

¿Que es CLOUD SECURITY TEST®?.....	1
¿Qué significa “On Results Penetration Testing”? .....	1
¿En qué se diferencia respecto de evaluaciones continuas para certificación WEB?.....	1
¿Quiénes pueden suscribirse?.....	1
¿Cómo me suscribo al servicio CLOUD SECURITY TEST®? .....	2
¿Que obtengo con la compra de vulnerabilidades o verificaciones?.....	2
¿Qué significa Hacking Secure®?.....	2
¿Como puedo usar el SELLO de “Hacking Secure®”? .....	3
¿Como pago por las vulnerabilidades?.....	3
¿Cuál es el listado de pruebas de seguridad? .....	3
¿Cuál es el catálogo de vulnerabilidades que puedo comprar? .....	4
¿Cuál es el criterio de costos por vulnerabilidad? .....	6
¿Cómo se desarrolla el servicio? .....	6

**¿Que es CLOUD SECURITY TEST®?**

Es el primer y único servicio de evaluaciones periódicas de seguridad basado en el modelo de On-Results Services, sin costo de inversión y donde solo, a partir del descubrimiento de vulnerabilidades y en base a su necesidad, usted decide cuales problemas desea conocer, analizar y profundizar para resolver en forma inmediata.

**¿Qué significa “On Results Penetration Testing”?**

Es la nueva generación de servicios de evaluaciones de seguridad ofrecida con una metodología de comercialización de “desembolso por resultados”. Somos los primeros en establecer el nuevo concepto de provisión de servicios de evaluaciones de seguridad donde el cliente abona exclusivamente las vulnerabilidades que concretamente presentan inconvenientes reales para su resolución.

**¿En qué se diferencia respecto de evaluaciones continuas para certificación WEB?**

Nuestra metodología de evaluación contempla procedimientos operativos con idénticos niveles de calidad de servicio a los existentes en nuestros Penetration Testing Tradicionales (NO un VRA), que se caracterizan por analizar, valorizar el negocio y detallar su estado en informes ejecutivos y técnicos. A esto se agrega un nivel adicional de evaluación producto de la ejecución y gestión continua de análisis de riesgos en toda la infraestructura de borde, lo que permite avalar el compromiso para TODO el DOMINIO en Internet de la empresa.

**¿Quiénes pueden suscribirse?**

Todas aquellas compañías con capacidad de contratación que pertenezcan al mercado hispano-americano y tengan como mínimo un dominio corporativo en Internet (DOMINIO.com, DOMINIO.com.ar, etc).



### ¿Cómo me suscribo al servicio CLOUD SECURITY TEST®?

Para la suscripción del servicio usted deberá seguir los siguientes pasos:

- I. **REGISTRACIÓN:** A través de nuestro sitio WEB, deberá completar toda la información necesaria y requerida en el formulario de Registro.
- II. **SUSCRIPCIÓN:** Confirmamos su identidad, convenimos una conferencia telefónica y le contamos todos los detalles y responsabilidades del servicio.
- III. **ALTA:** Cargamos toda su información en nuestros sistemas y le entregamos el acceso al aplicativo de "Cloud Security Network" donde podrá acceder al Portal Web y comenzar a tratar los resultados.

### ¿Que obtengo con la compra de vulnerabilidades o verificaciones?

Con cada una de las compras, sean éstas vulnerabilidades o verificaciones se hace entrega de un "informe de descubrimiento" y un "informe de verificación" correspondientemente.

Los "informe de descubrimiento" incluyen:

- La descripción y explicación técnica detallada de la vulnerabilidad.
- La matriz de riesgo aplicada.
- Las recomendaciones para la resolución de la misma.

Los "informe de verificación" incluyen:

- La descripción y explicación técnica detallada de la vulnerabilidad.
- La matriz de riesgo aplicada.
- Las pruebas, confirmación y evidencia de resolución efectiva.

Con la compra de dos (2) vulnerabilidades mensuales se hace entrega de un "informe ejecutivo" con las siguientes características:

- El alcance operativo desarrollado al día de la fecha.
- Las vulnerabilidades adquiridas, no adquiridas y aquellas verificadas y no verificadas.
- La perspectiva general de riesgo del dominio, con la valoración de nivel global del riesgo de la compañía.
- Conclusiones y recomendaciones de los analistas.

### ¿Qué significa Hacking Secure®?

Hacking Secure® es el término utilizado en el SELLO que podrán utilizar los clientes suscriptos en todos sus sitios como acreditación de su compromiso con la seguridad en Internet.



### ¿Como puedo usar el SELLO de “Hacking Secure®”?

Usted adquiere el derecho de uso del SELLO a partir de la primera compra y podrá utilizarlo en todos los sitios de su dominio y sin importar la cantidad. Sus clientes haciendo CLICK en el sello incluido en su WEB obtienen un certificado virtual de validación. Dicho certificado podrá ser utilizado y referenciado por usted en otros contextos y de acuerdo con sus estrategias comerciales. La inclusión del SELLO en su sitio WEB es muy sencilla ya que solo requiere agregar unas pequeñas líneas de código HTML en sus páginas.

### ¿Como pago por las vulnerabilidades?

A través del DASHBOARD seleccionará las vulnerabilidades que quiera adquirir y nuestro sistema nos enviará la orden de compra correspondiente. Con la recepción de la orden de compra, nos ponemos en contacto con usted con la Orden de Pago correspondiente con las siguientes alternativas:

- Con DineroMail.
- Con PayPal.
- Con una transferencia bancaria.

### ¿Cuál es el listado de pruebas de seguridad?

A continuación enumeramos el listado de pruebas que serán realizadas en forma continua por nuestro equipo de investigadores, que representa a su vez el catálogo de vulnerabilidades que usted podrá gestionar, seguir y remediar.

#### Detección de vulnerabilidades en aplicativos WEB y Base de Datos



- ▶ SQL Injection
- ▶ Remote File Inclusion
- ▶ Local File Inclusion
- ▶ Authentication bypass
- ▶ File Upload
- ▶ Cross Site Scripting
- ▶ LDAP Injection
- ▶ Session Fixation
- ▶ X-Path Injection
- ▶ Injection Header
- ▶ HTTP Response Splitting



#### Detección de vulnerabilidades en su infraestructura de red

- ▶ Port Scanning
- ▶ Servidores de correo electrónico
- ▶ Servidores de nombres de dominio
- ▶ Validación de certificados SSL



**Detección de riesgos de pérdida o manipulación de información**

- ▶ Debilidades de CAPTCHA
- ▶ Errores de diseño
- ▶ Contraseñas débiles.

**¿Cuál es el catálogo de vulnerabilidades que puedo comprar?**

El siguiente listado representa las vulnerabilidades que pueden ser descubiertas y podrán ser adquiridas. Es el mismo listado anterior, pero incluyendo las denominaciones y descripciones que utilizaremos en nuestro sistema Cloud Security Network y en todos los informes.

Nombre corto	Nombre largo y descripción.
<b>SQL Injection</b>	<b>Manipulación de base de datos</b> Es uno de los ataques más conocidos y de mayor impacto hoy en día. Los servidores de base de datos que se encuentran como back-end de los aplicativos WEB de su compañía, guardan información confidencial y de negocio, que pueden ser vulnerables a sustracción de información con técnicas de inyección de código.
<b>Remote File Inclusion</b>	<b>Ejecución de código arbitrario</b> La inclusión de páginas dinámicas sin las correctas validaciones puede ser utilizada por un atacante para ejecutar código remoto que le permita acceder al equipo.
<b>Local File Inclusion</b>	<b>Lectura de archivos de sistema y/o ejecución de código arbitrario</b> Sin la correcta validación para la inclusión de páginas locales un atacante podría acceder a archivos de configuración, credenciales de acceso y hasta ejecutar código arbitrario.
<b>Authentication bypass</b>	<b>Manipulación del sistema de autenticación y/o autorización.</b> Una incorrecta definición e implementación de los sistemas de autenticación y autorización para usuarios en los aplicativos podría permitir accesos no autorizados, robo de información y fraude.
<b>File Upload</b>	<b>Carga de archivos maliciosos.</b> La manipulación aplicativa durante la carga de archivos puede permitir ataques de pérdida de información, disrupción de servicios y/o acceso al servidor.
<b>Cross Site Scripting</b>	<b>Ejecución de código arbitrario en clientes.</b> Vulnerabilidades destacadas por la falta de validación de entradas en aplicaciones WEB que permite la ejecución de código arbitrario en los clientes que pueden ser utilizados para ataques de Phishing, Malwares y Worms.
<b>LDAP Injection</b>	<b>Robo de información en árbol LDAP.</b> La escasa validación de entradas de usuario en aplicaciones WEB con Back-end LDAP permite a un atacante el acceso, y robo de información en el árbol de datos.
<b>Session fixation</b>	<b>Robo de sesión de usuarios.</b> La falta de controles en la implementación de mecanismos de autenticación y autorización pueden provocar el robo de identidad de usuarios, operaciones fraudulentas y violación de la privacidad de los usuarios.
<b>X-Path Injection</b>	<b>Manipulación de información aplicativa.</b> Vulnerabilidades presentes con la falta de validación en las estructuras X-Path que

