

**Servicios de seguridad de la infraestructura de IBM -  
Unified Threat Management - Select**

# Índice

<b>1.</b>	<b>Alcance de los servicios</b>	<b>4</b>
<b>2.</b>	<b>Definiciones</b>	<b>4</b>
<b>3.</b>	<b>Servicios</b>	<b>5</b>
3.1	Centros de operaciones de seguridad	5
3.2	Portal	6
3.2.1	Responsabilidades del Portal de IBM	6
3.2.2	Sus responsabilidades de Portal	6
3.3	Contactos de servicio	6
3.3.1	Responsabilidades de contactos de servicios de IBM	7
3.3.2	Sus Responsabilidades de contactos de servicios	8
3.4	Inteligencia de seguridad	9
3.4.1	Responsabilidades de inteligencia de seguridad de IBM	9
3.4.2	Sus Responsabilidades de inteligencia de seguridad	9
3.5	Implementación y activación	9
3.5.1	Responsabilidades de Implementación y activación de IBM	9
3.5.2	Sus Responsabilidades de Implementación y activación	13
3.6	Recopilación y Archivado	14
3.6.1	Responsabilidades de Recopilación y Archivado de IBM	15
3.6.2	Sus Responsabilidades de Recopilación y Archivado	15
3.7	Análisis automatizado	16
3.7.1	Responsabilidades de análisis automatizado de IBM	16
3.7.2	Sus Responsabilidades de análisis automatizado	16
3.8	Gestión de políticas	17
3.8.1	Responsabilidades de gestión de políticas de IBM	17
3.8.2	Sus Responsabilidades de gestión de políticas	17
3.9	Soporte de red privada virtual	18
3.9.1	Responsabilidades de soporte de red privada virtual de IBM	18
3.9.2	Sus Responsabilidades de soporte de red privada virtual	18
3.10	Salud del agente gestionado y Monitoreo de disponibilidad	18
3.10.1	Responsabilidades de IBM por la Salud del agente gestionado y el Monitoreo de disponibilidad	18
3.10.2	Sus Responsabilidades por la Salud del agente gestionado y el Monitoreo de disponibilidad	19
3.11	Gestión de agentes	20
3.11.1	Responsabilidades de gestión de agentes de IBM	20
3.11.2	Sus Responsabilidades de gestión de agentes	20
3.12	Informes de seguridad	21
3.12.1	Responsabilidades de informes de seguridad de IBM	21
3.12.2	Sus Responsabilidades de informes de seguridad	21
<b>4.</b>	<b>Servicios opcionales</b>	<b>21</b>
4.1	Monitoreo y notificación de eventos	21
4.1.1	Responsabilidades de notificación y monitoreo de eventos de IBM	22
4.1.2	Sus Responsabilidades de notificación y monitoreo de eventos	22
4.2	Seguridad de contenido	23
4.2.1	Responsabilidades de seguridad del contenido de IBM	23
4.2.2	Sus Responsabilidades de seguridad del contenido	23
4.3	Espera en frío	24
4.3.1	Responsabilidades de espera en frío de IBM	24

4.3.2	Sus Responsabilidades de espera en frío.....	24
4.4	Espera en caliente.....	24
4.4.1	Responsabilidades de espera en caliente de IBM .....	24
4.4.2	Sus Responsabilidades de espera en caliente.....	24
4.5	Alta disponibilidad .....	25
4.5.1	Responsabilidad de alta disponibilidad de IBM .....	25
4.5.2	Sus Responsabilidad de alta disponibilidad .....	25
4.6	Agregador en sitio .....	26
4.6.1	Responsabilidades del Agregador en sitio de IBM.....	26
4.6.2	Sus Responsabilidades del Agregador en sitio .....	27
4.7	Integración del sistema de Tickets .....	28
4.7.1	Responsabilidades de integración del sistema de tickets de IBM .....	28
4.7.2	Sus Responsabilidades de integración del sistema de tickets .....	28
4.8	Entrega de eventos y logs de seguridad .....	28
4.8.1	Responsabilidades de entrega de eventos y logs de seguridad de IBM .....	28
4.8.2	Sus Responsabilidades de entrega de eventos y logs de seguridad .....	28
<b>5.</b>	<b>Acuerdos de nivel de servicio.....</b>	<b>29</b>
5.1	Disponibilidad de SLA .....	29
5.2	Recursos de SLA .....	30

## Descripción de servicios

### Servicios de seguridad de la infraestructura de IBM - Unified Threat Management - Select

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

Servicios de seguridad de infraestructura de IBM – Unified Threat Management – Select (denominado “UTM – Select” o “Servicios”) están diseñados para brindar monitoreo y soporte para dispositivos de amenazas unificadas (denominados “Agentes”) en una variedad de plataformas y tecnologías. Dichos Agentes no deben usarse para ningún otro propósito mientras estén gestionados por IBM.

UTM – Select se entrega en dos paquetes diferenciados:

- Paquete de protección – incluye el Sistema de prevención de intrusos (“IPS”) y soporte de firewall; y
- Paquete de contenidos – paquete opcional agregado que incluye la gestión y el soporte de módulos de filtrado Web, antispam y antivirus.

