ana.lucia.caceres@khipu.com envió un correo electrónico a fmatus@i3g.cl suplantando el correo de Ana Lucía Cáceres.



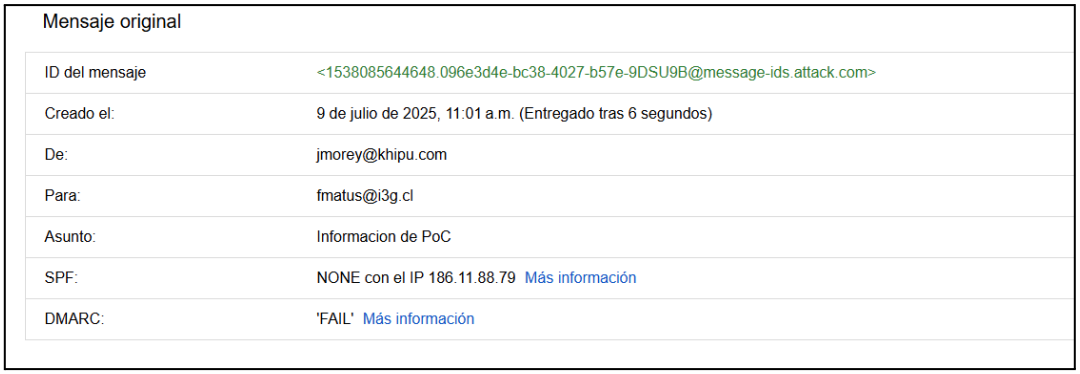

```
Delivered-To: fmatus@i3g.cl
Received: by 2002:a05:7022:6099:b0:a6:7965:daf with SMTP id k25csp8359039dlk;
        Wed, 9 Jul 2025 07:57:44 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IHUyo0+2YwLcqnPYFTmfts/dxcK1Nr3lFLna1qaIB+WDnwtzobRZMiVOwxsZaFRjVPJp1um
X-Received: by 2002:a05:6402:2749:b0:608:2ea3:6538 with SMTP id 4fb4d7f45d1cf-611a6e20ec0mr2580878a12.16.1752073063833;
        Wed, 09 Jul 2025 07:57:43 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1752073063; cv=none;
        d=google.com; s=arc-20240605;
        b=XBcVGc7HaEH2GGwnfbOAfTBRWwkwFYX43uzmbCoZnPyGmL5j06FkPOVFW+vwVMTDZu
         H2hez9kzvIb++g2Yx3jKAxnbV6lQYMeaikQRAzhDSx45TwYEdWQTKZWlAXvoW4OQ0AIg
         EOtS+VpJQias50xwQlxDg3rVBUOaWgy8v8YVjoc8FV+7aqD3nfC645n+evfyOZ9K5GFT
         Nj8Gu5Fe3QINA5V3uJYilViEKjNqZPsZZVRlh4LzFM5/mcZrf72WN7eOxgqABEGqy/eD
         TvyrbqdSRt6FT8QKKRbNf50awhv36CjFXF1o1T/P2SMH4bOfCt9YTHx0SUgFmbFZd/wN
         8umA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=message-id:mime-version:date:subject:to:from;
        bh=TW02V9PMiSeNvGc/h5rJt6PnfP5yqD1cOhiuKQg8GZU=;
        fh=EJCQ0444/1LHjGMCmDNIIJnIYqOja7JeiGxGawl0sOw=;
        b=B6MtyQc6ha1MzDcNtfxB6p0UJiWbkz1HWTeMCbHM0/AoJMOAb3Xtfr9wZaDniUizCO
         Vk9RSmuKs656X3KYrRVqHb5h8OHc97oROPYNroxmv5DSi9YCIg3nDxtZcs5mhxYOD5VI
         mg8vMBEg/X/zz/cSWDZs6hEjQb02FwuPYP7Cv0Ve//qI7FWM7gmb/vVuCrc51J9g4sAa
         ZwQoFrthwgoEkkgeMgi8LeUzhpXzxh6TX8sSeQ+lQl8sONj+xli7PsDENWCdjD3QiMrS
         LKip5Knh62HzklIQanMmHafeSk+ThXDbgnqR2FHG2kQpa2erGFpxQ4Ijeawks9xsglif
         zvPw==;
        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=NONE sp=NONE dis=NONE) header.from=khipu.com
Return-Path: <any@mailfrom.notexist.khipu.com>
Received: from helo.attack.com ([186.11.88.79])
        by mx.google.com with ESMTP id 4fb4d7f45d1cf-60fca663631si8702414a12.6.2025.07.09.07.57.40
        for <fmatus@i3g.cl>;
        Wed, 09 Jul 2025 07:57:43 -0700 (PDT)
Received-SPF: none (google.com: any@mailfrom.notexist.khipu.com does not designate permitted sender hosts) client-ip=186.11.88.79;
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=NONE sp=NONE dis=NONE) header.from=khipu.com
From: <ana.lucia.caceres@khipu.com>
To: <fmatus@i3g.cl>
subject: Informacion de PoC
Date: Wed, 09 Jul 2025 14:57:34 +0000
Content-Type: text/plain; charset="UTF-8"
MIME-Version: 1.0
Message-ID: <153800856446648.096e3d4e-bc38-4027-b57e-TQOPFP@message-ids.attack.com>
X-Email-Client: https://github.com/chenjj/espoofer

Estimado/a,

 esto es un PoC que demuestra la suplantacion

Saludos
```

