

## **Servicios de seguridad gestionados IBM (Cloud Computing) – Hosted Vulnerability Management**

# Índice

<b>1. Alcance de los servicios</b> .....	3
<b>2. Definiciones</b> .....	3
<b>3. Servicios</b> .....	4
3.1 Centros de operaciones de seguridad .....	5
3.2 Portal.....	5
3.2.1 Responsabilidades del Portal de IBM .....	5
3.2.2 Sus responsabilidades de Portal.....	5
3.3 Contactos de servicios.....	5
3.3.1 Responsabilidades de contactos de servicios de IBM.....	6
3.3.2 Sus Responsabilidades de contactos de servicios .....	6
3.4 Inteligencia de seguridad.....	8
3.4.1 Responsabilidades de inteligencia de seguridad de IBM .....	8
3.4.2 Sus Responsabilidades de inteligencia de seguridad .....	8
3.5 Implementación y activación.....	10
3.5.1 Responsabilidades de Implementación y activación de IBM .....	10
3.5.2 Sus Responsabilidades de Implementación y activación .....	12
3.6 Recopilación y Archivado.....	14
3.6.1 Responsabilidades de Recopilación y Archivado de IBM .....	14
3.6.2 Sus Responsabilidades de Recopilación y Archivado.....	14
3.7 Salud del agente gestionado y Monitoreo de disponibilidad .....	15
3.7.1 Responsabilidades de IBM por el estado del agente gestionado y el Monitoreo de disponibilidad .....	15
3.7.2 Sus Responsabilidades por el estado del agente gestionado y el Monitoreo de disponibilidad .....	16
3.8 Gestión de agentes.....	16
3.8.1 Responsabilidades de gestión de agentes de IBM .....	16
3.8.2 Sus Responsabilidades de gestión de agentes.....	16
3.9 Informes de servicios .....	17
3.9.1 Responsabilidades de informes de servicios de IBM .....	17
3.9.2 Sus Responsabilidades de informes de servicios .....	17
<b>4. Servicios opcionales</b> .....	17
4.1 Acceso fuera de banda .....	17
4.1.1 Responsabilidad de acceso fuera de banda de IBM .....	17
4.1.2 Su Responsabilidad de acceso fuera de banda .....	17
4.2 Servicios de proveedores de análisis aprobados por PCI.....	18
4.2.1 Responsabilidades del Proveedor de análisis aprobado por IBM PCI.....	18
4.2.2 Sus Responsabilidades del Proveedor de análisis aprobado por PCI .....	18
<b>5. Contratos de nivel de servicio</b> .....	20
5.1 Disponibilidad de SLA .....	20
5.2 Recursos de SLA .....	20
<b>6. Otros Términos y Condiciones</b> .....	21
6.1 General.....	21
6.2 Permiso para realizar pruebas .....	21
6.3 Sistemas de terceros.....	21
6.4 Aviso.....	22
6.5 Convenios de la Industria de tarjetas de crédito.....	22

## Descripción de servicios

### Servicios de seguridad gestionados IBM (Cloud Computing) – Hosted Vulnerability Management

ADEMÁS DE LOS TÉRMINOS Y CONDICIONES ESPECIFICADOS A CONTINUACIÓN, ESTA DESCRIPCIÓN DE SERVICIOS INCLUYE LAS “DISPOSICIONES GENERALES DE SERVICIOS DE SEGURIDAD GESTIONADOS POR IBM” (“DISPOSICIONES GENERALES”) PRESENTES EN [http://www-935.ibm.com/services/us/iss/html/contracts\\_worldwide\\_landing.html](http://www-935.ibm.com/services/us/iss/html/contracts_worldwide_landing.html) E INCORPORADAS EN EL PRESENTE POR REFERENCIA.

#### 1. Alcance de los servicios

Los Servicios de seguridad gestionados IBM (Cloud Computing) – Hosted Vulnerability Management (denominado “VMS” o “Servicios”) son un servicio de análisis de vulnerabilidades diseñado para brindarle las herramientas necesarias para cumplir con un conjunto de necesidades (como ser soporte para su evaluación interna de auditoría y riesgos, cumplimiento con las normas, y requisitos de cumplimiento con la industria). VMS incluye un conjunto amplio de funcionalidad aunque usted debe solicitar específicamente que se configure un ambiente para usted si desea informes certificados de Proveedores de análisis aprobados de la Industria de tarjetas de crédito (“PCI”).

IBM brinda VMS como la solución que usted debe operar. IBM brinda la aplicación de análisis y el soporte técnico para la aplicación; sin embargo, usted es responsable de operar los Servicios y por los resultados logrados por los Servicios.

Las decisiones con respecto a qué vulnerabilidades podrán detectarse por VMS quedan a discreción exclusiva de IBM. Dichas decisiones se basarán en la severidad, preponderancia y capacidad de VMS para detectar con seguridad la vulnerabilidad, y la prioridad de la vulnerabilidad con respecto a las amenazas que se cubren.

VMS se brinda en dos tipos diferenciados de análisis que se pueden emplear juntos o por separado;

- Externo - IBM aloja y gestiona los escáneres de vulnerabilidad en Internet. Dichos escáneres se pueden utilizar para analizar sus direcciones de IP públicas y aplicaciones Web, y están diseñados para detectar la vulnerabilidad de exposiciones a riesgos de seguridad abiertas en Internet.
- Interno – le permite evaluar las vulnerabilidades de seguridad en su red de empresas, utilizando un dispositivo de análisis gestionado por IBM en las instalaciones (denominado “Agente”). Dichos Agentes no deben usarse para ningún otro propósito mientras estén gestionados por IBM.

Las funciones de los servicios descritas en el presente dependen de la disponibilidad y soporte de productos y funciones de productos que se utilizan. Aún en el caso de productos soportados, puede que no todas las funciones sean soportadas. IBM hace disponible la información de funciones soportadas a pedido. Esto incluye tanto el hardware, software y firmware brindados por IBM como los no brindados.

#### 2. Definiciones

**Condición de alerta (“AlertCon”)** – métrica de riesgo global desarrollada por IBM, mediante métodos exclusivos. La AlertCon se basa en una variedad de factores, incluida la cantidad y severidad de vulnerabilidades conocidas, las formas de aprovechar dichas vulnerabilidades, la disponibilidad de dichas formas al público, la actividad de gusanos de propagación en masa, y la actividad de amenazas globales. Los cuatro niveles de AlertCon se describen en el portal de Servicios de seguridad gestionados por IBM (“IBM MSS”) (denominado “Portal”).

**Proveedor de análisis aprobado (“ASV”)** – proveedor de soluciones de análisis de vulnerabilidad, aprobado por el PCI SSC. Dichos ASV brindan servicios a organizaciones sujetas a los estándares de seguridad de datos de la Industria de tarjetas de crédito (“PCI”).

**Materiales educativos** – incluyen, entre otros, manuales de laboratorio, notas de instructores, literatura, metodologías, curso electrónico e imágenes de caso de estudio, políticas y procedimientos, además de cualquier propiedad relacionada con la capacitación creada por o en nombre de IBM. De aplicarse, los materiales educativos pueden incluir manuales de participantes, documentos de ejercicio, documentos de laboratorio y diapositivas de presentación provistas por IBM.

**Escaneo de vulnerabilidad interna** – análisis de vulnerabilidad que se originan desde un analizador de

IBM ubicado fuera de su ambiente físico. Los análisis externos estimulan el punto de vista de una amenaza externa (por ejemplo, un pirata informático que accede a su ambiente desde la Internet pública). **Análisis de vulnerabilidad interna**- análisis de vulnerabilidad que se originan desde un dispositivo de análisis ubicado en sus instalaciones. Los análisis internos pueden brindar un análisis más completo de las máquinas de destino evitando interferencia de análisis por firewalls y otros dispositivos de seguridad. **Consejo de estándares de seguridad de la Industria de tarjetas de crédito (“PCI SSC”)**– organización responsable de definir los estándares de seguridad de datos para organizaciones que manejan datos de tarjetas de crédito.

### 3. Servicios

La siguiente tabla resalta las funciones de Servicios mensurables. Las secciones siguientes brindan descripciones narrativas de cada función de Servicios.

