



# OWL Security

Prevención Proactiva en Ciberseguridad

Gestión y Seguimiento Online de Riesgos y Vulnerabilidades

The background of the lower half of the page is a dark blue and black gradient. It features a grid of glowing orange and white hexagons. Some hexagons contain a white padlock icon. In the background, there is a faint pattern of binary code (0s and 1s).

# Servicio de Ciberseguridad Preventiva Owl Security

## Presentación del Servicio

El Servicio Owl Security es una solución proactiva para la detección temprana y seguimiento de vulnerabilidades tecnológicas presentes en Servidores, Aplicaciones y toda clase de dispositivo de comunicación e IoT.

El servicio se apoya en una aplicación web para reportar los hallazgos y hacerles seguimiento hasta su solución y cierre. Un sistema de reportes y estadística en línea, y el conocimiento de nuestros especialistas le permitirá contar con toda la información para corregir cualquier riesgo y prevenir potenciales ataques.

Las Vulnerabilidades y Riesgos de Ciberseguridad son detectados en un proceso similar al Hacking Ético, pero en un modelo de búsqueda cotidiana. Cada vulnerabilidad que se detecta es informada a través de la plataforma web y el usuario recibe un correo electrónico con el detalle del hallazgo. A partir de este momento, se genera un intercambio de información entre el cliente y los especialistas de Owl Security para apoyar en la corrección y cierre definitivo del riesgo.

## Objetivos a Analizar

Se considera que un objetivo a analizar puede ser un Servidor, un Dispositivo de Comunicación, un Proceso de una Aplicación Web, Aplicación Móvil, o cualquier otro elemento que disponga de una dirección IP y que esté expuesto a vulnerabilidades. Cada uno de los elementos objeto del análisis y detección es llamado **Unidad Tecnológica**.

Un servidor Web que ofrece un aplicativo transaccional podrá ser considerado en más de una unidades de análisis. Por ejemplo, el Servidor mismo será una Unidad Tecnológica, considerando su sistema operativo y todos los servicios web expuestos. Por otra parte, el aplicativo y sus procesos serán considerados como unidades independientes, por tratarse de procesos sistémicos.

Ejemplos de Unidades Tecnológicas relacionadas a procesos:

- Sistema de Matrícula e Inscripción de Carga Académica
- Proceso de Compra Online, desde la creación de carro de compra hasta la confirmación de pago.
- Pago de Cuentas OnLine, desde la consulta de estado hasta el pago.
- Requerimientos tipo Reserva de Hora, Envío de documentos, Consultas de Datos, etc.

## **Condiciones Comerciales**

Se consideran los siguientes aspectos comerciales

- a) El contrato de servicio tendrá una duración inicial de 24 meses, y se considerará una renovación automática, por periodos iguales, en la medida que ambas partes acuerden mantener su vigencia.
- b) Se consideran salidas anticipadas, que estarán estipuladas en el Contrato.
- c) El servicio considera un primer pago por concepto de Setup Fee, equivalente a la mitad de un mes de servicio. Este pago se realiza por una única vez.
- d) Un anexo del contrato consistirá en el Acuerdo de Confidencialidad (NDA). Este acuerdo tiene por objetivo resguardar el uso que se puede dar a la información obtenida como parte de los análisis de seguridad. Como premisa fundamental se entenderá que ninguna información puede ser expuesta en forma pública o privada, fuera de la plataforma Owl Security, sin la expresa autorización del cliente.
- e) Respecto a la confidencialidad, se deja establecido que no existe ninguna razón para que los datos de las vulnerabilidades detectadas sea expuestos, incluso frente a situaciones de término de contrato anticipado o frente a disputas legales o de cualquier índole.
- f) Con todo, los datos obtenidos como parte de la entrega del Servicio son de propiedad del Cliente y cada vez que sea requerido, y particularmente una vez terminado el Contrato, éstos serán entregados, en forma íntegra y sin ninguna consideración adicional, en formato XML, organizados y clasificados para el uso y destino que el Cliente estime conveniente. Todo lo anterior, sin perjuicio de los reportes en línea que entregará esta información al Cliente, cada vez que lo requiera durante la vigencia del contrato.

## **Condiciones Técnicas**

Se consideran los siguientes aspectos técnicos del servicio

- a) El servicio es entregado en modalidad full Cloud, lo que implica que ningún componente es instalado en dependencias del cliente. Esto se cumple considerando que todas las Unidades Tecnológicas objeto de este servicio están expuestas a Internet y pueden ser alcanzadas en forma pública.

- b) Si las Unidades Tecnológicas se encuentran dentro de la red corporativa, será necesario la instalación de una sonda, en común acuerdo de las partes, que es instalada, configurada y administrada por el Servicio, en forma remota, a través de una conexión SSH (preferida) o VPN. La habilitación, configuración y administración de la sonda no tiene cargo monetario sobre el servicio, sin embargo podrían existir costos asociados a la tecnología requerida para la implementación, por ejemplo servidores físicos o virtuales.
- c) Las Vulnerabilidades detectadas serán informadas vía correo electrónico al cliente y quedarán inmediatamente disponible en la plataforma Owl Security para su consulta y gestión.
- d) Toda la comunicación entre el Cliente y los especialistas de Owl Security se realizará a través de las herramientas de comunicación disponibles, esto es Mensajería Interna de la plataforma y Correo Electrónico. Para eso se dispondrá de la casilla [tracker@owlsecurity.cl](mailto:tracker@owlsecurity.cl). Los contactos comerciales serán escalados a través del administrador del contrato.
- e) El tratamiento de una vulnerabilidad considera las siguientes etapas y responsabilidades:

<b>Etapas</b>	<b>Responsable</b>
Detección de la Vulnerabilidad	Owl Security
Informe en Plataforma	Owl Security
Corrección de la Vulnerabilidad	Cliente
Respuesta a Consultas del Cliente	Owl Security
Validación de la Corrección Aplicada	Owl Security
Cierre del Caso	Owl Security

## **Prueba de Concepto**

Las condiciones generales para la realización de una prueba de concepto son las siguientes:

- a) Se habilitará un usuario en la plataforma OwlSecurity <https://demo.owlsecurity.cl> para que el cliente pueda acceder a revisar vulnerabilidades. Este usuario será de uso exclusivo para el cliente que participa en el prueba de concepto. Eventualmente podrá habilitarse más de un usuario si es requerido.

- b) Se realizará una detección de vulnerabilidades sobre algunos de los servidores del cliente, previo acuerdo, y los hallazgos serán informados en la plataforma OwlSecurity como si fuera un cliente contratado.
- c) La cantidad de vulnerabilidades que serán informadas fluctúa entre 3 y 5, por una única vez, con la finalidad de que el cliente pueda familiarizarse con la plataforma.
- d) El cliente podrá utilizar la plataforma para solucionar las vulnerabilidades informadas, interactuando con el equipo de soporte de OwlSecurity, tal como lo hace un cliente con contrato vigente.
- e) Si el cliente no desea una POC, de todas formas puede acceder e interactuar con la cuenta Demo, en <https://demo.owlsecurity.cl> Usuario: demo, Password: demo.
- f) Una vez finalizada la POC, el cliente que desee continuar con el servicio recibirá la información sobre los hallazgos a través de la plataforma, dando así inicio formal a la entrega del Servicio. Si el cliente desiste, todos los datos relativos a sus servidores será eliminado completamente de la plataforma.
- g) La POC no tendrá costo para el cliente y se podrá extender por un máximo de 30 días.
- h) Para la realización de la POC se debe considerar la firma de un acuerdo de confidencialidad que garantice al Cliente el resguardo de la información, incluso si no se llega a contratar el servicio.

## **Acceso a la Plataforma Demo**

Está disponible una plataforma de demostración, completamente operativa para realizar evaluaciones sobre el servicio, sin ningún compromiso.

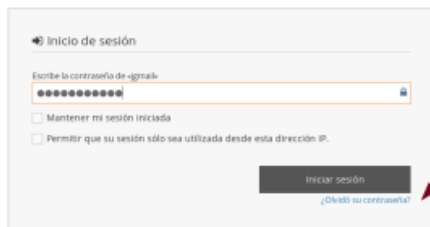
En las siguientes páginas se muestra los aspectos básicos para ingreso y uso de esta plataforma.

## Ingreso a la plataforma demo

Desde el sitio web:  
<https://demo.owlsecurity.cl>  
Usuario/Password: demo/demo



Ingreso con nombre de usuario o correo electrónico



Recuperar clave olvidada o bloqueada por tres intentos de login fallidos

## Vista General y Resumen de Actividades

Menú de Opciones

Resumen de vulnerabilidades.  
Simbología y colores representan el Estado y nivel de Riesgo

[Link para acceder al detalle](#)





## Vista de Vulnerabilidades

**Cre y almacena filtros personalizados**

**Vulnerabilidades según filtro**

**Opciones para exportación**

Informador	Asignada a	Monitorizado por	Nota de	Prioridad	Severidad	Visibilidad	Ver incidencias Fijadas
Cuquierno	Cuquierno	Cuquierno	Cuquierno	Cuquierno	Cuquierno	Cuquierno	0
Categoría	Outlier (sin filtros)	Estado	Resolución	Filtrar por fecha de inicio	[Cuquierno]	Filtrar por fecha de última actualización	No
Cuquierno	versión 39 (agrupado)	Cuquierno	Cuquierno	No	informativa		
Post	Plataforma	SO	Modelo de SO	Resolución	alta		
Cuquierno	Cuquierno	Cuquierno	Cuquierno	Cuquierno	media		
Origen CVE					alta		
Cuquierno					oficial		

P	ID	Categoría	Severidad	Estado	Actualizada	Resumen
	0000017	General	media	asignada (Gmail Javier Gallardo)	15-12-2018	Múltiples Vulnerabilidades en Servicio OpenSSL
	0000016	General	alta	asignada (Gmail Javier Gallardo)	15-12-2018	Escritorio Remoto de Windows con bajo nivel de Protección
	0000015	General	alta	asignada (Gmail Javier Gallardo)	15-12-2018	Apache Tomcat End of Life
	0000014	General	alta	asignada (Gmail Javier Gallardo)	15-12-2018	WordPress

## Detalle de Vulnerabilidad (1)

**Sección superior con datos de identificación y seguimiento de estado actual de resolución**

ID	Proyecto	Categoría	Visibilidad	Fecha de envío	Última actualización
0000016	TestPY	[Todos los proyectos] General	público	15-12-2018 01:16	15-12-2018 01:16

Informador	javier Gallardo Warden	Asignada a	Gmail Javier Gallardo		
Prioridad	normal	Severidad	alta	Reproducibilidad	siempre
Estado	asignada	Resolución	abierta		
Plataforma	www.acme.cl (200.10.56.121)	SO	Windows Server	Versión de SO	

## Detalle de Vulnerabilidad (2)

Sección inferior muestra el detalle técnico de la vulnerabilidad

<b>Resumen</b>	000016: Escritorio Remoto de Windows con bajo nivel de Protección
<b>Descripción</b>	<p>Se detecta el uso del servicio de Escritorio Remoto de Windows con acceso universal, es decir, que se puede acceder a él desde cualquier ubicación.</p> <p>Este tipo de accesos no es recomendable, ya que un atacante que logre obtener las credenciales de administración podría acceder y tomar el control absoluto sobre el servidor.</p> <p>Para obtener las credenciales se pueden utilizar distintas técnicas entre las que se cuentan los ataques de inyección ARP combinados con un Man in the Middle, utilizando software disponible en la red. Ver referencia para un ejemplo sencillo.</p> <p>En forma adicional, para la instalación vigente se detecta que el protocolo TLSv1.0 acepta cifrado que actualmente es considerado débil, ya que un ataque de fuerza bruta es factible para obtener la clave de acceso: TLS_RSA_WITH_RC4_128_MD5</p>
<b>Solución</b>	<p>El Servicio de Escritorio Remoto puede ser protegido tomando las siguientes medidas:</p> <ol style="list-style-type: none"><li>1) Configurar que el acceso sólo esté permitido desde IP conocidas. Esto se puede realizar en el Firewall de Windows Server o en un firewall perimetral de la red.</li><li>2) Utilizar clave de usuario segura y reemplazarla regularmente. Se considera una clave segura aquella que tiene como mínimo 10 caracteres y considera, a lo menos, tres de los siguientes elementos: letras mayúscula, letras minúsculas, números y caracteres especiales. Los números y letras no deben ser consecutivos. La rotación de clave, es decir, su cambio en el tiempo, no debe superar los 90 días.</li><li>3) Utilizar encriptación de alto nivel de seguridad. Certificados TLSv1.0 o superior con clave de encriptación de 512 bits o más.</li></ol>
<b>Información adicional</b>	<p>Ejemplo de Ataque sobre Escritorio Remoto: <a href="https://multi-byte.aesniderhonto.com/how-to-hack-like-pro-fuck-remote-desktop-protocol-rdp-snatch-tyadmin-password-014970/">https://multi-byte.aesniderhonto.com/how-to-hack-like-pro-fuck-remote-desktop-protocol-rdp-snatch-tyadmin-password-014970/</a></p> <p>Información sobre la configuración de Algoritmos de Cifrado en Windows Server se puede encontrar en : <a href="https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc">https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc</a></p>
<b>Etiquetas</b>	Sin etiquetas adjuntas.
<b>Adjuntar Etiquetas</b>	Deparado por [1] <input type="text"/> Etiquetas existentes <input type="text"/> <input type="button" value="Ajustar"/>
<b>Código CVE</b>	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
<input type="button" value="Editar"/> <input type="button" value="Monitorizar"/>	

## Notas y Comentarios

Las notas permiten la comunicación entre el especialista y el resolutor.

Añadir nota

Nota

Subir archivos  
Tamaño máximo: 2,097,152

Coloca archivos aquí para cargarlos (o pulsa)

Añadir nota