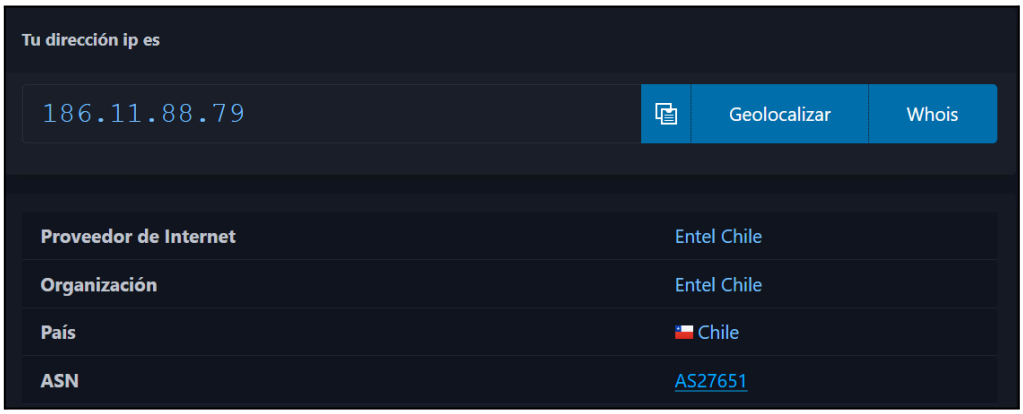
Prueba de Concepto 2

Se envía correo haciendo uso de usuario jmorey@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 **186.11.88.79**





Se recomienda considerar una de las configuraciones recomendadas para proteger el DNS frente a suplantaciones.

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.

```
;; ⟶»HEADER«⟵ opcode: QUERY, status: NOERROR, id: 43152
;; flags: qr rd ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
khipu.com.              0       IN      TXT     "ZOOM_verify_osCsH8GBFypuixTxFnKcNY"
khipu.com.              0       IN      TXT     "atlassian-domain-verification=t7s7g3X/wu3DQ3aoap/Cb16dCMLVGq0lioFxFlphk
aYbQn5f1evcVda/vwwDGezh"
khipu.com.              0       IN      TXT     "brevo-code:b763e3f9ee8c696328599cb4a16831dd"
khipu.com.              0       IN      TXT     "cursor-domain-verification-2nvrgr=wxp7gSNRnOACXNBlat3BFqATv"
khipu.com.              0       IN      TXT     "google-site-verification=OfTdiWiMkzurJ3Y2gNa7seqGblftGY184qQ01xAOxQA"
khipu.com.              0       IN      TXT     "v=spf1 include:_spf.google.com include:servers.mcsv.net include:spf.sen
dinblue.com include:amazonses.com include:spf.mindfree.cloud include:mail.zendesk.com ~all"

;; Query time: 311 msec
;; SERVER: 172.23.192.1#53(172.23.192.1) (UDP)
;; WHEN: Tue Jul 08 19:53:38 -04 2025
;; MSG SIZE  rcvd: 573
```

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 169.47.100.12

Testing SSL server khipu.com on port 443 using SNI name 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:www.khipu.com
Issuer:   Sectigo RSA Extended Validation Secure Server CA

Not valid before: Jan  8 00:00:00 2025 GMT
Not valid after:  Feb  8 23:59:59 2026 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	Nº	Subdominios
1	accountlink.khipu.com	24	lms.khipu.com
2	antibotasa.khipu.com	25	magic.khipu.com
3	app.khipu.com	26	oldjs.khipu.com
4	bi.khipu.com	27	oper.khipu.com
5	bi.khipu.com	28	prodociscl.khipu.com
6	cerebro.khipu.com	29	site.khipu.com
7	cl.khipu.com	30	st.khipu.com
8	demo.khipu.com	31	status.khipu.com
9	dev.khipu.com	32	stress.khipu.com
10	dev.whmcs.khipu.com	33	tokengenerator.khipu.com
11	docsst.khipu.com	34	vtexcallback.khipu.com
12	docs.khipu.com	35	www.app.khipu.com
13	drummer.khipu.com	36	www.bi.khipu.com
14	easytaxitopup.khipu.com	37	www.demo.khipu.com
15	jsscl.khipu.com	38	www.dev.khipu.com
16	js.khipu.com	39	www.dev.whmcs.khipu.com
17	kauthorizer.khipu.com	40	www.khipu.com
18	kh04.khipu.com	41	www.magic.khipu.com
19	kh08.khipu.com	42	www.site.khipu.com
20	khashier.khipu.com	43	www.stress.khipu.com
21	khenshinwsociscl.khipu.com	44	zoom.khipu.com
22	khipu.com		
23	lbkhipu01.mindfree.cl		

Servicios Activos

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

Nº	Servicios HTTP Activos
1	https://antibotasa.khipu.com/
2	https://cerebro.khipu.com/
3	https://dev.khipu.com/
4	https://docs.khipu.com/
5	https://drummer.khipu.com/
6	https://js.khipu.com/
7	https://khashier.khipu.com/
8	https:/khipu.com/
9	https://lms.khipu.com
10	https://magic.khipu.com/
11	https://oper.khipu.com/
12	https://st.khipu.com/
13	https://status.khipu.com/
14	https:/www.khipu.com/