## Preguntas Frecuentes (FAQ)

	permite a un atacante manipular las entradas de usuarios con el fin de modificar o robar dichas estructuras y/o archivos XML de aplicación con información aplicativa privada.
<b>Debilidad de Captcha</b>	<b>Abuso de formularios WEB</b> Los sistemas CAPTCHA débiles que sean implementados para el control de suscripciones, registración y el envío de información de usuarios carecen de complejidad suficiente para evitar operaciones automatizadas de abuso y violación de procesos de negocio.
<b>Contraseñas débiles</b>	<b>Descubrimiento de Credenciales de usuarios</b> La falta de políticas de complejidad de contraseñas y las implementaciones productivas sin procedimientos adecuados permite a los atacantes descubrir contraseñas débiles de usuarios finales y/o cuentas administrativas.
<b>Error de diseño</b>	<b>Violación de funcionalidades aplicativas</b> Las funcionalidades ofrecidas por los aplicativos WEB con escasos controles técnicos pueden generar abusos y violación de las políticas de uso establecidas en sus procesos de negocio.
<b>Validación de certificados SSL</b>	<b>Suplantación y validez de su dominio corporativo.</b> Validar los certificados SSL nos permite identificar y confirmar la veracidad del origen de los datos en su sitio en Internet, como así también fortalecer el flujo de datos para mantener la privacidad de sus usuarios.
<b>Injection Header</b>	<b>Abuso de respuestas WEB en clientes</b> Algunas implementaciones con una precaria comprobación de variables permiten a los atacantes manipular las respuestas HTTP para generar ataques de ejecución de código arbitrario en los clientes, utilizado en la ejecución de técnicas de Phishing.
<b>HTTP response splitting</b>	<b>Manipulación del contenido de respuestas WEB</b> Las implementaciones con falta de comprobación de variables pueden generar una manipulación del contenido de la respuesta HTTP y combinarse con otras técnicas de Malware, Phishing y Worms.
<b>E-MAIL Vulnerabilities</b>	<b>Abuso de identidades corporativas y SPAMMING</b> Los servidores de correo electrónico pueden poseer vulnerabilidades que permitan a un atacante descubrir usuarios y generar ataques de abuso de identidades corporativas para utilizar en técnicas de Phishing y SPAMMING.
<b>DNS Vulnerabilities</b>	<b>Robo de dominios corporativos.</b> La falta de controles y los descuidos en la configuración de los servidores de dominio permiten que un atacante pueda realizar ataques de envenenamiento de cache o negación de servicio que pone en riesgo su negocio.
<b>Port Scanning</b>	<b>Protocolos y puertos en Internet.</b> Identificar que tipo de conexiones se pueden realizar a sus servidores, es de vital importancia para saber los potenciales ataques a los que se encuentra expuesto. La identificación de protocolos, servicios y aplicaciones brinda información suficiente para mejorar los procesos operativos de control y acceso de su negocio.

### ¿Cuál es el criterio de costos por vulnerabilidad?

Las vulnerabilidades están agrupadas por niveles de importancia para aspectos de negocio (grises oscuro a mas claro en cuadro anterior), resultando en ese orden las vulnerabilidades de mayor a menor "importe". Dicho importe tiene un factor de multiplicación asociado al riesgo que cada vulnerabilidad representa para esa compañía y/o negocio en particular.

### ¿Cómo se desarrolla el servicio?

Luego del proceso de ALTA de suscripción, su DOMINIO se incorpora a nuestro procedimiento interno de evaluación continua desarrollada en forma metódica por especialistas de seguridad que aportan un alto nivel de análisis y valoración de los resultados que se obtienen. A continuación enumeramos las distintas situaciones que forman parte de nuestra metodología operativa Cloud Security Test®.

- I. **HALLAZGO:** Para la identificación de las vulnerabilidades listadas, se utilizan herramientas y técnicas que nos permiten descubrir los riesgos a los que se encuentra expuesta la infraestructura de borde de su compañía.
- II. **ANÁLISIS:** Nuestros analistas en seguridad examinan detalladamente las vulnerabilidades y debilidades detectadas, recolectando evidencia concreta que permita confirmar cada una de ellas.
- III. **VALORACIÓN:** Nuestros especialistas clasifican la información de acuerdo a nuestro "Procedimiento de criterio de riesgo piramidal" que nos permite establecer el nivel de riesgo de las vulnerabilidades detectadas y los planes de remediación.
- IV. **INFORME:** La información analizada y valorada se organiza en un "informe de descubrimiento" por cada vulnerabilidad, y la misma se ingresa en la base de datos como "disponible" para poder ser seleccionada por el cliente.
- V. **COMPRA:** El Cliente es notificado por email de cada descubrimiento disponible; ingresando al DASHBOARD genera la "Orden de Compra" sobre la/s selección/es de vulnerabilidades y/o verificaciones. Cuando se cancela el saldo de la Orden de pago, el "informe de descubrimiento" o el "informe de verificación" puede ser descargado desde el mismo portal.
- VI. **VERIFICAR:** Con el "informe de descubrimiento" usted estaría en condiciones de resolver la vulnerabilidad descubierta, asimismo las vulnerabilidades en el DASHBOARD solo aparecerán como solucionadas al haber "Verificado" su corrección.