#### Resumen de funciones de servicios

Services Feature	Metric or Qty	Service Level Agreements
Disponibilidad de Servicios	100%	SLA de disponibilidad de Servicios
Disponibilidad del Portal IBM MSS	99.9%	Disponibilidad del Portal IBM MSS
Contactos de seguridad autorizados	3 usuarios	N/A
Alerta de salud del agente	15 minutos	SLA de monitoreo del sistema proactivo
Cantidad/frecuencia de análisis externo/interno	Ilimitada	N/A
Implementación de análisis de vulnerabilidad	+/- 1 hora	SLA de implementación de análisis
Características de los servicios PCI ASV	Métrica or Cantidad	Contratos de nivel de servicio
Pedido de cambio del alcance de PCI	Unlimited	N/A
Reconocimiento del pedido de cambio del alcance de PCI	2 hours	SLA de reconocimiento del pedido de cambio del alcance de PCI
Implementación del pedido de cambio del alcance de PCI	72 hours	SLA de implementación del pedido de cambio del alcance de PCI
Pedido de revisión de la excepción de vulnerabilidad de PCI	Unlimited	N/A
Respuesta al pedido de revisión de la excepción de vulnerabilidad de PCI	72 hours	SLA del pedido de revisión de la excepción de PCI
Atestación de PCI ASV	One per quarter	N/A

### 3.1 Centros de operaciones de seguridad

Los Servicios de seguridad gestionados por IBM se entregan desde una red de Centros de operaciones de seguridad de IBM ("SOCs"). IBM brindará acceso a los SOC 24 horas al día, 7 días a la semana.

### 3.2 Portal

El Portal le brinda acceso a un ambiente (y herramientas asociadas) diseñado para monitorear y gestionar su postura de seguridad fusionando datos de servicio y tecnología de proveedores y geografías múltiples en una interfaz común basada en la Web.

El Portal también se puede utilizar para entregar Materiales educativos. Dichos Materiales educativos son licenciados, no vendidos y permanecen como propiedad exclusiva de IBM. IBM le entrega una licencia de conformidad con los términos brindados en el Portal. LOS MATERIALES EDUCATIVOS SE BRINDAN "COMO SE ENCUENTRAN" Y SIN GARANTÍA NI INDEMNIZACIÓN DE NINGÚN TIPO POR PARTE DE IBM, YA SEA EXPRESA O IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR Y NO VIOLACIÓN DE DERECHOS PRIVADOS Y DE PROPIEDAD INTELECTUAL

#### 3.2.1 Responsabilidades del Portal de IBM

IBM:

- a. brindará acceso al Portal 24 horas al día, 7 días a la semana. El Portal brindará:
  - (1) Planillas de análisis por defecto y planillas de informes;
  - (2) conciencia y alerta de inteligencia de seguridad;
  - (3) información sobre el ticket de servicios;
  - (4) Iniciación y actualizaciones de tiquetes y flujo de trabajo;
  - (5) conversación en línea y colaboración con analistas de SOC;
  - (6) un panel de informes de planillas;
  - (7) Acceso a resultados de análisis;
  - (8) autorización para descargar datos; y
  - (9) acceso a Materiales educativos de acuerdo con los términos provistos por el Portal; y
- b. disponibilidad del portal de conformidad con las métricas provistas en la sección de esta Descripción de servicios titulada "Contratos de nivel de servicios", "Disponibilidad de Portal".

#### 3.2.2 Sus responsabilidades de Portal

Usted acuerda:

- a. usar el Portal para realizar actividades de Servicios operacionales diarias;
- b. asegurarse de que los empleados que acceden al Portal en su nombre cumplan con los Términos de uso del presente incluidos, entre otros, los términos asociados con los Materiales educativos y otros artículos para entregar, como los informes de análisis y resumen;
- c. guardar adecuadamente las credenciales de inicio de sesión al Portal (incluida la no divulgación de dichas credenciales a toda persona no autorizada);
- d. notificar inmediatamente a IBM si se sospecha que sus credenciales de inicio de sesión han sido comprometidas; e
- e. indemnizar y eximir a IBM de toda pérdida en la que usted u otras partes hayan incurrido como resultado de no haber guardado sus credenciales de inicio de sesión.

### 3.3 Contactos de servicios

Puede elegir de entre niveles múltiples de acceso a los SOC y el Portal para acomodarse a los diferentes roles dentro de su organización.

#### **Contactos de seguridad autorizados**

Un Contacto de seguridad autorizado se define como un tomador de decisiones en todos los asuntos operacionales pertenecientes a los Servicios de seguridad gestionados por IBM.

#### **Contactos de servicios designados**

Un contacto de servicios designado se define como un tomador de decisiones en un subgrupo de cuestiones operacionales que pertenecen a los Servicios de seguridad gestionados por IBM, un Agente, o grupo de Agentes. IBM sólo se relacionará con un Contacto de servicios designado con respecto a las actividades operacionales dentro del subgrupo por el que dicho contacto es responsable (por ejemplo, contacto de interrupción de Agente).

#### **Usuarios del Portal**

IBM brinda niveles múltiples de acceso para usuarios del Portal. Estos niveles de acceso se pueden

aplicar a un Servicio de seguridad gestionado por IBM, un Agente o grupo de Agentes. Los usuarios del Portal estarán autenticados vía la tecnología de codificación de contraseña estática o clave pública que usted provea (por ejemplo, muestra de ID segura de RSA) basada en sus requisitos.

### **3.3.1 Responsabilidades de contactos de servicios de IBM**

#### **Contactos de seguridad autorizados**

IBM:

- a. le permitirá crear hasta tres Contactos de seguridad autorizados;
- b. brindará a cada Contacto de seguridad autorizado:
  - (1) permisos de Portal administrativo a sus Agentes;
  - (2) la autorización de crear Contactos de servicios designados ilimitados y usuarios de Portal;
  - (3) la autorización para delegar responsabilidad a Contactos de servicios designados;
- c. se relacionará con Contactos de seguridad autorizados con respecto a asuntos de soporte y notificación que pertenecen a los Servicios; y
- d. verificará la identidad de Contactos de seguridad autorizados mediante un método de autenticación que usa una frase de acceso de desafío precompartida.

#### **Contactos de servicios designados**

IBM:

- a. verificará la identidad de Contactos de servicios designados mediante un método de autenticación que usa una frase de acceso de desafío precompartida.
- b. Se relacionará únicamente con Contactos de servicios designados con respecto al subgrupo de cuestiones operacionales por las que dicho contacto es responsable.

#### **Usuarios del Portal**

IBM:

- a. brindará acceso al Portal con capacidades que pueden incluir (según corresponda):
  - (1) Envío de solicitudes de servicios a los SOC;
  - (2) Comunicación con “chat en línea” que se comunica con analistas de SOC con respecto a incidentes específicos o tiquetes, generados como parte de los Servicios;
  - (3) Creación de tiquetes relacionados con servicios internos y asignación de dichos tiquetes a usuarios de Portal;
  - (4) análisis, visualizaciones y actualización de tiquetes relacionados con Servicios;
  - (5) Creación y modificación de planillas de análisis personalizado (excepto planillas PCI);
  - (6) creación y modificación de planillas de informes personalizados (excepto informes PCI);
  - (7) Envío de pedidos de excepción de vulnerabilidad;
  - (8) Revisión y aprobación de excepciones de vulnerabilidad (excepto las excepciones PCI);
  - (9) Definición de sitios de análisis (direcciones IP y dominios Web a incluirse en el alcance del análisis) junto con los usuarios y políticas relacionados con el sitio (excepto el alcance PCI);
  - (10) programación y ejecución de análisis;
  - (11) programación y ejecución de informes;
- b. Autenticará a usuarios del Portal que usen contraseña estática; y
- c. Autenticará a usuarios de Portal con una tecnología de codificado de clave pública que usted brinde (por ejemplo, muestra de ID seguro de RSA) según sus requisitos.

### **3.3.2 Sus Responsabilidades de contactos de servicios**

#### **Contactos de seguridad autorizados**

Usted acuerda:

- a. Brindarle a IBM información de contacto para cada Contacto de seguridad autorizado. Dichos Contactos de seguridad autorizados serán responsables de:
  - (1) crear Contactos de servicios designados y delegar responsabilidades y permisos a dichos contactos, según corresponda;

- (2) crear usuarios de Portal;
  - (3) autenticar con los SOC mediante una frase de acceso de desafío precompartida; y
  - (4) mantener rutas de notificación junto con su información de contacto, y brindar dicha información a IBM;
- b. Asegurar al menos un Contacto de seguridad autorizado disponible 24 horas al día, 7 días a la semana;
- c. Actualizar a IBM en un lapso de tres días calendario cuando se modifica su información de contacto; y
- d. y reconocer que usted no puede contar con más de tres Contactos de seguridad autorizados más allá de la cantidad de servicios de IBM o suscripciones de Agente que contrató.