Las funciones de los servicios descritas en el presente dependen de la disponibilidad y soportabilidad 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 hardware, software y firmware brindados por IBM como no.

#### 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”).

**antispam** – está diseñado para minimizar el volumen de e-mail de spam a casillas de correos de usuarios

**antivirus** – está diseñado para escanear muchos tipos de transferencias de archivos (tales como páginas Web, tráfico de e-mail e intercambios de protocolo de transferencia de archivos (“FTP”)) en busca de gusanos, virus y otras formas de malware.

**Materiales educativos** – incluyen, entre otros, manuales de laboratorio, notas de instructores, literatura, metodologías, curso electrónico e imágenes de estudio de caso, 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.

**firewall** – dispositivo de seguridad de red diseñado para bloquear el acceso no autorizado y permitir configuraciones basadas en una configuración de reglas permiso, negación, codificación, decodificación o proxy alineadas con la política de seguridad de Recipientes de servicios.

**Sistema de prevención de intrusos** – dispositivo de seguridad de red o aplicación de software que emplea técnicas de detección y prevención para monitorear actividades de red en busca de comportamiento malicioso o no deseado. Este monitoreo puede identificar y, en algunos casos, bloquear posibles violaciones a la seguridad en tiempo real.

**Red virtual privada (“VPN”)** – utiliza redes de telecomunicaciones públicas para realizar comunicaciones privadas de datos, mediante la codificación. La mayoría de las implementaciones usa Internet como la infraestructura pública, junto con una variedad de protocolos especializados para soportar comunicaciones privadas.

**Filtrado Web**— está diseñado para asistir al contenido objetable de bloques del destinatario de los servicios, mitigar las amenazas de la Web, y regir el comportamiento de visualización Web del personal detrás del Agente gestionado.

### 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**

<b>Función de servicio</b>	<b>Métrica o cantidad</b>	<b>Acuerdos de nivel de servicio</b>
<a href="#">Disponibilidad de servicios</a>	100%	<a href="#">Disponibilidad de servicios</a>
<a href="#">Disponibilidad del Portal IBM MSS</a>	99.9%	<a href="#">SLA de disponibilidad del Portal IBM MSS</a>
<a href="#">Contactos de seguridad autorizados</a>	3 usuarios	N/A
<a href="#">Archivado de log/evento</a>	Hasta 7 años (1 año por defecto)	N/A
<a href="#">Identificación de incidentes de seguridad</a>	100%	<a href="#">Identificación de incidentes de seguridad</a>
<a href="#">notificación de alertas de incidentes de seguridad</a>	60 minutos	<a href="#">SLA de alerta de incidentes de seguridad</a>
<a href="#">Solicitud de cambio de política</a>	4 por mes	N/A
<a href="#">Reconocimiento de solicitud de cambio de política</a>	2 horas	<a href="#">SLA de reconocimiento de solicitud de cambio de política</a>
<a href="#">Implementación de solicitud de cambio de política</a>	8 horas	<a href="#">SLA de implementación de solicitud de cambio de política</a>
<a href="#">Alerta de salud del agente</a>	15 minutos	<a href="#">SLA de monitoreo del sistema</a>
<a href="#">Actualizaciones de contenido</a>	48 horas	<a href="#">SLA de actualización del contenido</a>
<a href="#">identificación de incidentes de seguridad</a> (servicio opcional agregado)	15 minutos	<a href="#">SLA de notificación de incidentes de seguridad</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 geograffas 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) información y alerta de inteligencia de seguridad;
  - (2) Configuración de agentes y detalles de políticas;
  - (3) Información sobre el incidente de seguridad y el ticket de servicios;
  - (4) Iniciación y actualizaciones de tickets y flujo de trabajo;
  - (5) conversación en vivo y colaboración con analistas de SOC;
  - (6) un panel de informes de planillas;
  - (7) acceso a logs y eventos de Agentes archivados y en tiempo real;
  - (8) Autorización para descargar datos de log;
  - (9) capacidades interrogación de log y eventos de seguridad granular; y
  - (10) 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 “[Acuerdos 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;
- 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 comprometida; 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 servicio

Puede elegir 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 métodos 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 niveles múltiples de acceso al Portal:
  - (1) Capacidades de usuarios administrativos que incluirán:
    - (a) Crear usuarios de Portal;
    - (b) La creación y edición de grupos de Agentes personalizados;
    - (c) El envío de pedidos de cambio de política a los SOC para Agentes gestionados o un grupo de Agentes;
    - (d) Envío de solicitudes de servicios a los SOC;
    - (e) Comunicación con “chat en vivo” que se comunica con analistas de SOC con respecto a incidentes específicos o tickets, generados como parte de los Servicios;
    - (f) Creación de tickets relacionados con servicios internos y asignación de dichos tickets a usuarios de Portal;
    - (g) interrogación y visualizaciones y actualización de tickets relacionados con Servicios;
    - (h) Visualización y edición de detalles de Agentes;
    - (i) Visualización de políticas de Agentes;
    - (j) Creación y edición de listas de observación de vulnerabilidad;
    - (k) El monitoreo de eventos en vivo;
    - (l) Análisis de datos de eventos y log de seguridad;
    - (m) Programación de descargas de daos de log y eventos de seguridad;
    - (n) Programación y ejecución de informes;

