Preguntas frecuentes para completar el SAQ a través de la herramienta ZeroRisk de Advantio

Algunas directrices y respuestas a Preguntas Frecuentes:

SAQ (Cuestionario de Autoevaluación)

- **Los navegadores homologados para el uso de la aplicación son los siguientes:**

  Microsoft IE version 10+
  Microsoft Edge version 14+
  OSX Safari 9+
  Mozilla Firefox 34+
  Google Chrome 42+
  Si en algún momento el explorador nos "echa" de la sesión, la solución más práctica es abrir una ventana privada o de incógnito y completar el proceso desde la misma. O bien limpiar los cookies del registro del navegador.

- El cuestionario **no tiene que completarse en una sola sesión**. Se puede interrumpir en cualquier momento y retomarlo después.
- El proceso a través del cuestionario dispone de un **chat online** para ir consultando dudas que surjan en el momento.
- La primera indicación a tener en cuenta es que, especialmente en aquellos casos en que los **datafonos** que nos ha provisto el banco estén **conectados a través de ADSL** en lugar de línea telefónica, se va a requerir consultar al informático para responder a algunas preguntas técnicas.
- El proceso comienza con una serie de preguntas para identificar el **SAQ (Cuestionario de Autoevaluación)**, que corresponde a cada agencia, en función de su uso de medios de pago por tarjeta.
- En el siguiente paso, si el banco ha indicado a la agencia, con claridad, el SAQ que debe rellenar, puede elegirlo directamente. En caso contrario, nuestra herramienta le guiará para identificarlo fácilmente.
  En caso de que alguna agencia inicie el proceso de evaluación y entienda que **escogió el SAQ incorrecto**, puede dirigirse a nosotros para resetear el proceso y que vuelva a empezar desde el principio.
- Incluso si el SAQ que la aplicación nos ofrece es un **SAQ D** y no parece encajarnos, muy probablemente será un **SAQ D simplificado**, en el que se habrán descartado como "no aplicables" una cantidad importante de preguntas. (Observar el porcentaje de finalización que aparece en la parte superior izquierda).

- Para que el SAQ resulte en estado “completado” la respuesta a todas las preguntas del formulario debe ser “SI”. Las preguntas a las que entendemos que debemos responder “NO”, requerirán que tomemos acción para rectificar la forma en que estamos operando en nuestra empresa y ajustarlo al requisito que indicaba la pregunta en cuestión.

- Preguntas relacionadas con el entorno de red, en caso de **datafonos conectados por ADSL (Diagrama)**

COMERCIOS CON DATÁFONOS CONEXIÓN ADSL

Componentes técnicos necesarios

La siguiente recomendación se focaliza en minimizar el número de componentes técnicos necesarios dentro del entorno de cumplimiento PCI DSS para los datafonos.

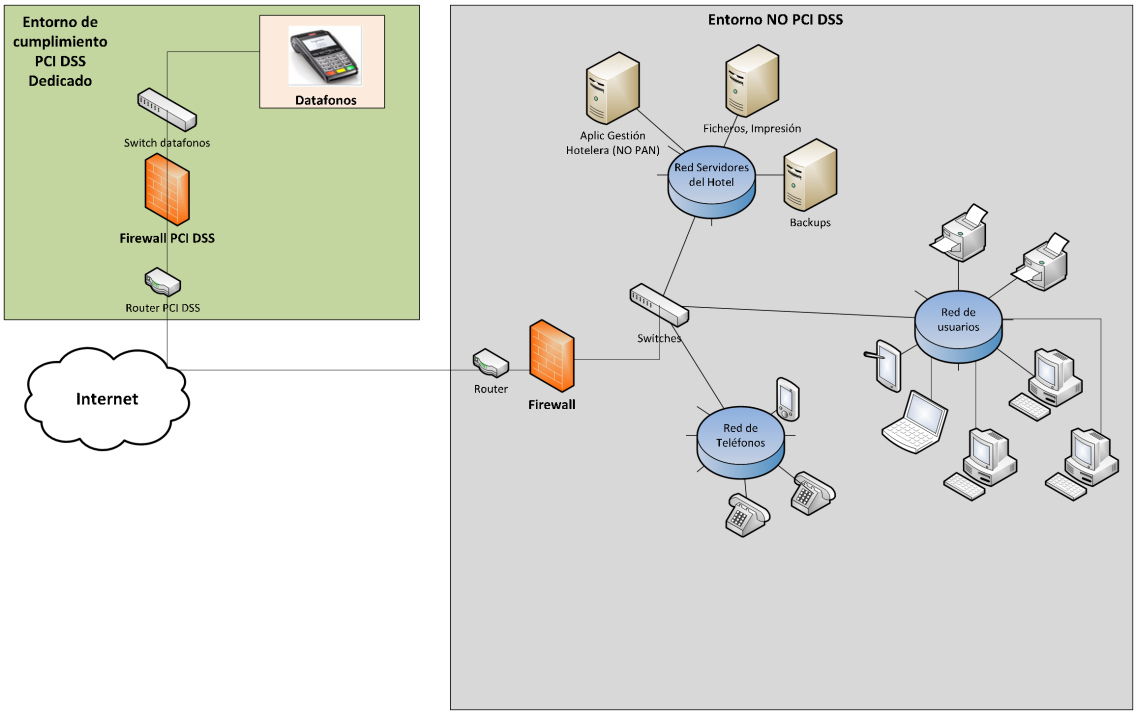
El entorno tecnológico de cumplimiento PCI DSS propuesto estará formado por:

- Datafonos
- Router de conexión a Internet
- Firewall perimetral
- Switch de comunicaciones dedicado a los datafonos
- Redes Wireless: No existirán redes Wireless salvo si los datafonos son inalámbricos, pero en este caso la certificación PCI PTS del dispositivo ya garantiza la seguridad de los datos en tránsito. Por ejemplo, el router de acceso a Internet no debe ser Wireless y si lo es deberá estar desactivada la interfaz Wireless.

Alternativas de aislamiento

En los siguientes esquemas se proporcionan dos visiones para implementar el aislamiento del entorno PCI DSS:

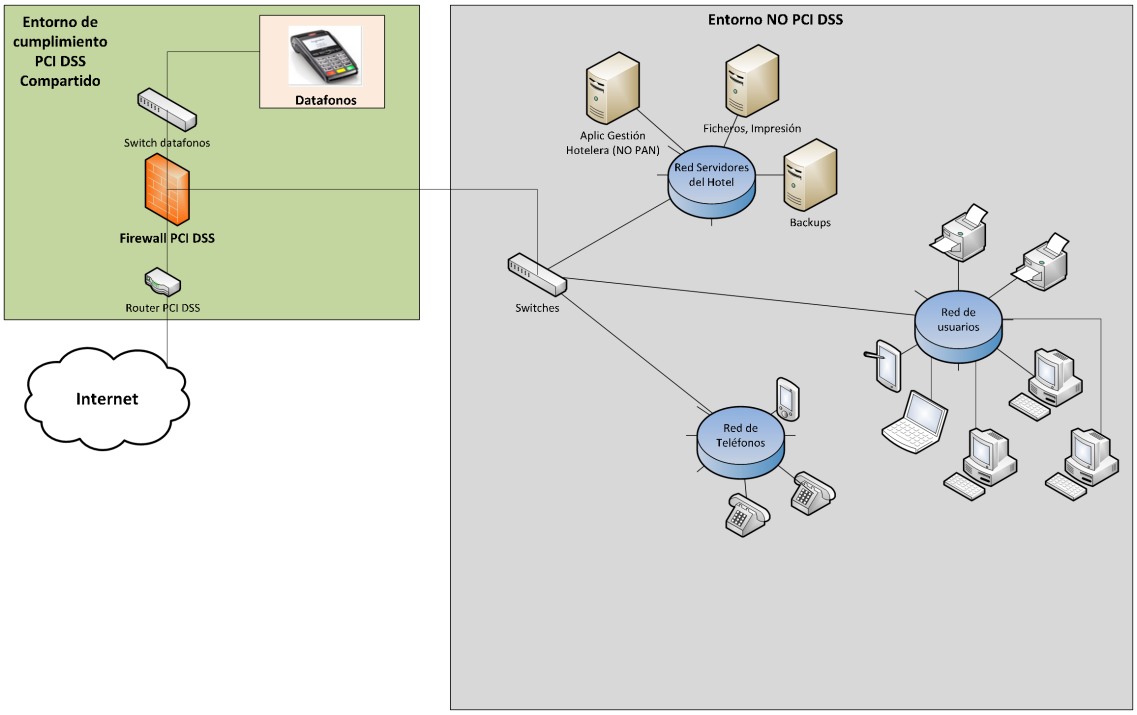
ENTORNO PCI DSS DEDICADO



Todos los componentes tecnológicos comentados anteriormente estarían dedicados exclusivamente a la red PCI.

Esto conlleva una mayor inversión económica (Firewall, router, conexión a Internet) pero proporciona una separación completa entre red PCI y red No PCI. El mantenimiento del cumplimiento con PCI DSS no impacta en el resto de procesos de negocio de la agencia, únicamente en el pago presencial con los datafonos.

ENTORNO PCI DSS PARCIALMENTE COMPARTIDO



En este caso, el router y el firewall perimetral, con el objetivo de reducir inversión por parte de la agencia, serán compartidos entre la red PCI y la red No PCI. Estos dos elementos se encargan de separar los dos segmentos de red y como tal, tienen que estar siempre dentro del cumplimiento de PCI DSS aplicando todos los controles necesarios.

La ventaja de este esquema es el reaprovechamiento de elementos tecnológicos y por tanto la reducción de la inversión económica.

La desventaja es que PCI DSS es una norma muy exigente en cuanto a medidas de seguridad y por tanto compartir estos elementos puede limitar la flexibilidad y rapidez a la hora de poder implementar cambios en la red No PCI (nuevos servicios, paradas de servicio por actualizaciones en el firewall y en el router, etc.). Si se disponen de dispositivos dedicados a la red PCI DSS, la agencia podría implementar en el router y firewall de la red No PCI las medidas de seguridad que considere oportunas en base al riesgo que suponga para su negocio.

- **SOPORTE** ofrecido por Advantio en la herramienta ZeroRisk: se trata de soporte técnico, no relacionado con dudas sobre las preguntas del SAQ.

P: ¿Por qué se propone como opción de contratación la Premium que incluye 3 años? ¿Puedo escoger otra opción?

R: El cuestionario de autoevaluación SAQ debe ser completado anualmente. El portal Advantio ZeroRisk contiene funcionalidades que sirven de un año para el siguiente y lo simplifica, (ej. Avisa cuando vence al final del año e informa de novedades relativas a PCI). Todo lo cual ha hecho que todos los estamentos involucrados en la preparación de este proyecto hayan recomendado plantearlo como paquete para 3 años.
Se puede acceder a otras opciones de contratación a través de un link bajo el botón “Seleccionar”.

P: ¿Por qué veo un vídeo cuando entro en la aplicación por primera vez? ¿Puedo desactivarlo?

R: El video es una breve introducción que tiene como objetivo aumentar su conciencia sobre el proceso (y usted puede saltarse mirarlo si lo prefiere).

Después de finalizar el asistente de inscripción, no se volverá a mostrar.

P: ¿Qué es el asistente de inscripción?

R: El asistente de inscripción le guiará automáticamente a través de las preguntas SÍ/NO para que se pueda detectar el SAQ correcto/relevante.

Al utilizar la aplicación, evolucionará a lo largo de una serie de estados, desde la inicial no inscrita hasta la conformidad (no inscrita > inscrita > inscrita > no conforme > conforme).

Una vez que se identifica y asigna una categoría de SAQ, su estatus se inscribe y después de eso, hay un par de pasos lejos del cumplimiento de PCI DSS.

La meta se está cumpliendo. Cuando sea compatible, la presentación y descarga SAQ será posible.

P: ¿Qué es un SAQ? ¿Qué significa SAQ?

R: Los cuestionarios de autoevaluación del DSS PCI (SAQ) son herramientas de validación destinadas a ayudar a los comerciantes y proveedores de servicios a informar sobre los

resultados de su autoevaluación del DSS PCI. Los diferentes tipos de SAQ le ayudan a identificar qué SAQ se aplica mejor a su organización.

Las entidades deben asegurarse de que cumplen todos los requisitos para un determinado SAQ (antes de utilizar el SAQ).

Se recomienda a los comerciantes que se pongan en contacto con su banco comercial (adquirente) o con la (s) marca (s) de pago aplicable (s) para identificar el SAQ apropiado en función de su elegibilidad.

P: ¿Qué son los controles de compensación?

R: En el sector de las tarjetas de pago, se introdujeron controles compensatorios en PCI DSS 1.0, para dar a las organizaciones una alternativa a los requisitos de seguridad que no podían satisfacerse debido a limitaciones tecnológicas o empresariales legítimas. Según el Consejo PCI, los controles compensatorios deben realizarse:

1) Cumplir con la intención y el rigor del requisito original declarado

2) Proporcionar un nivel de defensa similar al requerido originalmente establecido

3) Estar "por encima y más allá" de otros requisitos PCI DSS (no simplemente en cumplimiento de otros requisitos PCI DSS)

4) Estar en consonancia con el riesgo adicional impuesto por no respetar el origen.

P: ¿Cuál es la tasa de porcentaje (%) (por ejemplo, 43%, 50%, 50%, 80%, etc.) además de mi SAQ?

R: Ese número es un indicador que muestra qué porcentaje de las preguntas (en el SAQ) se ha completado (respuesta).

A medida que continúe contestando las preguntas, la tasa de finalización se actualizará simultáneamente.

Cuando llega al 100%, significa que todas las preguntas son contestadas, y usted puede enviar su SAQ

GENESiS (Escaneos de Vulnerabilidad de Red)

- Una vez dentro del portal (Dashboard), se puede seleccionar **GENESiS**, a la izquierda.
- El primer paso es dar de alta la IP o el Dominio. Seleccionar "**IP"** si se dispone de la numeración 199.34.218.66. O "**Dominio",** si se dispone de la URL (ej: advantio.com)
- Una vez que tenemos dada de alta la IP o Dominio, se solicita un nuevo Scan y se ejecuta. Hay que hacer un scan cada 3 meses.

P: ¿Qué es GENESiS?

R: GENESiS es el módulo que se utiliza ZeroRisk para ejecutar los escaneos ASV automáticamente; a través de Qualys.
ASV significa (Approved Scanning Vendor).

P: ¿Qué es ASV Scan y por qué se necesita?

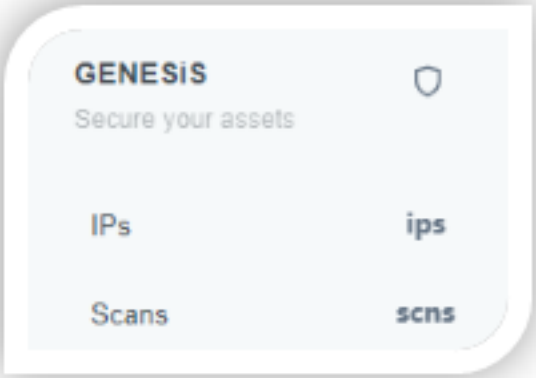
R: Los escaneos ASV son necesarios por la presencia del Requisito 11.2.2.
El Consejo PCI ordena que todas las direcciones IP orientadas a Internet sean exploradas en busca de vulnerabilidades.
Para demostrar el cumplimiento, los comerciantes y proveedores de servicios deben tener análisis periódicos de seguridad definidos por cada empresa de tarjetas de pago. Estos escaneos son realizados a través de Internet por un ASV (Approved Scanning Vendor) y es una herramienta indispensable para ser utilizada en conjunto con el programa de gestión de vulnerabilidades. Los escaneos ayudan a identificar las vulnerabilidades y configuraciones erróneas de los sitios web, aplicaciones e infraestructuras de tecnología de la información (TI) con direcciones IP (Protocolo de Internet).

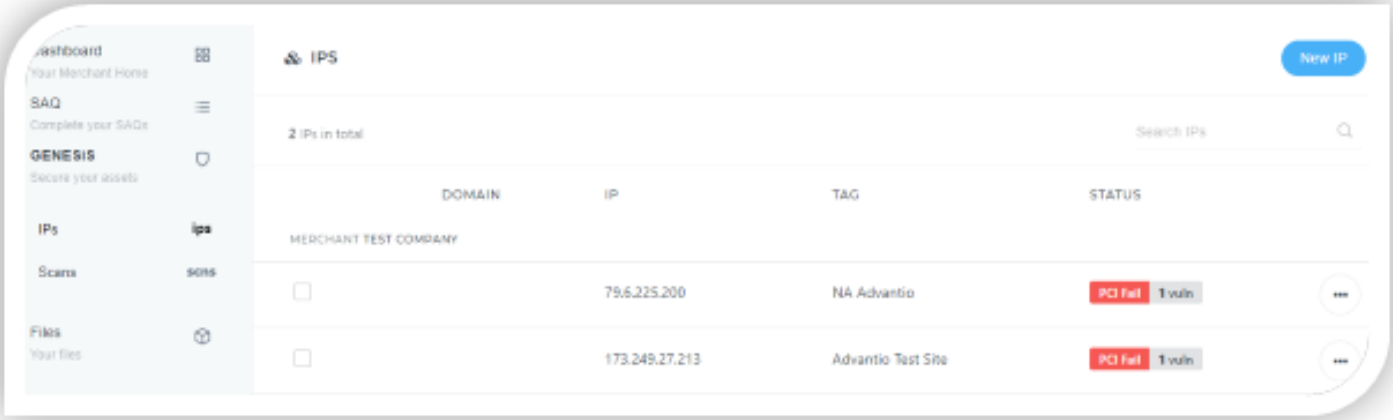
P: ¿Qué IP o Dominio debo escanear?

R: Si la agencia tiene plataforma de e-commerce a través de la página web pública, es necesario escanear el dominio de la web.
Adicionalmente es necesario escanear la dirección IP pública del router que da servicio a la red de la oficina.

P: ¿Cómo puedo añadir las direcciones IP/IP a escanear?

R: Se pueden añadir hasta un máximo de 20 IPs. Para registrar/declarar una IP, acceda al submenú **IPs** (bajo GENESiS), luego haga clic en Nueva IP:

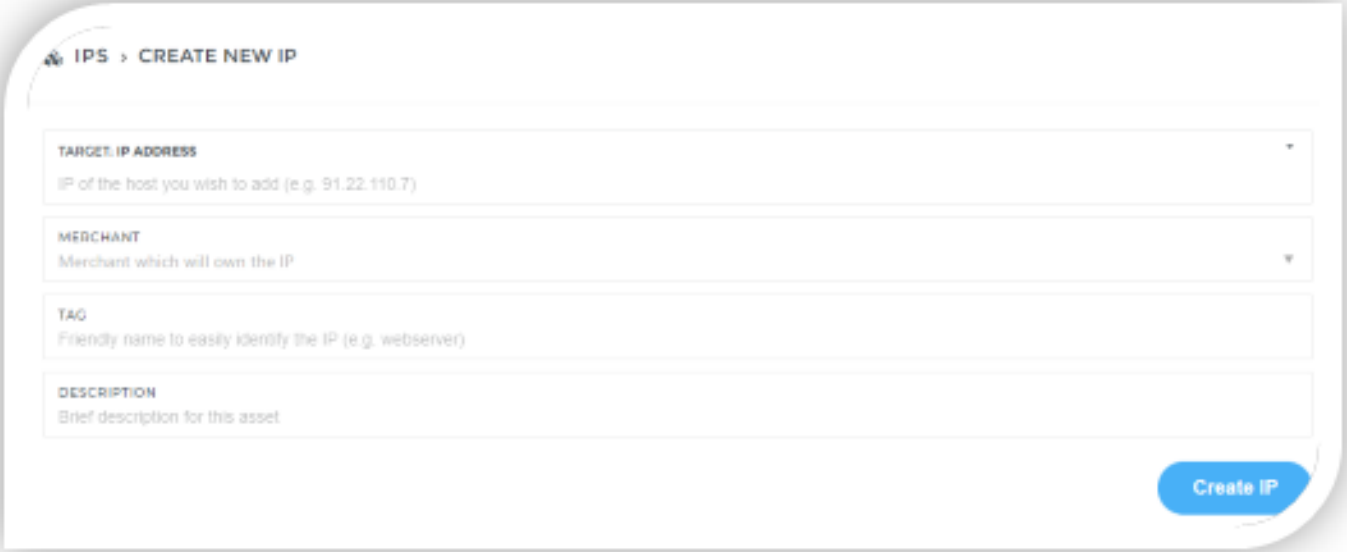




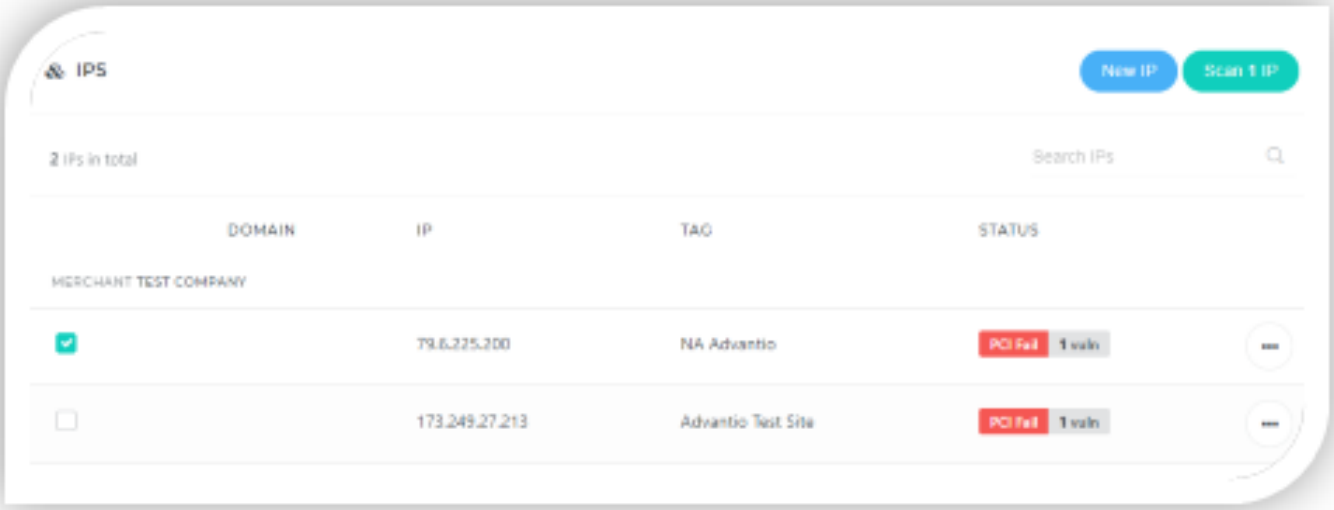
Proveer:

Dirección IP de destino
Detalles del comerciante
Etiqueta fácil de usar
Breve descripción

Pulse el botón Crear IP.

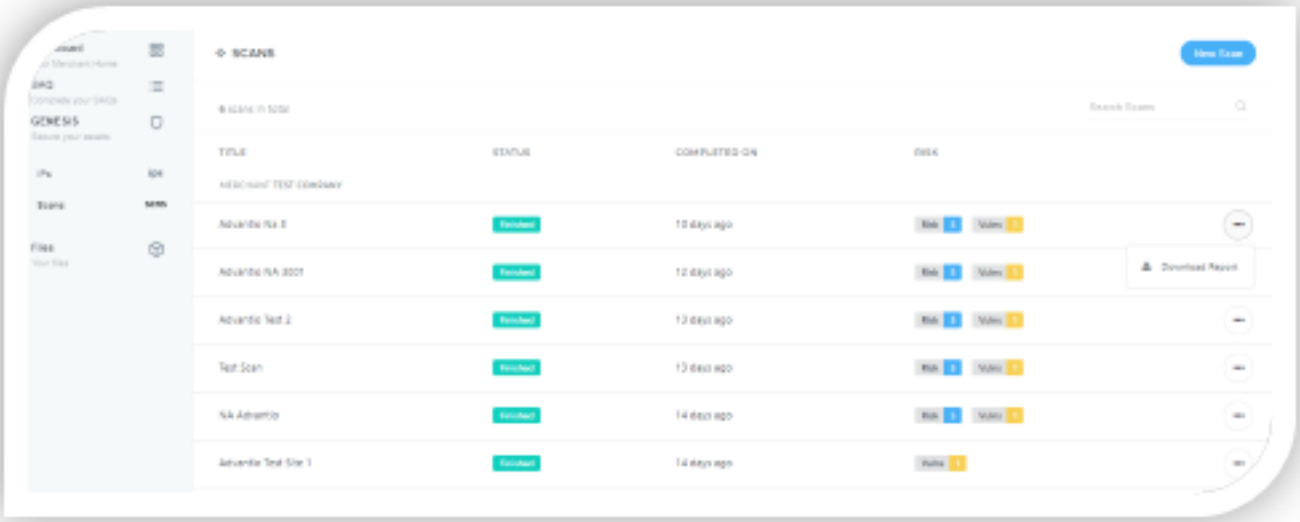


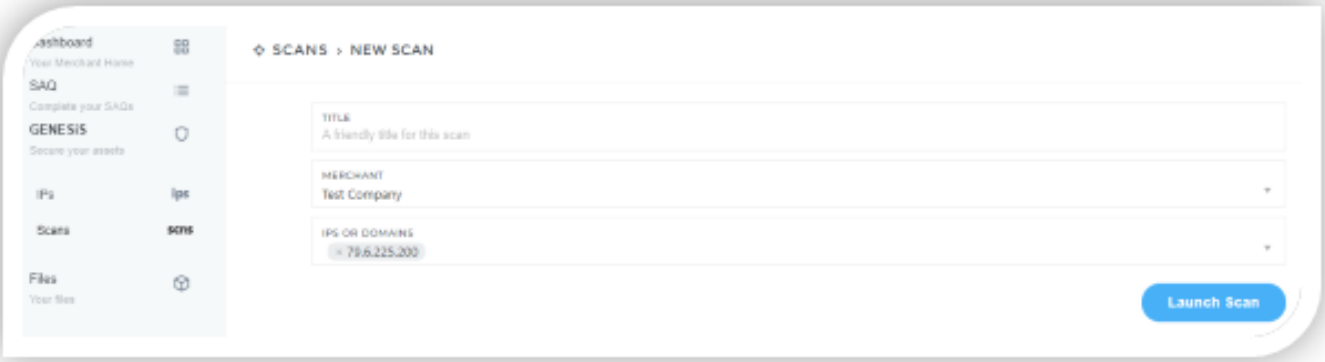
Una vez que la IP ha sido ingresada, marque con una cruz la que se va a escanear.
Importante marcar de una vez todas las que tengan que escanearse. En este caso solo se consumirá 1 escaneo, de los 5 incluidos en el paquete Premium, (todas las IPs quedarán escaneadas con dicho escaneo).
Luego, haga clic en SCAN 1 IP



Alternativamente, para iniciar un escaneo;

1 Ir a **GENESiS**
2 Haga clic en el submenú **Escaneos**
3 Pulse en **Nuevo Escaneo**
4 Rellene el nombre (título) de la exploración, los detalles del usuario (es decir, el nombre del comerciante) y las direcciones IP o dominios que se van a escanear.
Importante marcar de una vez todas las que tengan que escanearse. En este caso solo se consumirá 1 escaneo, de los 5 incluidos en el paquete Premium, (todas las IPs quedarán escaneadas con dicho escaneo).
Luego, haga clic en SCAN IP
5 Una vez listo, pulse **Iniciar escaneo.**

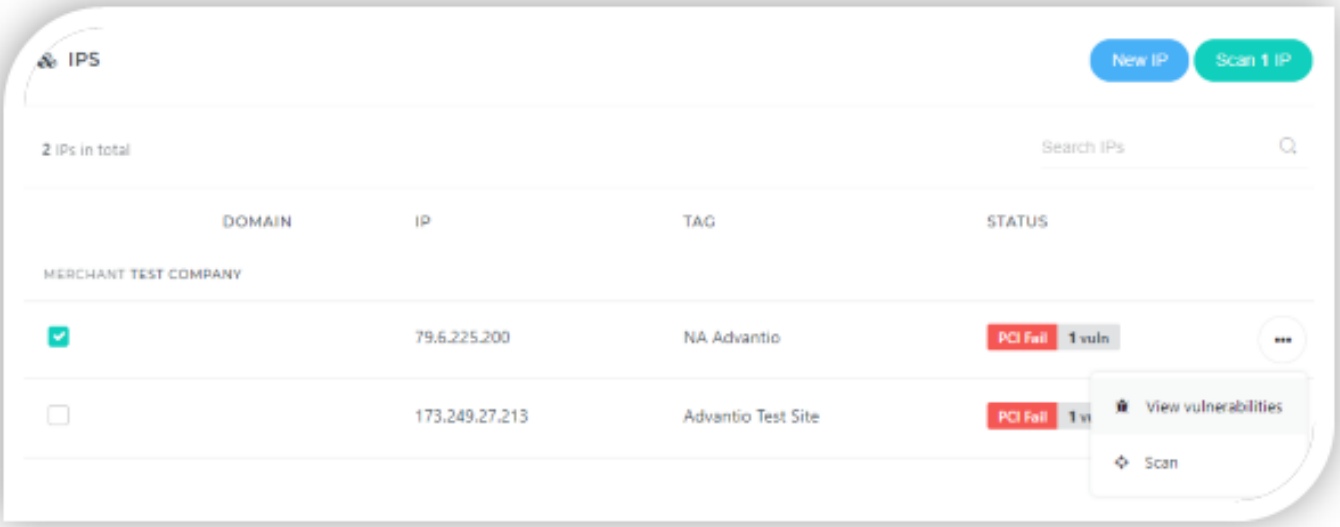




P: El escaneo ha terminado (finalizado), ¿cómo puedo ver el resultado?

R: Tan pronto como se finaliza el análisis, se generan resultados de pruebas (findings) y se puede acceder a estos pulsando **Ver vulnerabilidades**.

1 Ir a **GENESiS**
2 Pulse sobre el submenú **IPs**
3 Encuentre la IP escaneada
4 Haga clic en el icono horizontal de la elipsis/triple punto **(...)**
5 Haga clic en **"Ver vulnerabilidades".**

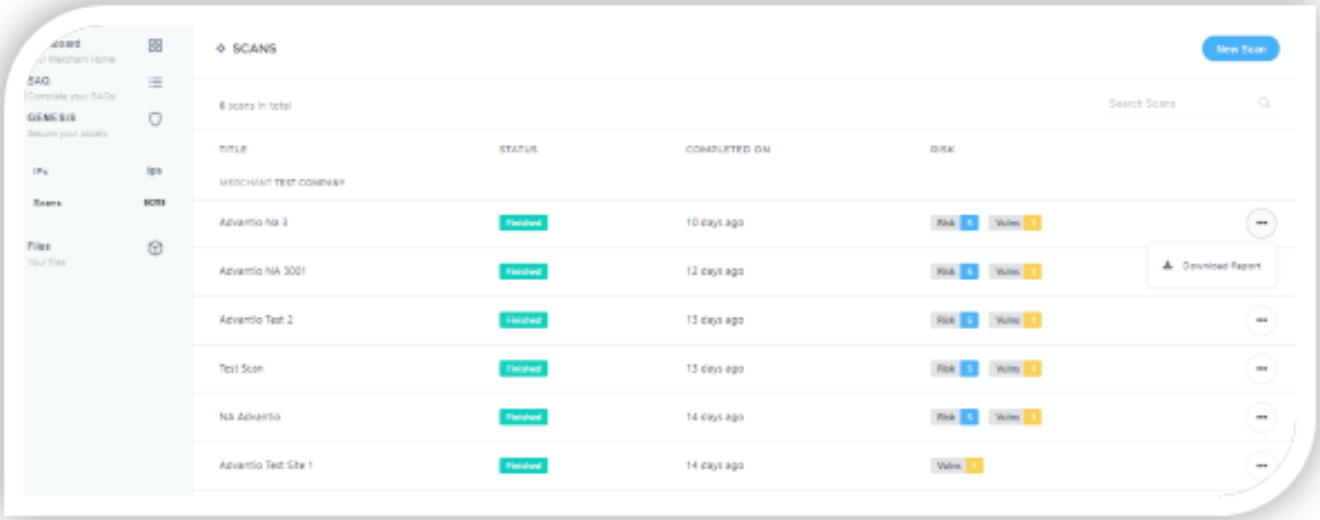


P: El escaneo ha terminado (finalizado), ¿cómo puedo obtener el informe?

R: Tan pronto como se realiza el escaneo, el informe (en formato pdf) se puede descargar.

1 Ir a **GENESiS**
2 Haga clic en el submenú **Escaneos**
3 Pulsar el icono de la elipsis horizontal/triple punto (...)

4 A continuación, pulse el botón **"Descargar informe"**.



P: ¿Cómo puedo interpretar el riesgo?

R: Los ASVs producen un informe informativo basado en los resultados de las exploraciones de la red. El informe describe el tipo de vulnerabilidad o riesgo, un diagnóstico de los problemas asociados y una guía sobre cómo corregir o reparar las vulnerabilidades aisladas. El informe asigna una "calificación/puntuación" para las vulnerabilidades identificadas en el proceso de análisis.

o **Nivel 5 (gravedad urgente),** vulnerabilidades habilitan a los intrusos remotos con capacidades remotas de raíz o administrador remoto; para que los hackers puedan comprometer a todo el host, los hackers remotos pueden tener capacidades completas de lectura y escritura del sistema de archivos, y pueden ejecutar comandos como usuario de raíz o administrador. La presencia de puertas traseras y troyanos también califican como vulnerabilidades de Nivel 5

o **Nivel 4 (gravedad crítica),** vulnerabilidades habilitan a los intrusos con usuario remoto, pero no capacidades de administrador remoto o usuario root. Las vulnerabilidades de nivel 4 proporcionan a los hackers un acceso parcial a los sistemas de archivos (por ejemplo, acceso de lectura total sin acceso de escritura total). Las vulnerabilidades que exponen información altamente sensible califican como vulnerabilidades de Nivel 4

o **Nivel 3 (alta gravedad)** proporcionan a los hackers acceso a información específica almacenada en el host, incluidas las configuraciones de seguridad. Este nivel de vulnerabilidad podría dar lugar a un posible uso indebido del host por parte de los intrusos. Entre los ejemplos de vulnerabilidades del nivel 3 se incluyen la divulgación parcial del contenido de los archivos, el acceso a determinados archivos del host, la exploración de directorios, la divulgación de reglas de filtrado y mecanismos de seguridad, la susceptibilidad

a ataques de denegación de servicio (DoS) y el uso no autorizado de servicios como la retransmisión de correo electrónico.

- **Nivel 2 (gravedad media),** exponen cierta información sensible del host, como las versiones precisas de los servicios. Con esto, los hackers podrían investigar posibles ataques contra un host
- **Nivel 1 (Vulnerabilidad de baja gravedad)**, expone información, como puertos abiertos.