**Contactos de servicios designados**

Usted acuerda:

- a. brindar a IBM información de contacto y responsabilidad de roles por cada Contacto de servicios designado. Dichos Contactos de servicios designados serán responsables de autenticar con los SOC mediante una frase de acceso; y
- b. reconocer que un Contacto de servicios designado puede tener que estar disponible 24 horas al día, 7 días a la semana según un subgrupo de responsabilidades por las que debe responder (es decir, parada de Agente).

### **Usuarios del Portal**

Usted acuerda:

- a. Que los usuarios del Portal usarán el Portal para realizar actividades diarias de servicios operacionales;
- b. ser responsable de brindar muestras de ID seguro de RSA soportadas por IBM (según corresponda); y
- c. reconocer que los SOC solo se relacionarán con Contactos de seguridad autorizados y Contactos de servicios designados.

### **3.4 Inteligencia de seguridad**

El Centro de análisis de amenazas de IBM X-Force® se encarga de la inteligencia de seguridad. El Centro de análisis de amenazas de X-Force publica un nivel de amenazas de AlertCon en Internet. La AlertCon describe posiciones de alerta progresiva de condiciones actuales de amenaza de seguridad en Internet. Si las condiciones de amenaza a la seguridad en Internet se elevan a AlertCon 3, indicando ataques específicos que requieren de la acción defensiva inmediata, IBM le brindará acceso en tiempo real a los informes de situación global de IBM. Como usuario del Portal, tiene acceso al Servicio de análisis de amenazas alojado por X-Force. El Servicio de análisis de amenazas alojado por X-Force incluye acceso al Boletín trimestral de información de amenazas de IBM X-Force ("IQ de amenazas").

Mediante el Portal, puede crear una lista de observación de vulnerabilidades con información de amenazas personalizadas. Asimismo, cada usuario del Portal puede solicitar un e-mail de evaluación por Internet cada día hábil. Esta evaluación brinda un análisis de las condiciones actuales de amenazas conocidas de Internet, datos de métricas de puertos en Internet en tiempo real, además de noticias sobre alertas individualizadas, recomendaciones y seguridad.

Nota: Su acceso y uso de la Inteligencia de seguridad brindada vía el Portal (incluidas las IQ de amenazas y el e-mail de evaluación diaria de Internet) quedan sujetos a los Términos de uso del presente. Si dichos Términos de uso entraren en conflicto con los términos de esta Descripción de servicios o cualquier documento contractual relacionado, prevalecerán los Términos de uso del portal. Además de los Términos de uso brindados en el Portal, su uso de cualquier información en cualquier link o sitio Web no perteneciente a IBM y recursos queda sujeto a los términos de uso publicados en sitios Web no pertenecientes a IBM, y recursos.

#### **3.4.1 Responsabilidades de inteligencia de seguridad de IBM**

IBM:

- a. le brindará acceso al Servicio de análisis de amenazas alojado por X-Force;
- b. le brindará un nombre de usuario, contraseña, URL y permisos para acceder al Portal;
- c. desplegará información de seguridad en el Portal a medida que se hace disponible;
- d. si lo configura usted, brindará inteligencia de seguridad específica a su lista de observación de vulnerabilidad, vía el Portal;
- e. si lo configura usted, envíe un e-mail de evaluación de seguridad en Internet cada día hábil;
- f. publicará una AlertCon en Internet vía el Portal;
- g. declarará una emergencia de Internet si el nivel de AlertCon diario llega a AlertCon 3. En dicho evento, IBM le brindará acceso en tiempo real a la información de situación global de IBM;
- h. brindará funcionalidad de características del Portal para que cree y mantenga una lista de observación de vulnerabilidades;
- I. brindará información adicional de alerta, recomendación o cualquier otro asunto de seguridad significativo según lo considere necesario IBM; y
- j. brindará acceso a la IQ de Amenazas vía el Portal.

#### **3.4.2 Sus Responsabilidades de inteligencia de seguridad**

Acuerda usar el Portal para:

- a. suscribirse al e-mail diario de evaluación de seguridad en Internet, si lo desea;

b. crear una lista de observación de vulnerabilidades, si lo desea; y

- c. acceder a la IQ de amenazas; y
- d. acordar adherirse al contrato de licencias y no enviar información de servicios a individuos que no cuenten con una licencia adecuada.

### **3.5 Implementación y activación**

Durante la implementación y activación, IBM trabajará con usted para configurar los Servicios y, si corresponde, implementar agentes de análisis interno.

Nota: Las actividades de implementación y activación se realizan una vez durante la realización de los servicios. Si decide reemplazar, actualizar o mover a su o sus Agentes durante el contrato de servicios, IBM puede solicitar que dicho o dichos Agentes sean reimplementados o reactivados (denominado "Reimplementación"). Dichas reimplementaciones se brindarán a un costo adicional según lo especificado en el Programa. Los costos de reimplementación se aplican solamente a reemplazos de hardware, actualizaciones o movimientos que usted inicie. Dichos cargos no se aplican a fallas de Agentes que resulten en actividades de Autorización de devolución de materiales al agente ("RMA").

#### **3.5.1 Responsabilidades de Implementación y activación de IBM**

##### **Actividad 1 – Arranque del proyecto**

El propósito de esta actividad es realizar una llamada de comienzo del proyecto, de aplicarse. IBM le enviará un e-mail de bienvenida y (de corresponder) realizará una llamada de inicio, durante hasta una hora por hasta tres miembros de su personal, para:

- a. presentar su Punto de contacto al especialista de implementación asignado por IBM;
- b. revisar las respectivas responsabilidades de cada parte;
- c. establecer expectativas de programación; y
- d. comenzar la evaluación de sus requisitos y ambiente.

##### ***Crterios de finalización;***

Esta actividad estará completa cuando IBM haya realizado la llamada de Arranque del proyecto.

##### ***Materiales entregables:***

- Ninguno

##### **Actividad 2 – Requisitos de hardware de agentes de análisis interno**

El propósito de esta actividad es establecer requisitos de hardware para el o los motores de análisis internos que se ubicarán en sus instalaciones.

IBM:

- a. le presentará un documento denominado "Instrucciones de instalación del analizador de vulnerabilidad en las instalaciones del cliente ("CPE")", el cual detalla:
  - (1) especificaciones de hardware que debe brindar; y
  - (2) los pasos que debe tomar para configurar e instalar los motores de análisis interno para usar con los Servicios;
- b. brindarle acceso a la imagen de software que incluye al sistema operativo y software de análisis para aplicar al hardware que usted brinda.

##### ***Crterios de finalización;***

Esta actividad estará completa cuando IBM le haya entregado a su Punto de contacto las Instrucciones de instalación del analizador de vulnerabilidad de las instalaciones del cliente ("CPE").

##### ***Materiales entregables:***

- Instrucciones de instalación del analizador de vulnerabilidad en las instalaciones del cliente ("CPE")

##### **Actividad 3 – Requisitos de acceso a la red para Análisis interno**

El propósito de esta actividad es establecer los requisitos de acceso a la red.

IBM:

- a. le brindará un documento denominado "Requisitos de acceso a la red", detallando:
  - (1) Cómo se conectará IBM de manera remota a la red;
  - (2) Requisitos técnicos específicos para permitir dicha conectividad remota;

Nota: IBM podrá realizar cambios al documento de "Requisitos de acceso a la red", según lo considere apropiado, en toda la realización de los Servicios.

- b. se conectará a su red por medio de Internet, usando métodos de acceso estándar de IBM; y
- c. de ser apropiado, usará una red privada virtual de sitio a sitio ("VPN") para conectarse a su red. IBM brindará dicho VPN a un costo adicional según lo especificado en el Programa.

***Crterios de finalizaci3n;***

Esta actividad estar3 completa cuando IBM haya brindado su Punto de contacto con el documento de Requisitos de acceso a la red.

***Materiales entregables:***

- Documento de Requisitos de acceso a la red

**Actividad 4 - Evaluaci3n**

El prop3sito de esta actividad es realizar una evaluaci3n de su ambiente actual, adem3s de metas comerciales y tecnol3gicas, y (de aplicarse) permitir el desarrollo de la estrategia de seguridad requerida para la implementaci3n y el uso de uno o m3s Agentes de an3lisis interno.

***Tarea 1 – Recopilaci3n de datos***

IBM:

- a. le brindar3 un Punto de Contacto con un formulario de recopilaci3n de datos en el que deber3 documentar art3culos tales como:
  - (1) Nombres de miembros del equipo, informaci3n de contacto, roles y responsabilidades;
  - (2) Requisitos 3nicos para pa3ses y sitios;
  - (3) cantidad y tipo de usuario finales;
  - (4) Impulsores y/o dependencias comerciales clave que podr3an influir en la entrega o los plazos de los Servicios; y
  - (5) Direcciones y dominios de PCI IP sujetos a PCI (de aplicarse).

***Tarea 2 – Ambiente de evaluaci3n para An3lisis interno***

IBM:

- a. usar3 la informaci3n brindada en el formulario de recopilaci3n de datos para evaluar su ambiente existente;
- b. determinar3 una 3ptima ubicaci3n de agentes; y
- c. de corresponder, brindar3 recomendaciones para ajustar la disposici3n de la red y las pol3ticas de seguridad para permitir el an3lisis de los objetivos deseados.

***Crterios de finalizaci3n;***

Esta actividad se ver3 completa cuando IBM haya completado la evaluaci3n de su ambiente.

***Materiales entregables:***

- Ninguno

**Actividad 5 – Implementaci3n de An3lisis interno**

El prop3sito de esta actividad es implementar el o los Agentes.

***Tarea 1 – Configurar al Agente***

IBM:

- a. evaluar3 en forma remota al o los Agentes para verificar que cumplan con las especificaciones de IBM;
- b. identificar3 al hardware del Agente que no cumple con los niveles actuales soportados por IBM; y
- c. brindar3 soporte telef3nico en l3nea para asistirlo al cargar la imagen del software y configurar al Agente con una direcci3n de IP p3blica y configuraciones relacionadas. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementaci3n de IBM.

***Tarea 2 – Instalar al Agente***

IBM:

- a. brindará soporte en línea, por teléfono y/o e-mail, para asistirlo en ubicar documentos de proveedores aplicables que detallan los procedimientos de instalación y cableado físicos. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- b. brindará recomendaciones para ajustar la disposición de la red para mejorar la seguridad (de aplicarse); y
- c. configurará al Agente de manera remota, incluido el registro del Agente con la infraestructura de IBM MSS.

Nota: Puede contratar por separado para que IBM brinde servicios de instalación física.

***Crterios de finalización;***

Esta actividad estará completa cuando el Agente esté registrado con la infraestructura de IBM MSS.

***Materiales entregables:***

- Ninguno

**Actividad 6 – Pruebas y verificación**

El propósito de esta actividad es realizar las pruebas y verificación de los Servicios.

IBM:

- a. para cada agente
  - (1) verificará la conectividad de los Agentes con la infraestructura de IBM MSS;
  - (2) verificará la entrega de datos de análisis de los Agentes con la infraestructura de IBM MSS;
  - (3) verificará la disponibilidad y funcionalidad del Agente en el Portal;
  - (4) realizará pruebas de garantía de calidad del Agente;
- b. realizará pruebas de aceptación de Servicios;
- c. demostrará en forma remota las principales funciones del Portal por hasta diez miembros de su personal, por hasta una hora.

***Crterios de finalización;***

Esta actividad estará completa cuando IBM haya verificado la disponibilidad y funcionalidad del Agente en el Portal.

***Materiales entregables:***

- Ninguno

**Actividad 7 – Activación de servicios**

El propósito de esta actividad es activar los Servicios. IBM:

- a. asumirá la gestión y soporte del o los Agentes;
- b. configurará a los Agentes en “activo”;
- c. trasladará a los Agentes a los SOC para gestión y soporte continuos.

***Crterios de finalización;***

Esta actividad estará completa cuando se activen los Servicios y los Agentes estén configurados en “activo”.

***Materiales entregables:***

- Ninguno

### **3.5.2 Sus Responsabilidades de Implementación y activación**

**Actividad 1 – Arranque del proyecto**

Usted acuerda:

- a. atender la llamada de Arranque del proyecto; y
- b. revisar las respectivas responsabilidades de cada parte.

**Actividad 2 – Requisitos de hardware de agentes del analizador interno**

Usted acuerda:

- a. brindar hardware del servidor de conformidad con los requisitos del sistema presentes en las Instrucciones de configuración del analizador de vulnerabilidad de las Instalaciones del cliente ("CPE") para cualquier instalación para la que solicita análisis interno;
- b. y reconocer que todo el hardware que brinda, que no cumpla con los requisitos de sistema brindados por IBM, puede resultar en una falla de instalación u operación del paquete de software;
- c. seguir las instrucciones de instalación provistas para cargar y configurar la imagen de software del motor de análisis interno; y
- d. asegurarse de que se haya cubierto todo el hardware provisto bajo un contrato de servicios activo por la duración de los Servicios.

### **Actividad 3 – Requisitos de acceso a la red para Análisis interno**

Usted acuerda:

- a. revisar y cumplir con el documento de "Requisitos de acceso a la red" de IBM durante la implementación y todo el término del contrato; y
- b. ser responsable único por cualquier costo incurrido como resultado del uso por IBM de una VPN de sitio a sitio para conectarse a su red.

### **Actividad 4 - Evaluación**

#### ***Tarea 1 – Recopilación de datos***

Usted acuerda:

- a. completar y devolver cuestionarios y/o formularios de recopilación de datos a IBM en un plazo de cinco días de su recepción;
- b. obtener y brindar información, datos, consentimientos, decisiones y aprobaciones aplicables según los requisitos de IBM para la implementación de Servicios, en un plazo de dos días hábiles desde el pedido de IBM;
- c. trabajar de buena fe con IBM para evaluar de manera precisa su ambiente de red;
- d. brindar contactos dentro de su organización, y especificar una ruta de notificación en su organización, en caso de que IBM deba contactarlo; y
- e. actualizar a IBM en un lapso de tres días calendario cuando se modifica su información de contacto.

#### ***Tarea 2 – Ambiente de evaluación para Análisis interno***

Usted acuerda:

- a. implementar los cambios solicitados en la disposición de su red y las políticas de seguridad para permitir el análisis de objetivos de análisis deseados; y
- b. situar a los Agentes de análisis en su red para que puedan llegar a los dispositivos de destino de tal forma que los firewalls y otros dispositivos de seguridad no interfieran con los análisis.

### **Actividad 5 – Implementación de Análisis interno**

#### ***Tarea 1 – Configurar al Agente***

Usted acuerda:

- a. actualizar su hardware para cumplir con las especificaciones de IBM;
- b. descargar e instalar la imagen de software del Agente brindado por IBM (es decir, medios de carga física, según corresponda);
- c. configurar al Agente con una dirección de IP pública y configuraciones relacionadas; y
- d. asistir a IBM en cumplir con la configuración y política del Agente existente (de aplicarse).

#### ***Tarea 2 – Instalar al Agente***

Usted acuerda:

- a. trabajar junto con IBM en localizar documentos de proveedores que detallen procedimientos de instalación y cableado físicos. Deberá programar dicho respaldo por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- b. ser responsable del cableado y la instalación físicos del o los Agentes;
- c. realizar cualquier ajuste especificado por IBM a la disposición de su red y las políticas de seguridad para permitir el análisis de los objetivos de análisis deseados; y

- d. situar a los Agentes de análisis en su red para que puedan llegar a los dispositivos de destino y no permitan que los firewalls y otros dispositivos de seguridad interfieran con los análisis.

### **Actividad 6 – Pruebas y verificación**

Usted acuerda:

- a. ser responsable por el desarrollo de todos sus planes de pruebas de aceptación específicos;
- b. ser responsable de realizar pruebas de aceptación de sus aplicaciones y la conectividad de red; y
- c. reconocer que las pruebas de aceptación adicionales realizadas por usted, o la falta de ellas, no impide que IBM configure al Agente en “activo” en los SOC para soporte y gestión continuos.

### **Actividad 7 – Activación de servicios**

Usted reconoce:

- a. que usará los Servicios para analizar solamente las direcciones de IP y/o los dominios Web que usted posea o tenga autoridad legal para analizar; y
- b. que para obtener resultados de análisis completos y precisos, debe configurar y mantener su topología de red y dispositivos de seguridad para permitir un tráfico de análisis sin filtros de sus motores de análisis a sus objetivos de análisis seleccionados.

## **3.6 Recopilación y Archivado**

IBM utiliza el Sistema de protección de X-Force para recopilar, organizar, archivar y recuperar datos e informes de análisis de los Servicios. El Portal le brinda una visualización de los Servicios las 24 horas del día, los 7 días de la semana, incluido el acceso en línea al historial de análisis y los informes almacenados dentro de la infraestructura del Sistema de Protección X-Force.

### **3.6.1 Responsabilidades de Recopilación y Archivado de IBM**

IBM:

- a. recopilará datos de análisis generados por el o los Agentes cuando dichos datos lleguen a la infraestructura de IBM MSS;
- b. recopilará datos de análisis generados por la infraestructura de análisis externo de IBM;
- c. depurará los logs de análisis temporarios generados por los Agentes y analizadores externos después de importar los resultados de los análisis a la base de datos del Sistema de Protección X-Force;
- d. de aplicarse, disponga de los resultados de análisis individuales de PCI para ver en el Portal por dos años;
- e. disponga de resultados de análisis individuales que no sean de PCI para ver en el Portal por seis meses;
- f. en el caso de análisis individuales que no pertenezcan a PCI, una vez vencido el período inicial de seis meses, disponga de resultados resumidos de análisis por 18 meses; y
- g. depure datos según los períodos de retención descritos anteriormente.

### **3.6.2 Sus Responsabilidades de Recopilación y Archivado**

Usted acuerda:

- a. y reconocer que:
  - (1) IBM depurará logs de análisis temporal y resultados de análisis individuales de conformidad con los marcos de tiempo declarados en la sección “Responsabilidades de recopilación y archivado de IBM” anterior;
  - (2) Sin tener en cuenta los períodos de retención especificados en la sección “Responsabilidades de recopilación y archivado de IBM” anterior, si se rescinden o cancelan los Servicios por cualquier motivo, IBM quedará eximida de su obligación de almacenar sus datos de Servicios;
  - (3) todos los datos de análisis se transmitirán a los SOC por Internet;
  - (4) IBM solo puede recopilar y analizar datos que lleguen con éxito a la infraestructura de IBM MSS; y
  - (5) IBM no garantiza el envío legal de ningún dato de Servicio en ningún sistema legal local o internacional. La admisión de evidencia se basa en las tecnologías presentes y su capacidad de probar el manejo adecuado de datos y la cadena de custodia para cada grupo de datos presentado; y
- b. usar el Portal para revisar los resultados de análisis.

### 3.7 Salud del agente gestionado y Monitoreo de disponibilidad

IBM monitoreará el estado de salud y la disponibilidad de los escáneres internos. Dicho monitoreo está diseñado para asistir en la cada vez mayor disponibilidad y tiempo de actividad de los Agentes.

Según la cantidad de direcciones de IP del contrato activo de Servicios VMS, IBM monitoreará una cantidad específica de Agentes según la siguiente tabla.

Direcciones de IP		Cantidad de dispositivos permitidos
De	A	
1	199	2
200	999	6
1.000	2.999	12
3.000	29.999	16
30.000+ IPs		Una cada 2.000 IPs

Usted reconoce que si necesita Agentes adicionales, se aplicarán cargos adicionales de monitoreo de Agentes.

#### 3.7.1 Responsabilidades de IBM por el estado del agente gestionado y el Monitoreo de disponibilidad

##### **Actividad 1 - Monitoreo**

El propósito de esta actividad es monitorear el estado y el rendimiento de los Agentes.

##### **Monitoreo basado en Agentes**

IBM instalará software en Agentes para monitorear el estado y el rendimiento de sistemas, y le informará a los SOC las métricas de informes.

IBM:

- a. para plataformas candidatas, instalará software de monitoreo en Agentes;
- b. analizará y responderá a métricas clave, que pueden incluir:
  - (1) Capacidad de disco duro;
  - (2) Utilización de CPU;
  - (3) Utilización de memoria; y
  - (4) Disponibilidad de procesos; y
- c. responderá a alertas generadas por el software de monitoreo.

##### **Actividad 2 – Resolución de problemas**

El propósito de esta actividad es estudiar e investigar si los Agentes no se desempeñan como se esperaba o se identifica un problema de salud del Agente.

IBM:

- a. creará un ticket de problemas si existe un problema de rendimiento del Agente o un posible problema en el estado del Agente;
- b. comenzará estudiando e investigando los problemas documentados;
- c. si se identifica al Agente como posible fuente de un problema relacionado con la red, examinará la configuración y funcionalidad del Agente por posibles problemas; y
- d. desplegará el estado del Agente y el ticket de parada en el Portal.

##### **Actividad 3 - Notificación**

El propósito de esta actividad es notificarlo si el Agente no puede alcanzarse por medios estándares en banda.

IBM:

- a. lo notificará si el Agente no se puede alcanzar por medios estándares en banda. Dicha notificación se realizará por vía telefónica con un procedimiento de notificación predeterminado dentro del marco de tiempo establecido en la sección de esta Descripción de servicios titulada "Contratos de nivel de servicios", "Monitoreo del sistema proactivo";
- b. comenzará la investigación de problemas relacionados con la configuración o funcionalidad del Agente, después de la iniciación de notificación telefónica; y

- c. desplegará el estado del Agente y los tiquetes de parada en el Portal.

### **3.7.2 Sus Responsabilidades por el estado del agente gestionado y el Monitoreo de disponibilidad**

#### **Actividad 1 - Monitoreo**

Para esta actividad no se le requiere ninguna responsabilidad adicional.

#### **Actividad 2 – Resolución de problemas**

Usted acuerda:

- a. participar en las sesiones de resolución de problemas con IBM (según se solicite);
- b. ser responsable por la configuración en forma remota y la resolución de problemas, si decidió no implementar una solución fuera de banda (“OOB”), o si la solución OOB no está disponible por alguna razón; y
- c. reconocer que si se elimina un Agente gestionado como raíz de un problema en particular, IBM no realizará ninguna otra resolución de problemas.

#### **Actividad 3 - Notificación**

Usted acuerda:

- a. proveer sus rutas de notificación e información de contacto;
- b. actualizar a IBM en un lapso de tres días calendario cuando se modifica su información de contacto; y
- c. asegurarse de disponer de un Contacto de seguridad autorizado o un Contacto de servicios designados de parada de Agente, 24 horas al día, 7 días a la semana.

### **3.8 Gestión de agentes**

Las actualizaciones de aplicaciones y seguridad de agentes son componentes fundamentales de una empresa.

#### **3.8.1 Responsabilidades de gestión de agentes de IBM**

IBM:

- a. será el único proveedor de gestión a nivel de software para los Agentes;
- b. conservará información sobre el estado del sistema;
- c. instalará parches y actualizaciones de software para mejorar el rendimiento, permitir una funcionalidad adicional, o resolver un problema de aplicación. IBM no asume responsabilidad alguna, y no brinda garantías con respecto a los parches, actualizaciones o contenido de seguridad de proveedores;
- d. declarará por adelantado una ventana de mantenimiento de actualizaciones de Agentes que puedan necesitar un tiempo de inactividad de la plataforma o de su asistencia para finalizar; y
- e. declarará claramente, en la notificación de la ventana de mantenimiento, los impactos esperados y sus requisitos específicos.

#### **3.8.2 Sus Responsabilidades de gestión de agentes**

Usted acuerda:

- a. realizar actualizaciones especificadas por IBM en el hardware para soportar al software y firmware actuales;
- b. trabajar con IBM para realizar actualizaciones de Agentes (según se requiera);
- c. ser responsable de todos los cargos relacionados con las actualizaciones de hardware;
- d. conservar las licencias actuales y los contratos de soporte y mantenimiento;
- e. asegurarse de que los consentimientos apropiados con sus proveedores sean correctos para permitir que IBM aproveche los contratos de soporte y mantenimiento existentes en su nombre. Si no se llega a dichos contratos, IBM no podrá contactar directamente al proveedor para resolver problemas de soporte; y
- f. reconocer:
  - (1) que todas las actualizaciones se transmiten y aplican por Internet;
  - (2) el viaje de datos en Internet se codifica con algoritmos de cifrado específicos estándares en la industria siempre que sea posible;
  - (3) si no se consiguen los consentimientos del proveedor o se revocan en cualquier momento durante la vigencia del contrato, IBM puede suspender los servicios y/o SLA;

- (4) El no cumplimiento con las actualizaciones de software solicitadas por IBM puede resultar en la suspensión de entrega de servicios y/o SLA; y
- (5) El no cumplimiento con las actualizaciones de hardware solicitadas por IBM puede resultar en la suspensión de entrega de servicios y/o SLA.

### **3.9 Informes de servicios**

Al utilizar el Portal, tendrá acceso a información de Servicios e informes con vistas personalizables de activos y resultados de análisis.

#### **3.9.1 Responsabilidades de informes de servicios de IBM**

IBM le proveerá acceso a capacidades de informes en el Portal, las cuales incluyen:

- a. cantidad de SLA invocados y cumplidos;
- b. cantidad, tipos y resumen de solicitudes/tiquetes de Servicios;
- c. detalles de análisis realizados en diferentes formatos predefinidos y personalizables; y
- d. disposición de informes generados (PDF, CSV, XML, etc.) para que descargue del Portal por un año desde la fecha de creación (dos años para informes PCI).

#### **3.9.2 Sus Responsabilidades de informes de servicios**

Usted acuerda:

- a. generar los informes de Servicios usando el Portal; y
- b. ser responsable de programar los informes (según corresponda).

## **4. Servicios opcionales**

Los servicios opcionales seleccionados por usted, junto con cualquier costo adicional por dichos servicios, se especificará en el Programa.

### **4.1 Acceso fuera de banda**

El acceso OOB es una función muy recomendada que asiste a los SOC si se pierde la conectividad de un Agente. Si se dan dichos problemas de conectividad, los analistas del SOC pueden discar en el módem para verificar si el Agente está funcionando adecuadamente para determinar la fuente de la parada antes de que le llegue a usted.

#### **4.1.1 Responsabilidad de acceso fuera de banda de IBM**

A pedido suyo, sin costo adicional, IBM:

- a. brindará soporte en línea, por teléfono e e-mail, para asistirlo en ubicar documentos de proveedores aplicables que detallan los procedimientos de instalación y cableado físicos;
- b. configurará el dispositivo OOB para acceder a los Agentes gestionados; o
- c. trabajará de buena fe con usted para utilizar una solución OOB existente aprobada por IBM.

#### **4.1.2 Su Responsabilidad de acceso fuera de banda**

Usted acuerda:

- a. brindar nuevas soluciones OOB:
  - (1) adquirir un dispositivo OOB soportado por IBM;
  - (2) instalar y conectar en forma física el dispositivo OOB al Agente;
  - (3) brindar una línea telefónica análoga dedicada para acceder;
  - (4) conectar físicamente el dispositivo OOB a la línea telefónica dedicada y mantener la conexión;
  - (5) ser responsable por todos los costos relacionados con el dispositivo OOB y la línea telefónica; y
  - (6) ser responsable por todos los cargos relacionados con la gestión continua de la solución OOB;
- b. Brindar soluciones OOB existentes:
  - (1) asegurarse de que la solución no permita a IBM acceder a dispositivos no gestionados;
  - (2) asegurarse de que la solución no requiera de la instalación de software especializado;
  - (3) proveerle a IBM las instrucciones detalladas para acceder a Agentes gestionados; y

- (4) ser responsable de todos los aspectos de gestionar la solución OOB;
- c. y reconocer que las soluciones OOB deben estar aprobadas por IBM;
- d. mantener el contrato actual de soporte y mantenimiento para el OOB (según corresponda); y
- e. ser responsable por la configuración en forma remota y la resolución de problemas, si decide no implementar una solución OOB, o si la solución OOB no está disponible por alguna razón

#### **4.2 Servicios de proveedores de análisis aprobados por PCI**

Puede solicitar que IBM actúe como ASV para permitirle enviar informes de análisis certificados por ASV a sus bancos de adquisición o marcas de pago.

##### **4.2.1 Responsabilidades del Proveedor de análisis aprobado por IBM PCI**

A pedido suyo, sin costo adicional, IBM:

- a. establecerá un ambiente separado dentro de VMS para realizar los análisis de PCI;
- b. establecerá, con su aporte, sitios dentro de VMS que definan los componentes de análisis (direcciones IP y/o dominios) que se someterán al análisis de PCI;
- c. realizará, según lo programado por usted, análisis de vulnerabilidad de conformidad con el requisito del Estándar de seguridad de datos de PCI ("DSS") 11.2;
- d. responderá a los requisitos de cambio de alcance de PCI (agregados y eliminaciones al alcance de PCI presentado anteriormente):
  - (1) Aceptando una cantidad ilimitada de requisitos de cambio del alcance de PCI, por medio del Portal;
  - (2) Reconociendo los pedidos de cambio de alcance de PCI por medio del Portal con los marcos de tiempo establecidos en la sección de Descripción de Servicios titulada "Contratos de nivel de servicios", Reconocimiento de solicitudes de cambio del alcance de PCI";
  - (3) Revisando los pedidos de cambio del alcance de PCI para verificar que haya brindado la documentación adecuada para justificar el cambio de alcance;
  - (4) Implementando los cambios del alcance de PCI con los marcos de tiempo establecidos en la sección de Descripción de Servicios titulada "Contratos de nivel de servicios", "Implementación de solicitudes de cambio de alcance de PCI";
- e. responderá a los pedidos de excepción de vulnerabilidad (por ejemplo, sospecha de positivos falsos):
  - (1) Aceptando una cantidad ilimitada de pedidos de excepción de vulnerabilidad enviados por usted por medio del Portal;
  - (2) Revisando los pedidos de excepción para verificar que haya brindado la documentación adecuada para justificar la excepción solicitada;
  - (3) Aprobando o rechazando pedidos de excepción de vulnerabilidad, a discreción exclusiva de IBM, dentro de los marcos de tiempo establecidos en la sección de esta Descripción de servicios titulada "Contratos de nivel de servicios", "Respuesta al pedido de excepción de vulnerabilidad de PCI";
- f. llevará a cabo la Atestación de informes de análisis ASV de la carátula de Cumplimiento de análisis y los informes de análisis que debe enviar a bancos de adquisición o marcas de pago; y
- g. retendrá informes de análisis y documentos de trabajo relacionados, de conformidad con los Requisitos de validación para Proveedores de análisis aprobados.

Nota: Su acceso y uso de los informes brindados por medio del Portal también quedan sujetos a los Términos de uso del presente. Si dichos Términos de uso entraren en conflicto con los términos de esta Descripción de servicios o cualquier documento contractual relacionado, prevalecerán los Términos de uso del portal por sobre los de esta Descripción de servicios. Además de los Términos de uso brindados en el Portal, su uso de cualquier información en cualquier link o sitio Web no perteneciente a IBM y recursos queda sujeto a los términos de uso publicados en sitios Web no pertenecientes a IBM, y recursos.

##### **4.2.2 Sus Responsabilidades del Proveedor de análisis aprobado por PCI**

Usted acuerda:

- a. identificar a los usuarios del Portal autorizados para usar el ambiente de PCI dentro de VMS;
- b. definir el alcance del análisis de vulnerabilidad externa, el cual incluye:
  - (1) brindarle a IBM las direcciones de IP y/o nombres de dominio de todos los sistemas de Internet;

- (2) solicitar cualquier cambio en el alcance de PCI por medio del Portal y brindar una justificación completa y precisa para dichos cambios en el alcance;
- (3) implementar una adecuada segmentación de red para toda dirección excluida de IP externa;
- c. ser responsable de asegurarse de contar con la autoridad legal para analizar direcciones de IP y/o dominios Web en el alcance solicitado de PCI;
- d. y reconocer que es responsable exclusivo de que el alcance para los análisis de PCI sea preciso y completo (es decir, las direcciones de IP y/o dominios Web);
- e. asegurarse de que los dispositivos no interfieran con el análisis ASV, incluida:
  - (1) La configuración de sistemas de detección de intrusos (IDSs), sistemas de prevención de intrusos (IPSs) y otros dispositivos para que no interfieran con el análisis (es decir, permitir un acceso sin filtros a la red para sistemas de destino desde los motores de análisis interno de IBM);
  - (2) La coordinación con IBM si cuenta con nivelador de carga en uso;
- f. si se están utilizando los niveladores de carga, brindar:
  - (1) garantía documentada de que la infraestructura detrás del o los niveladores de carga está sincronizada en términos de configuración, o
  - (2) garantía documentada de que el alcance brindado por PCI a IBM identifica en forma única todos los dispositivos de nivelación de carga para que se pueda realizar un análisis completo;
- g. ser responsable de coordinar con su proveedor de servicios de Internet ("ISP") y/o proveedores de hosting para permitir un tráfico de red completamente sin filtros entre los motores de análisis externo de IBM y su o sus redes;
- h. si disputa resultados de análisis por una vulnerabilidad en particular:
  - (1) utilizar el Portal para solicitar una excepción y brindar documentación suficiente a IBM para asistirle en la investigación y resolución de los hallazgos disputados (por ejemplo, sospecha de positivos falsos), y brindará la Atestación correspondiente dentro de VMS;
  - (2) enviar evidencia generada por el sistema tal como screen dumps, archivos de configuración, versiones de sistema, versiones de archivos y una lista de parches instalados. Dicha evidencia generada por el sistema debe estar acompañada por una descripción de cuándo, dónde y cómo se obtuvo; y
  - (3) reconocerá que IBM puede solicitarle contratar (a cargo suyo) a un Asesor de seguridad calificada ("QSA") de PCI antes de aprobar ciertas disputas (tales como controles de compensación propuestos);
- i. usar el Portal para iniciar el análisis;
- j. revisar el informe de análisis y corregir cualquier vulnerabilidad percibida que resulte en un análisis en incumplimiento;
- k. usar el Portal para reanalizar toda dirección de IP en incumplimiento para aprobar el análisis trimestral;
- l. usar el Portal para solicitar que IBM lleve a cabo una Atestación PCI ASV trimestral de Cumplimiento con el análisis;
- m. descargar informes completos de análisis ASV y enviarlos a sus compradores o marcas de pago, de conformidad por lo indicado por las marcas de pago;
- n. que al descargar y enviar informes ASV a compradores o marcas de pago, usted autentica y reconoce:
  - (1) que usted no alteró ni alterará los informes ASV generados por el sistema de forma alguna antes de enviarlos a sus compradores o marcas de pago;
  - (2) ser responsable del alcance adecuado de los análisis y haber incluido todos los componentes en el análisis que deben incluirse en el alcance de PCI DSS;
  - (3) haber implementado segmentación de red, si se excluye algún componente del alcance de PCI DSS;
  - (4) haber brindado evidencia precisa y completa para soportar cualquier disputa sobre los resultados de los análisis; y

- (5) los resultados del análisis solo indican si los sistemas analizados cumplen con el requisito de análisis de vulnerabilidad (PCI DSS 11.2) y no son indicio de cumplimiento general con ningún otro requisito de PCI DSS.

## 5. Contratos de nivel de servicio

Los SLA de IBM establecen los objetivos de tiempo y las contramedidas de eventos específicos que resultan de los Servicios. Los SLA entran en vigencia cuando se completa el proceso de implementación, se ha configurado al o los Agentes (de haber alguno) en “activo”, y se han establecido con éxito el soporte y gestión del Agente en “activo” en los SOC. Se dispone de recursos de SLA siempre y cuando cumpla con sus obligaciones de conformidad con lo definido en esta Descripción de servicios y todos los documentos contractuales relacionados.

### 5.1 Disponibilidad de SLA

Los valores por defecto de SLA descritos a continuación comprenden las métricas medidas para la entrega de los Servicios. A menos que se especifique explícitamente a continuación, no se aplicará garantía alguna para los Servicios entregados de conformidad con esta Descripción de servicios. Los únicos recursos por no cumplir con los valores por defecto de SLA se especifican en la sección de esta Descripción de servicios titulada “Recursos de SLA”.

- Disponibilidad de servicios – IBM brindará 100% de disponibilidad de servicios para los SOC.
- Disponibilidad del Portal – IBM brindará 99,9% de accesibilidad al Portal fuera de los plazos especificados en la sección de esta Descripción de servicios titulada “Mantenimiento de portales de emergencia y programados”.
- Monitoreo proactivo de sistemas – IBM lo notificará en un lapso de 15 minutos después de determinar que su Agente es inalcanzable mediante la conectividad en banda estándar.
- Implementación de análisis – IBM comenzará con la implementación de una evaluación de vulnerabilidad programada en una hora (más o menos una hora) del tiempo programado por usted (o IBM en su nombre) y se habrán completado todos los análisis. Este SLA se aplica solamente a pedidos de análisis configurados correctamente, Agentes en las instalaciones del cliente que se encuentran en línea y accesibles por la infraestructura de SOC, y objetivos de análisis completamente accesibles desde el motor de análisis designado.
- Reconocimiento del pedido de cambio del alcance de PCI – IBM reconocerá pedidos de cambio del alcance de PCI en un lapso de dos horas después haberlos enviado por medio del Portal.
- Implementación de cambios del alcance de PCI – IBM implementará cambios en el alcance de PCI dentro de 72 horas de recibir documentación suficiente y aceptable de usted para justificar el cambio del alcance de PCI.
- Respuesta al pedido de excepción de vulnerabilidad de PCI – IBM responderá con una aprobación o negación del pedido de excepción en un lapso de 72 horas de recibir la documentación suficiente y aceptable de usted que justifique el pedido de excepción de vulnerabilidad de PCI.

Nota: Puede enviar una cantidad ilimitada de pedidos de excepción de vulnerabilidad de PCI; sin embargo, solo los primeros 15 pedidos enviados quedarán sujetos a este SLA. Los pedidos posteriores (a los primeros 15 recibidos en un día) serán aceptados pero no considerados como prioridad, y no se verán sujetos a este SLA.

### 5.2 Recursos de SLA

Disponibilidad de servicios, Disponibilidad del portal, Monitoreo del sistema proactivo, implementación de análisis, reconocimiento del pedido de cambio del alcance de PCI, implementación del pedido de cambio del alcance de PCI, respuesta al pedido de excepción de vulnerabilidad de PCI – Si IBM no cumple con alguno de estos SLA, se enviará un crédito por los cargos aplicables por un día de los cargos mensuales de servicio VMS.

#### Resumen de los SLA y los Recursos

Contratos de nivel de servicio	Recursos de disponibilidad
Disponibilidad de servicios	Crédito por 1 día del cargo mensual de los Servicios
Disponibilidad del Portal	
Monitoreo de sistema proactivo	
Implementación de análisis	
Reconocimiento del pedido de cambio del alcance de PCI	

Implementación del pedido de cambio del alcance de PCI	
Respuesta al pedido de excepción de vulnerabilidad de PCI	

## 6. Otros Términos y Condiciones

### 6.1 General

Usted reconoce y acuerda:

- a. que todo el software brindado por IBM como parte de estos Servicios es licenciado, no vendido. Excepto por las licencias que se otorgan específicamente por el presente, todo derecho, título e interés en o para el software permanecerán en poder de IBM o sus licenciantes;
- b. que informará a IBM por escrito, al menos 30 días antes de la cancelación o rescisión de los Servicios, o inmediatamente si IBM rescinde la licencia para el software de análisis por alguna razón, más allá de su decisión de:
  - (1) hacer que IBM quite el software de análisis de manera remota o asistiéndolo en su remoción; o
  - (2) conservar el software de análisis.
 Si elige eliminar el software de análisis, acuerda cooperar con IBM brindando el acceso remoto necesario para que IBM remueva el software de análisis, o para asistir a IBM en su remoción.
- c. Además de los términos y condiciones enumerados anteriormente, se presentarán términos específicos de licencias para revisar y aceptar tanto cuando descarga como cuando instala el software.

### 6.2 Permiso para realizar pruebas

Ciertas leyes prohíben todo intento no autorizado de penetrar o acceder a sistemas computacionales. Usted autoriza a IBM a realizar los Servicios según lo descrito en el presente y reconoce que los Servicios constituyen un acceso autorizado a sus sistemas computacionales. IBM podrá divulgar esta concesión de autoridad a un tercero si lo considerare necesario para prestar los Servicios.

Los Servicios que presta IBM suponen ciertos riesgos y usted acuerda aceptar todos los riesgos relacionados con tales Servicios; siempre y cuando esto no limite la obligación de IBM de prestar los Servicios en virtud de los términos de este SOW. Usted reconoce y acuerda lo siguiente:

- a. Se pueden generar demasiados mensajes de log, dando como resultado demasiada ocupación de espacio de disco del archivo log;
- b. El rendimiento y la producción de sus sistemas, como el de los routers y firewalls relacionados, pueden verse temporalmente degradados;
- c. Algunos datos pueden modificarse temporalmente como resultado de vulnerabilidades de sondeo;
- d. Sus sistemas de computación pueden tildarse o caer, lo cual puede causar una falla en el sistema o indisponibilidad temporal del sistema;
- e. Durante cualquier actividad de pruebas se deberá renunciar a todo derecho o recurso del contrato de nivel de servicio;
- f. Un análisis puede activar las alarmas de los sistemas de detección de intrusos;
- g. Algunos aspectos de los Servicios pueden implicar la interceptación del tráfico de la red monitoreada para procurar eventos; y
- h. Las nuevas amenazas a la seguridad evolucionan constantemente y ningún servicio destinado a brindar protección contra amenazas a la seguridad podrá hacer invulnerables a los recursos de red de dichas amenazas ni garantizar que dicho servicio identifique todos los riesgos, exposiciones y vulnerabilidades. .

### 6.3 Sistemas de terceros

En el caso de sistemas (que para los propósitos de esta disposición incluyen, a modo enunciativo, aplicaciones y direcciones de IP) de terceros que quedarán sujetos a las pruebas del presente, usted acuerda:

- a. Que antes de que IBM comience con pruebas en un sistema de terceros, usted deberá obtener una carta firmada por el dueño de cada sistema, la cual autorice a IBM a prestar los Servicios en ese sistema, e indique que el dueño acepta las condiciones presentes en la sección titulada "Autorización para realizar pruebas", y entregarle a IBM una copia de dicha autorización;

- b. Ser el responsable exclusivo de comunicar cualquier riesgo, exposición y vulnerabilidad que las pruebas remotas de IBM al sistema del dueño identifiquen en estos sistemas, y
- c. Organizar y facilitar el intercambio de información entre el dueño del sistema e IBM, según IBM lo considere necesario.

Usted acuerda:

- d. Informar inmediatamente a IBM siempre que cualquier sistema sujeto a las pruebas del presente cambie de dueño;
- e. No divulgar los Materiales entregables, o el hecho de que IBM prestó los Servicios, fuera de su Empresa sin el previo consentimiento por escrito de IBM; e
- f. Indemnizar por completo a IBM por cualquier pérdida o responsabilidad en la que IBM incurra por reclamos de terceros como resultado de su incumplimiento de los requisitos de esta sección titulada "Sistemas de terceros" y por cualquier citación o reclamo contra IBM o sus subcontratistas o agentes, como resultado de (a) análisis de riesgo, exposiciones o vulnerabilidades a la seguridad en sistemas sujetos a los análisis del presente, (b) los resultados de dichos análisis que se le presentaron, o (c) su uso o divulgación de tales resultados.

#### **6.4 Aviso**

Usted comprende y acuerda que:

- a. queda a su exclusiva discreción usar o no cualquier información provista en virtud de los Servicios del presente. Por consiguiente, IBM no será responsable de ninguna acción que usted decida tomar o no tomar, en base a los servicios prestados y/o entregables provistos por el presente;
- b. IBM no presta servicios legales ni representa o garantiza que los servicios o productos que IBM presta u obtiene de usted, garantizarán su cumplimiento con alguna ley en particular, incluida, a título enunciativo, toda ley relacionada con la seguridad o privacidad; y
- c. Es su responsabilidad procurar un asesor legal competente que lo aconseje para identificar e interpretar toda ley relevante que pueda afectar a su empresa, y toda acción necesaria para cumplir con tal ley;

#### **6.5 Contratos de la Industria de tarjetas de crédito**

Usted reconoce que IBM es un ASV y opera bajo un contrato actual con el PCI SSC. De conformidad con los términos de dicho contrato, en este Informe de trabajo se incorporan las siguientes disposiciones intermediarias.

- a. Usted reconoce y acuerda que puede solicitar Servicios de IBM en relación con su obligación de cumplir con el Estándar de seguridad de datos de la Industria de tarjetas de crédito ("PCI-DSS"). Usted comprende que la administración del PCI-DSS en relación con las evaluaciones de seguridad se lleva a cabo por las más importantes marcas de tarjetas de crédito ("Marcas"), y dicha administración se coloca con el PCI SSC. Usted reconoce y acuerda que elige a IBM para brindar Servicios de una lista de proveedores aprobados por el PCI SSC (la "Lista ASV"). Asimismo, reconoce que para que IBM sea incluida en la Lista ASV, IBM debe firmar un contrato con el PCI SSC (el "Contrato ASV") cuya copia puede consultarse en [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org), "Requisitos de validación para Proveedores de análisis aprobados (ASVs) Versión 1.2", Apéndice A "Contrato de pruebas de cumplimiento con PCI ASV". También reconoce que partes del contrato requieren de la inclusión por parte de IBM de ciertas disposiciones en sus contratos con sus clientes.
  - (1) Usted comprende y acuerda que la inclusión de IBM en la Lista de ASV no es ni un aval ni una recomendación implícita o expresa de PCI SSC, ni garantía del PCI SSC o cualquiera de sus miembros con respecto a IBM, sus servicios o productos, o la funcionalidad, calidad o funcionamiento de ningún aspecto de lo mencionado anteriormente. Asimismo, usted comprende y acuerda que el PCI SSC no le demanda el uso de productos o servicios de IBM. También acuerda que para los propósitos de esta sección de "Contratos de la Industria de tarjetas de crédito", los significados de los términos capitalizados en los siguientes ítems a. 2, 3, 4, y 5 serán los presentes en el Contrato ASV.
  - (2) Usted comprende y acuerda que (i) IBM puede divulgar los resultados de pruebas y evaluaciones (incluidos los informes de análisis) e información relacionada según lo solicitado por el PCI SSC y/o sus Miembros, según lo que usted solicite, (ii) en la medida en que los miembros obtengan dicha información de conformidad con la cláusula anterior, dicho Miembro puede divulgar dicha información a medida que se la necesita a las respectivas Entidades financieras y Emisores de dicho Miembro además de a inspectores, reguladores y organismos gubernamentales, reguladores y de orden público relevantes, e (iii)

IBM puede divulgar dicha información según sea necesario para cumplir con sus obligaciones y requisitos de conformidad con el Contrato ASV, según lo especificado más detalladamente en la cláusula (4) a continuación. Usted acuerda que el PCI SSC o su comprador pueden divulgar Información confidencial obtenida por el PCI SSC en relación con el Contrato ASV a Miembros de conformidad con este ítem a.2, quienes a su vez podrán divulgar dicha información a sus respectivas Entidades financieras de miembros o demás miembros. Usted acuerda (i) dicha divulgación del PCI SSC y sus Miembros y (ii) toda divulgación de Información confidencial, incluidos, a título enunciativo, los resultados de pruebas y evaluaciones (incluidos los informes de análisis), e información relacionada, autorizada por este ítem a.2. En la medida en que tenga algún contrato de confidencialidad con IBM; los términos de este ítem a.2 son incorporados a dicho contrato por esta referencia.

- (3) Usted comprende que en el Contrato ASV, IBM acordó mantener ciertas prácticas de protección de datos con respecto a la Información personal, de haber alguna, recibida por IBM del PCI SSC o cualquier Miembro o Cliente, e IBM también acordó hacer disponible al PCI SSC y sus Miembros y/o Compradores/Emisores tales revisiones e informes adecuados para monitorear el cumplimiento de IBM con estos requisitos de práctica de protección de datos. Usted está de acuerdo con que IBM realice dichas revisiones e informes al PCI SSC y sus Miembros y/o Compradores/Emisores, como también acuerda brindarle al PCI SSC o cualquier Miembro y/o Comprador/Emisor tales informes y revisiones apropiados para monitorear el cumplimiento de IBM con los requisitos de práctica de protección de datos según lo soliciten razonablemente el PCI SSC o sus Miembros y/o Compradores/Emisores ocasionalmente.
- (4) Usted también comprende que IBM acordó, en el Contrato ASV, y bajo pedido por escrito del PCI SSC o cualquiera de sus miembros (cada uno representa una "Organización demandante") brindar a dicha Organización demandante los resultados de dichas pruebas y evaluaciones (incluidos los informes de análisis) como tal Organización puede solicitar razonablemente con respecto a (i) si la Organización demandante es un Miembro, cualquier Cliente del proveedor por el que IBM ha desarrollado una evaluación, y que es una Entidad financiera de tal Miembro, un Emisor de dicho miembro, un Comerciante autorizado a aceptar tales tarjetas de crédito del Miembro, un Comprador de cuentas de Comerciantes autorizados a aceptar tales tarjetas de crédito del Miembro o un Procesador que preste servicios a las Entidades financieras, Emisores, Comerciantes o Compradores de dicho Miembro, o (ii) si la Organización demandante es PCI SSC, cualquier Cliente del proveedor por el que el ASV ha llevado a cabo una prueba o evaluación. Usted está de acuerdo con la divulgación de los resultados de cualquier prueba o evaluación (incluidos los informes de análisis) relacionados y en otorgarle a IBM todos los derechos, licencias y demás permisos necesarios para que IBM cumpla con sus obligaciones y requisitos en virtud del Contrato ASV.

b. Su indemnización con respecto a los Servicios de la Industria de tarjetas de crédito

En la medida en que IBM brinde los Servicios como un ASV, usted defenderá, indemnizará y eximirá a IBM de todo reclamo, pérdida, responsabilidad, daño, juicio, acción legal, procesos gubernamentales, impuestos, penalidades o intereses, auditorías relacionadas, gastos legales y demás costos (incluidas, a título enunciativo, las tarifas y demás costos razonables de representación legal) que surjan de reclamos del LLC del Consejo de estándares de seguridad de PCI, sus miembros y respectivas filiales, además de todas las filiales, directores, funcionarios, empleados, agentes, representantes, contratistas independientes, abogados, sucesores y cesionarios de cualquiera de los mencionados anteriormente contra IBM o sus filiales relacionadas con los Servicios del presente.