- (2) Capacidades de usuarios regulares que incluirán todas las capacidades de usuario administrativo, para los Agentes a los que fueron asignadas, con la excepción de la creación de usuarios de Portal;
- (3) Capacidades de usuarios restringidas que incluirán todas las capacidades de usuario regular, para los Agentes a los que fueron asignadas, con la excepción de:
  - (a) La creación y envío de solicitudes de cambio de política;
  - (b) Actualización de tickets; y
  - (c) Edición de detalles de Agente;
- b. Lo autorizará a aplicar niveles de acceso a un agente o grupos de Agentes;
- c. Autenticará a usuarios del Portal que usen contraseña estática; y
- d. 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;
- 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;
- b. Y 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.

#### **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 las IQ de amenazas.

### **3.5 Implementación y activación**

Durante la implementación y activación, IBM trabajará con usted para implementar un nuevo Agente o comenzar la gestión de un Agente existente.

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 Agente durante el contrato de servicios, IBM puede solicitar que dicho Agente sea reimplementado o reactivado (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 – Inicio del proyecto**

El propósito de esta actividad es realizar una llamada de comienzo del proyecto. IBM le enviará un e-mail de bienvenida y 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 finalizaci3n***

Esta actividad estar1 completa cuando IBM haya realizado la llamada de inicio del proyecto.

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

- Ninguno

### **Actividad 2 – Requisitos de acceso a la red**

El prop3sito de esta actividad es establecer los requisitos de acceso a la red.

IBM:

- a. Le brindar1 un documento denominado “Requisitos de acceso a la red”, detallando:
  - (1) C3mo se conectar1 IBM de manera remota a la red;
  - (2) Requisitos t3cnicos espec1ficos para permitir dicha conectividad remota;

Nota: IBM podr1 realizar cambios al documento de “Requisitos de acceso a la red”, seg1n lo considere apropiado, en toda la realizaci3n de los Servicios.
- b. Se conectar1 a su red por medio de Internet, usando m3todos de acceso est1ndar de IBM; y
- c. De ser apropiado, usar1 una red privada virtual de sitio a sitio (“VPN”) para conectarse a su red. Dichas reimplementaciones se brindar1n a un costo adicional seg1n lo especificado en el Programa.

#### ***Crterios de finalizaci3n***

Esta actividad estar1 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 3 - Evaluaci3n**

El prop3sito de esta actividad es realizar una evaluaci3n de su ambiente actual, adem1s de metas comerciales y tecnol3gicas, para permitir el desarrollo de una estrategia de seguridad requerida para el Agente.

#### ***Tarea 1 – Reunir datos***

IBM:

- a. Le brindar1 un Punto de Contacto con un formulario de recuperaci3n de datos en el que deber1 documentar:
  - (1) Nombres de miembros del equipo, informaci3n de contacto, roles y responsabilidades;
  - (2) Requisitos 1nicos para pa1ses y sitios;
  - (3) Su infraestructura de red existente;
  - (4) Servidores cr1ticos;
  - (5) Cantidad y tipo de usuario finales; e
  - (6) Impulsores y/o dependencias comerciales clave que podr1an influir en la entrega o los plazos de los Servicios.

## **Tarea 2 – Evaluar ambiente**

IBM:

- a. Usará la información brindada en el formulario de recopilación de datos para evaluar su ambiente existente;
- b. Determinará una configuración óptima de Agentes; y
- c. De aplicarse, brindará recomendaciones para ajustar la política de un Agente o disposición de la red para mejorar la seguridad.

## **Tarea 3 – Evaluar agente existente**

IBM:

- a. Evaluará en forma remota al Agente para verificar que cumpla con las especificaciones de IBM;
- b. Identificará cuentas de usuario y aplicación para que sean eliminadas o agregadas, según se aplique;
- c. Para Agentes que no cumplan con las especificaciones de IBM:
  - (1) Identificará al software de Agente que requiera de actualizaciones, y/o
  - (2) identificará hardware de Agentes que requiera de actualizaciones para cumplir con listas de compatibilidad de proveedores aplicables.

### **Crterios de finalización**

Esta actividad estará completa cuando IBM haya evaluado su ambiente y al Agente existente (según se aplique).

### **Materiales entregables**

- Ninguno

## **Tarea 4 – Acceso fuera de banda**

El acceso fuera de banda es una función solicitada 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.

IBM:

- d. Brindará soporte en vivo, por teléfono e e-mail, para asistirlo en ubicar documentos de proveedores aplicables que detallan los procedimientos de instalación y cableado físicos;
- e. Configuraré el dispositivo OOB para acceder a los Agentes gestionados; o
- f. Trabajaré de buena fe con usted para utilizar una solución OOB existente aprobada por IBM.

### **Crterios de finalización**

Esta actividad estará completa cuando IBM haya configurado el dispositivo OOB para acceder al Agente gestionado.

### **Materiales entregables**

- Ninguno

## **Actividad 5 - Implementación**

El propósito de esta actividad es implementar el Agente.

### **Tarea 1 - Configurar al Agente**

IBM:

- a. Evaluará en forma remota al Agente para verificar que cumpla con las especificaciones de IBM;
- b. Identificará el software, hardware, y/o contenido de agentes que no cumpla con los niveles actuales soportados por IBM;
- c. Según corresponda, identificará actualizaciones requeridas de hardware para soportar listas aplicables de compatibilidad de hardware del proveedor;
- d. Configuraré remotamente al Agente, incluida la configuración de políticas, el robustecimiento del sistema operativo y el registro del Agente con la infraestructura de IBM MSS;

- e. Brindará soporte telefónico en vivo y la ubicación de documentos de proveedores para asistirlo en la configuración del Agente con una dirección de IP pública y configuraciones asociadas. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- f. Ajustará la política de Agentes para reducir la cantidad de alarmas erróneas (de aplicarse); y
- g. A pedido suyo, realizará la configuración y política en el Agente existente.

### ***Tarea 2 – Instalar al agente***

IBM:

- a. Brindará soporte en vivo, por teléfono y/o e-mail, para asistirlo en ubicar documentos de proveedores aplicables que detallan los procedimientos de instalación cableado físicos. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- b. Brindará recomendaciones para ajustarse a la disposición de la red para mejorar la seguridad (de aplicarse);
- c. Configuraré al Agente de manera remota, incluido el registro del Agente con la infraestructura de IBM MSS; y
- d. Ajustará la política de Agentes para reducir la cantidad de alarmas erróneas (de aplicarse).

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

### ***Criterios 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. Verificaré la conectividad de los Agentes con la infraestructura de IBM MSS;
- b. Realizaré pruebas de aceptación de Servicios;
- c. Verificaré la entrega de datos de log de los Agentes con la infraestructura de IBM MSS;
- d. Verificaré la disponibilidad y funcionalidad del Agente en el Portal;
- e. Realizaré pruebas de garantía de calidad del Agente; y
- f. Demostraré en forma remota las principales funciones del Portal por hasta diez miembros de su personal, por hasta una hora.

### ***Criterios 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. Asumiré la gestión y soporte del Agente;
- b. Configuraré al Agente en “activo”; y
- c. Trasladaré al Agente a los SOC para gestión y soporte continuos.

### ***Criterios de finalización***

Esta actividad estará completa cuando el Agente esté configurado en “activo”.

### ***Crterios de finalizaci3n***

- Ninguno

## **3.5.2 Sus Responsabilidades de Implementaci3n y activaci3n**

### **Actividad 1 – Inicio del proyecto**

Usted acuerda:

- Atender la llamada de inicio del proyecto; y
- Revisar las respectivas responsabilidades de cada parte.

### **Actividad 2 – Requisitos de acceso a la red**

Usted acuerda:

- Revisar y cumplir con el documento de “Requisitos de acceso a la red” de IBM durante la implementaci3n y todo el t3rmino del contrato; y
- Ser3 responsable 3nico por cualquier costo incurrido como resultado del uso de IBM de una VPN de sitio a sitio para conectarse a su red.

### **Actividad 3 - Evaluaci3n**

#### ***Tarea 1 – Reunir datos***

Usted acuerda:

- Completar y devolver cuestionarios y/o formularios de recopilaci3n de datos a IBM en un plazo de cinco d3as de su recepci3n;
- Obtener y brindar informaci3n, datos, consentimientos, decisiones y aprobaciones aplicables seg3n los requisitos de IBM para la implementaci3n de Servicios, en un plazo de dos d3as h3biles desde el pedido de IBM;
- Trabajar de buena fe con IBM para evaluar de manera precisa su ambiente de red;
- Brindar contactos dentro de su organizaci3n, y especificar una ruta de notificaci3n en su organizaci3n, en caso de que IBM deba contactarlo; y
- Actualizar a IBM en un lapso de tres d3as calendario cuando se modifica su informaci3n de contacto.

#### ***Tarea 2 – Evaluar ambiente***

Usted acuerda:

- Mantener licencias actuales, adem3s de soporte y mantenimiento para los Agentes; y
- Realizar todos los cambios solicitados por IBM a la disposici3n de su red para incrementar la seguridad.

#### ***Tarea 3 – Evaluar agente existente***

Usted acuerda:

- Asegurarse de que el Agente existente cumpla con las especificaciones de IBM;
- Eliminar o agregar aplicaciones y cuentas de usuarios especificadas por IBM;
- Si lo solicita IBM:
  - Pasar a una nueva versi3n del software de Agente especificado por IBM; y
  - Pasar a una nueva versi3n del hardware de Agente especificado por IBM

### **Actividad 4 - Acceso fuera de banda**

Usted acuerda:

- Brindar nuevas soluciones OOB:
  - Adquirir un dispositivo OOB soportado por IBM;
  - Instalar y conectar en forma f3sica el dispositivo OOB al Agente;
  - Brindar una l3nea telef3nica an3loga 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;
- e. 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;
- f. Y reconocer que las soluciones OOB deben estar aprobadas por IBM;
- g. Mantener el contrato actual de soporte y mantenimiento para el OOB (según corresponda); y
- h. Ser responsable de brindar toda la configuración y resolución de problemas en forma remota, si la solución OOB no está disponible por alguna razón.

### **Actividad 5 - Implementación**

#### ***Tarea 1 - Configurar al Agente***

Usted acuerda:

- a. Actualizar a la versión más reciente del software o contenido del Agente soportado por IBM (es decir, medios de carga físicos según corresponda);
- b. Actualizar el hardware para soportar listas de compatibilidad de hardware del proveedor (si se aplica);
- c. Ajustar la política de los Agentes según lo requerido por IBM;
- d. Configurar al Agente con una dirección de IP pública y configuraciones relacionadas; y
- e. 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; y
- c. Realizar cualquier ajuste especificado por IBM a la disposición de la red para incrementar la seguridad.

### **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**

Para esta actividad no se le requiere ninguna responsabilidad adicional.

## **3.6 Recopilación y Archivado**

IBM utiliza el Sistema de protección de X-Force para recopilar, organizar, archivar y recuperar datos de log y eventos de seguridad. El Portal le brinda una visualización de los Servicios las 24 horas del día, los 7 siete días de la semana, incluido el acceso en línea a raw logs recopilados y almacenados dentro de la infraestructura del Sistema de Protección X-Force. Los datos de log y eventos de seguridad podrán

visualizarse en línea en el Portal por un año. Al final del período de un año, los datos pasarán al almacenamiento fuera de línea (de aplicarse).

### 3.6.1 Responsabilidades de Recopilación y Archivado de IBM

IBM:

- a. Recopilará datos de log y eventos generados por el Agente gestionado cuando dichos datos lleguen a la infraestructura de IBM MSS;
- b. Restringirá los flujos de datos de log y eventos generados por el Agente gestionado cuando dichos flujos de datos excedan los 100 eventos por segundo ("EPS");
- c. Identificará en forma única los datos de log y eventos recopilados;
- d. Archivará datos recopilados en el Sistema de protección de X-Force;
- e. Brindará un año de almacenamiento de datos de log y eventos a menos que usted especifique lo contrario;
- f. Desplegará datos de log y eventos recopilados en el Portal por un año;
- g. De estar soportados, normalizará los datos de log y eventos para mejorar la presentación en el Portal;
- h. Comenzará depurando datos de log y eventos recopilados con un método primero en entrar, primero en salir ("FIFO"):
  - (1) Según el período de retención por defecto (un año) o sus períodos de retención definidos (de aplicarse); o
  - (2) Cuando la antigüedad de los datos de log y eventos haya excedido los siete años;

Nota: Más allá de cualquier período de retención definido por usted, IBM no retendrá datos de log y eventos por más de siete años. Si excede su período de retención de siete años en cualquier momento durante la vigencia del contrato, IBM comenzará depurando datos de log y eventos recopilados con el método FIFO.
- i. Si lo considera apropiado, recomendará que se utilice una VPN de sitio a sitio para codificar el tráfico no codificado en forma nativa por el Agente.

Nota: El recorrido de los datos en Internet se codifica con algoritmos de codificación estándares para la industria brindados en forma nativa por el Agente sólo cuando éste (provisto por usted) cuente con la capacidad para hacerlo.

### 3.6.2 Sus Responsabilidades de Recopilación y Archivado

Usted acuerda:

- a. brindar a IBM períodos de retención de eventos y log que no excedan los siete años;
- b. Usar el Portal para revisar y consultar datos de log y eventos de seguridad;
- c. Usar el Portal para mantener disponible la información de espacio de almacenamiento de log y eventos;
- d. Asegurar que se conserve un contrato Select de UTM activo por cada evento de seguridad único y fuente de log; y

Nota: Si los Servicios se rescinden por cualquier razón, IBM no tendrá la obligación de almacenar sus datos de log y eventos de seguridad.
- e. Y reconocer que:
  - (1) A menos que usted indique lo contrario por escrito, IBM conservará los datos de log y eventos recopilados por un año calendario;
  - (2) Todos los datos de log y eventos se transmitirán a los SOC por Internet;
  - (3) Si decide no utilizar una VPN de sitio a sitio recomendada por IBM para Agentes que no brinden algoritmos de codificación en forma nativa, los datos no codificados que viajen por Internet no serán codificados;
  - (4) IBM solo puede recopilar y archivar datos de log y eventos que lleguen con éxito a la infraestructura de IBM MSS;

- (5) IBM no garantiza el envío legal de ningún dato de log o eventos de seguridad 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;
- (6) IBM tiene el derecho de restringir flujos de eventos generados por el Agente que excedan los 100 EPS (de ser requerido);
- (7) IBM no almacenará datos de log y eventos por más de siete años; y
- (8) Sus períodos de retención definidos no podrán exceder los siete años. IBM comenzará depurando datos mediante el método FIFO cuando los datos de log y eventos excedan los siete años, más allá de sus períodos de retención especificados.

### **3.7 Análisis automatizado**

Los agentes son capaces de generar un gran volumen de alarmas en respuesta a las configuraciones de seguridad que están configurados para detectar. El verdadero riesgo de seguridad que corresponde a una condición en particular detectada no es siempre claro, y no es práctico bloquear todos los datos que puedan ser dañinos con el valor por defecto. El monitoreo y análisis adicional de estas alarmas es importante para contar con un sistema de seguridad que funcione bien.

IBM desarrolló y mantiene un motor de análisis de inteligencia automatizada privado (“AI”) como parte del Sistema de protección de X-Force. Los eventos de Agentes se envían al motor de análisis de AI para la correlación e identificación, a medida que son recopilados.

El motor de análisis de AI realiza las siguientes funciones básicas:

- Correlaciona alarmas tanto en tiempo real como históricas;
- Utiliza técnicas de análisis estadístico y basado en reglas;
- Aprovecha los datos sin procesar, normalizados y consolidados; y
- Opera en alarmas de aplicaciones y del sistema operativo.

Las alarmas de AI del Sistema de protección de X-Force se le entregan por medio del Portal. IBM le enviará un e-mail por hora para notificarle las alertas del Sistema de protección X-Force, resumiendo las alarmas de AI, si selecciona esta opción en el Portal.

El análisis automatizado junto con las posteriores alarmas de AI generados por el Sistema de protección X-Force están disponibles solamente en plataformas especificadas por IBM.

#### **3.7.1 Responsabilidades de análisis automatizado de IBM**

IBM:

- a. Enviará los datos de eventos recopilados al motor de análisis del Sistema de protección X-Force con motivo de correlación e identificación;
- b. Desplegará alertas generadas por el motor de análisis de AI del Sistema de protección X-Force en el Portal, a medida que dichas alarmas se hacen disponibles; y
- c. Si usted realiza la configuración, notificará las alertas del Sistema de protección X-Force dentro de los marcos de tiempo establecidos en la sección de esta Descripción de servicios titulada [“Acuerdos de nivel de servicios”](#), [“Notificación de alarmas del incidente de seguridad”](#).

#### **3.7.2 Sus Responsabilidades de análisis automatizado**

Usted acuerda:

- a. Ser responsable de habilitar/deshabilitar las reglas del motor de AI, mediante el Portal;
- b. Ser responsable de programar la notificación de alarmas del Sistema de protección X-Force, mediante el Portal; y
- c. Reconocer:
  - (1) Que el Portal puede usarse para monitorear y revisar alertas generadas por el motor de análisis de AI del Sistema de protección X-Force; y
  - (2) Que el análisis automatizado está disponible solamente en plataformas especificadas por IBM.

### 3.8 Gestión de políticas

IBM define un único cambio de políticas/configuración de Agentes basado en reglas como cualquier período autorizado para agregar o modificar una regla en un contexto con cinco objetos o menos en un solo pedido. Una solicitud de cambio que necesite agregar seis objetos o más o la manipulación de dos o más reglas se contará como dos o más pedidos. Si el pedido se aplica a cambios fuera de la política de Agentes basada en reglas, cada solicitud enviada se considerará como un único cambio.

Puede configurar al Agente gestionado con una sola política global que se aplica a todos los puertos

#### 3.8.1 Responsabilidades de gestión de políticas de IBM

IBM:

- a. Aceptará hasta cuatro solicitudes de cambio de políticas por mes de Contactos de seguridad autorizados o Contactos de servicios designados, por medio del Portal;
- b. Reconocerá los pedidos de cambio de política por medio del Portal con los marcos de tiempo establecidos en la sección de Descripción de Servicios titulada [“Acuerdos de nivel de servicios”](#), [“Reconocimiento de solicitudes de cambio de políticas”](#);
- c. Revisará las solicitudes de cambio de políticas emitidas para verificar que haya brindado toda la información requerida en dichas solicitudes;
- d. De ser necesario, notificará al emisor que se necesita de información adicional. Durante este tiempo, los contadores de acuerdos de nivel de servicios (“SLA”) se colocarán en espera;
- e. Preparará y revisará la configuración de cambios de política según lo que usted solicite;
- f. Implementará los pedidos de cambio de política con los marcos de tiempo establecidos en la sección de Descripción de Servicios titulada [“Acuerdos de nivel de servicios”](#), [“Implementación de solicitudes de cambio de políticas”](#);
- g. Documentará detalles de la solicitud de cambio de políticas en el sistema de tickets de IBM MSS;
- h. Desplegará tickets de solicitud de cambio de política en el Portal;
- i. A su pedido, y por un costo adicional (sujeto a la disponibilidad del recurso de IBM), brindará cambios de política adicionales;
- j. Realizará copias de seguridad de la configuración del Agente gestionado diariamente;
- k. Conservará 14 copias de seguridad de la configuración;
- l. Desplegará la configuración actual del Agente en el Portal; y
- m. Trimestralmente y con su solicitud por escrito:
  - (1) Auditará sus configuraciones de política para verificar la precisión; y
  - (2) Trabjará con usted para revisar los Agentes gestionados y brindará cambios recomendados a la estrategia de protección de red.

#### 3.8.2 Sus Responsabilidades de gestión de políticas

Usted acuerda:

- a. Asegurar el envío de todas las solicitudes de cambio de políticas por un Contacto de seguridad autorizado o un Contacto de servicios designados, usando el Portal, de conformidad con los procedimientos establecidos identificados anteriormente;
- b. Ser responsable de brindar la información suficiente para cada cambio de política solicitado para permitir que IBM realice con éxito dicho cambio;
- c. Ser responsable de notificar a IBM si desea que realice una revisión trimestral de políticas;
- d. Ser el único responsable de su propia estrategia de seguridad, incluidos los procedimientos de incidentes de seguridad; y
- e. Reconocer:
  - (1) Que IBM completará todos los cambios de políticas, no usted;
  - (2) Que la implementación de cambios de política que IBM considere que tienen un impacto adverso en la capacidad de los Agentes de proteger el ambiente de red resultarán en la suspensión de las SLA aplicables; y

- (3) Después del fin de un mes calendario, los cambios no usados se considerarán nulos y podrán no pasar al siguiente mes.

### **3.9 Soporte de red privada virtual**

Usando uno de los siguientes métodos, IBM activará sus funciones de VPN solicitadas del Agente gestionado:

- a. VPNs de sitio a sitio entre dos Agentes capaces de VPN gestionados por IBM, o un Agente gestionado por IBM y un dispositivo capaz de VPN no gestionado por IBM;
- b. VPNs de cliente a sitio mediante un modelo en el que IBM establece la configuración y le permite administrar usuarios de VPN de cliente a sitio; o
- c. VPNs de Capa segura de tomacorrientes por medio de un modelo en el que IBM establece la configuración y le permite administrar los usuarios de VPN de SSL.

El soporte de cliente a sitio y SSL VPNs está disponible solamente en plataformas especificadas por IBM.

#### **3.9.1 Responsabilidades de soporte de red privada virtual de IBM**

IBM:

- a. Configuraré hasta dos VPNs de sitio a sitio durante la implementación y activación de cada Agente;
- b. Brindaré soporte de métodos de autenticación estática y dinámica de la configuración de VPN;
- c. Configuraré VPNs de cliente a sitio y crearé y autorizaré hasta cinco usuarios de VPN de cliente a sitio;
- d. configuraré VPNs de SSL y crearé y autorizaré hasta cinco usuarios de VPN de SSL;
- e. Le brindaré permisos de acceso apropiados para administrar a sus usuarios de cliente a sitio o VPN de SSL; y
- f. Le brindaré una demostración de administración de usuarios de cliente a sitio o VPN de SSL (según corresponda).

#### **3.9.2 Sus Responsabilidades de soporte de red privada virtual**

Usted acuerda:

- a. Brindar a IBM toda la información requerida para habilitar sus funciones de VPN solicitadas;
- b. Ser responsable de crear y administrar a todos los usuarios de cliente a sitio y VPN de SSL luego de la habilitación inicial de IBM; y
- c. Reconocer:
  - (1) Que toda VPN de sitio a sitio que solicite luego de implementar y activar al Agente se contará en relación con la asignación de cambios de política del presente mes;
  - (2) Responsabilidad exclusiva por la obtención además de los cargos relacionados por toda aplicación de administración de cliente a sitio o VPN de SSL del fabricante de Agentes;
  - (3) Responsabilidad exclusiva por el soporte y mantenimiento además de los cargos relacionados por toda aplicación de administración de cliente a sitio o VPN de SSL asignada al fabricante de Agentes;
  - (4) Que IBM debe aprobar las soluciones de VPN de cliente a sitio; y
  - (5) Que la autenticación basada en certificados actualmente no se soporta como parte de la configuración de VPN.

### **3.10 Salud del agente gestionado y Monitoreo de disponibilidad**

IBM monitoreará el estado de salud y la disponibilidad de los Agentes gestionados. Dicho monitoreo está diseñado para asistir en incrementar la disponibilidad y tiempo de actividad de los Agentes.

#### **3.10.1 Responsabilidades de IBM por la Salud del agente gestionado y el Monitoreo de disponibilidad**

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

El propósito de esta actividad es monitorear la salud y el rendimiento de los Agentes. IBM MSS realizará esta tarea usando el monitoreo basado en Agentes o sin agentes.

### **Monitoreo basado en Agentes**

Cuando sea posible técnicamente, IBM instalará software en Agentes candidatos para monitorear la salud 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.

### **Monitoreo sin Agentes**

Cuando no sea técnicamente posible instalar el software de monitoreo, IBM monitoreará el flujo de datos proveniente de los Agentes y/o realizará un sondeo de las interfaces administrativas en los Agentes.

IBM:

- a. monitoreará las interfaces administrativas de los Agentes; y/o
- b. Monitoreará el flujo de eventos generado por los Agentes; e
- c. Iniciará verificaciones temporales adicionales si se pierde el contacto con el Agente gestionado.

### **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 la salud 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 la salud 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 "[Acuerdos 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 la salud del Agente y los tickets de parada en el Portal.

## **3.10.2 Sus Responsabilidades por la Salud del agente gestionado y el Monitoreo de disponibilidad**

### **Actividad 1 - Monitoreo**

Usted acuerda:

- a. Permitir a IBM instalar el software de monitoreo en todos los Agentes gestionados, en los que IBM considere dicha instalación como técnicamente posible; o

- b. Permitir a IBM monitorear las interfaces administrativas y el flujo de eventos de los Agentes gestionados cuando no sea técnicamente posible instalar software de monitoreo en dichos Agentes.

### **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 OOB, o si la solución OOB no está disponible por alguna razón
- 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.

## **3.11 Gestión de agentes**

Las actualizaciones de aplicaciones y seguridad de agentes son componentes fundamentales de una empresa. IBM usa un enfoque agnóstico de proveedores para la gestión de Agentes.

### **3.11.1 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 nuevas actualizaciones de contenido de seguridad en los Agentes, a medida que los proveedores aplicables van lanzándolas, dentro del marco temporal establecido en la sección de esta Descripción de servicios titulada “Acuerdos de nivel de servicios”, “[Actualización de contenido de seguridad proactivo](#)”;
- d. 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;
- e. 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
- f. Declarará claramente, en la notificación de la ventana de mantenimiento, los impactos esperados y sus requisitos específicos.

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

### **3.12 Informes de seguridad**

Al utilizar el Portal, tendrá acceso a la información de servicios e informes con vistas personalizables de la actividad en la empresa, el grupo de trabajo y los niveles de Agentes. El Portal también le brinda la capacidad de programar los informes personalizados.

#### **3.12.1 Responsabilidades de informes de seguridad 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/tickets de Servicios;
- c. Cantidad de incidentes de seguridad detectados, así como la prioridad y el estado;
- d. lista y resumen de incidentes de seguridad;
- e. Informes de Agente IDS/IPS que incluyen métricas de ataque, ataques evitados, impacto de vulnerabilidad, conteos/tendencias de eventos;
- f. Correlación y análisis de eventos; y
- g. Informes de firewall que incluyen resumen, análisis de tráfico, uso de protocolo y uso de IP específico y reglas.

#### **3.12.2 Sus Responsabilidades de informes de seguridad**

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 Monitoreo y notificación de eventos**

Los analistas de seguridad de IBM MSS realizarán el monitoreo y análisis de eventos para alarmas de AI de eventos generadas por el Sistema de protección X-Force que resultan del análisis automatizado realizado en los eventos IDS/IPS. IBM será el único que pueda determinar si un evento de seguridad se considera un incidente de seguridad o no. Los eventos identificados se clasificarán, priorizarán y escalarán según lo considere apropiado IBM. Las alarmas no eliminadas como disparadores benignos se clasifican como incidentes de seguridad ("SI").

Los incidentes de seguridad ("SI") se clasifican en una de las tres prioridades descritas a continuación:

- SI – Prioridad 1  
Las investigaciones que resultan en una clasificación de alta prioridad (i.e., Prioridad 1) requieren de una acción defensiva inmediata.
- SI – Prioridad 2  
Las investigaciones que resulten en una clasificación de prioridad media (es decir, Prioridad 2) requieren de una acción en el lapso de 12 - 24 horas desde la notificación.
- SI – Prioridad 3  
Las investigaciones que resulten en una clasificación de prioridad baja (es decir, Prioridad 3) requieren de una acción en el lapso de 1 - 7 días desde la notificación.

#### 4.1.1 Responsabilidades de notificación y monitoreo de eventos de IBM

A pedido suyo, y sin costo adicional especificado en el Programa, IBM:

- a. Monitoreará las alarmas de AI del sistema de protección X-Force que resulten del análisis de AI en tiempo real en datos de eventos de IDS/IPS;
- b. Realizará una investigación y análisis de alarmas de AI;
- c. Cuando sea posible, eliminará los positivos falsos y disparadores benignos y los clasificará como incidentes de seguridad comentados ("CSI");
- d. Identificará alarmas no eliminadas como disparadores benignos y clasificará dichas alarmas como incidentes de seguridad ("SIs"):
  - (1) Activará los contadores de SLA; y
  - (2) Priorizará los SI como altos, medios o bajos;
- e. Mediante la ruta de notificación estándar que usted brinde, escalará los SI a un Contacto de seguridad autorizado o Contactos de servicios designados según las "mejores prácticas" de notificación de seguridad de IBM dentro del marco de tiempo y usando el medio (por ejemplo e-mail o teléfono) establecido en la sección de esta Descripción de servicios titulada "[Acuerdos de nivel de servicios](#)", "[Notificación de incidentes de seguridad](#)";
- f. