



## Informe Mensual de Servicio

Periodo Octubre 2022

Elaborado por Felipe Jara

---

Santiago, 11 de noviembre de 2022

### 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
Octubre	3	31	2	29	93.5%
Septiembre	0	28	0	28	100%
Agosto	0	28	0	28	100%

## Vulnerabilidades abiertas durante el mes de Octubre 2022

---

Durante el mes de Octubre se reportaron las siguientes vulnerabilidades.

ID OWL Security	Fecha Reporte	Severidad	Categoría	Resumen	Estado
668	21-10-2022	alta	Obsolescencia	Versión de Wordpress con Múltiples Vulnerabilidades	Corregido
656	12-10-2022	informativa	Obsolescencia	Versión desactualizada de Plugin Wordpress Google Analytics	en corrección
655	12-10-2022	baja	Configuración	Se detecta archivos Debug en Wordpress	en corrección

## Vulnerabilidades según severidad

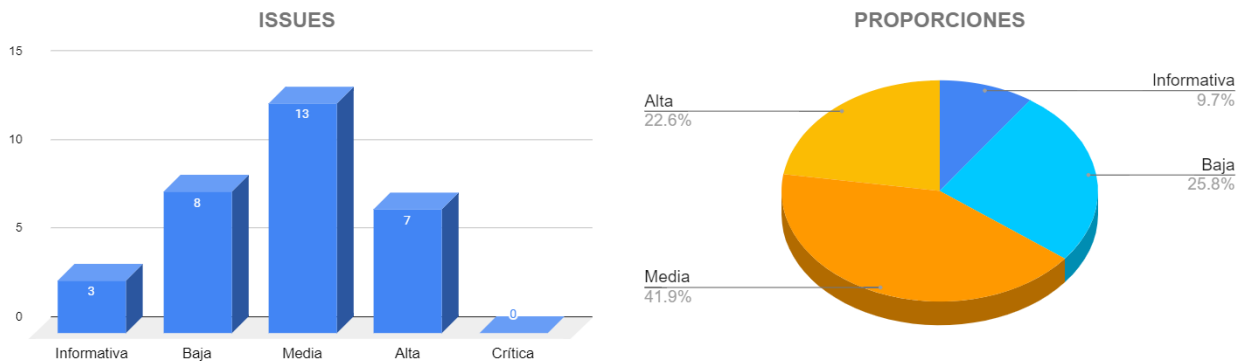
---

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	1	2	3	9.7%
Baja	1	7	8	25.8%
Media	0	13	13	41.9%
Alta	0	7	7	22.6%
Crítica	0	0	0	0.0%
<b>Total</b>	<b>2</b>	<b>29</b>	<b>31</b>	<b>100.0%</b>

## Gráfico según severidades



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

- La probabilidad de que sea explotada, considerando tanto el nivel de exposición como la facilidad.
- 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.

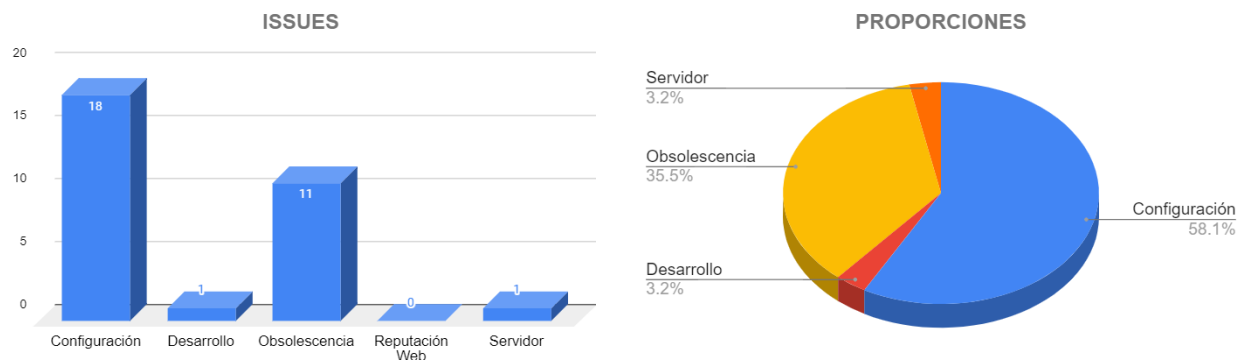
- **Informativa**, que no tienen ningún impacto potencial, pero reviste una buena práctica o recomendación del fabricante del equipo o software involucrado.

## Vulnerabilidad según Categoría

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

Severidad	En corrección	Resueltas	Total	Proporción sobre el total
Configuración	1	17	18	58.1%
Desarrollo	0	1	1	3.2%
Obsolescencia	1	10	11	35.5%
Reputación Web	0	0	0	0.0%
Servidor	0	1	1	3.2%
<b>Total</b>	<b>2</b>	<b>29</b>	<b>31</b>	<b>100%</b>

## 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.

## 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” y “ruf” indican que se encuentran configuradas las direcciones en donde se enviarán los reportes e información adicional a los casos.

```
;; ANSWER SECTION:  
_dmarc.khipu.com.      5      IN      TXT      "v=DMARC1; p=none; sp=none;  
rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m;  
rf=afrrf; pct=100; ri=86400"
```

	Test	Result
Status 	NameDMARC Policy Not Enabled	ResponseDMARC Quarantine/Reject policy not enabled
Status 	NameDMARC Record Published	ResponseDMARC Record found
Status 	NameDMARC Syntax Check	ResponseThe record is valid
Status 	NameDMARC External Validation	ResponseAll external domains in your DMARC record are giving permission to send them DMARC reports.
Status 	NameDMARC Multiple Records	ResponseMultiple DMARC records corrected to a single record.

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

```
;; ANSWER SECTION:
khipu.com.      300      IN       TXT      "statuspage-domain-verification=< 7s5mvcrxdtj5 >"
khipu.com.      300      IN       TXT      "v=spf1 include:amazonses.com include:spf.google.com
include:servers.mcsv.net include:spf.sendinblue.com mx ~all"
khipu.com.      300      IN       TXT      "MS=0C2391BB0288D08AB8BA6DD51B00EA8C087C23A4"
khipu.com.      300      IN       TXT      "Sendinblue-code:2589d4e965b6296bbb5d405597482a2b"
khipu.com.      300      IN       TXT      "google-site-verification=OfTdiWiMkzurJ3Y2gNa7seqGblft
GY184qQ001xA0xQA"
khipu.com.      300      IN       TXT      "mt-30037992"
khipu.com.      300      IN       TXT      "mt-79982204"
```

## Certificados Digitales

---

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

```
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.


```
Subject: khipu.com
Altname: DNS:khipu.com, DNS:www.khipu.com
Issuer: Sectigo RSA Extended Validation Secure Server CA
Not valid before: Jan 17 00:00:00 2022 GMT
Not valid after: Feb 17 23:59:59 2023 GMT
```



## Seguridad en Wordpress

---

Al cierre de este informe se pudo validar que la versión Wordpress configurada presenta las siguientes características.



**Versión Wordpress: 6.1** (Lanzamiento: 01-11-2022)  
**Nivel de Riesgo: Bajo**  
Ultima Versión Disponible: 6.1  
Su versión tiene **7 días** de Antigüedad.  
Nivel de Riesgo: Ultima Versión, no presenta riesgos

### Vulnerabilidades Detectadas en Wordpress

No se presentan Vulnerabilidades en Wordpress

### Plugins con Vulnerabilidades

\*\* No se detectaron Plugins Vulnerables \*

### Temas con Vulnerabilidades

**Tema Principal: Divi (Smart. Flexible. Beautiful. Divi is the most powerful theme in our collection.)**

- Versión: 4.19.0

- Vulnerabilidades Detectadas:

\*\* No se detectaron vulnerabilidades

\* No se detectaron Temas con Vulnerabilidades \*

La versión instalada de Wordpress que corresponde a la 6.1, se encuentra actualizada y su core no presenta vulnerabilidades. Tampoco se detectaron vulnerabilidades en plugins ni temas.

Finalmente, se encontró una nueva cuenta de usuario correspondiente a [rodrigo.schmidt@khipu.com](mailto:rodrigo.schmidt@khipu.com) . La lista de usuarios detectados es:

**Usuarios Detectados**

- 1) Felipe Fredes
- 2) [rodrigo.schmidt@khipu.com](mailto:rodrigo.schmidt@khipu.com)
- 3) felipe
- 4) khipu-intranet
- 5) khipucom
- 6) luisjofre
- 7) rodrigo-schmidtkhipu-com
- 8) yongsanchiong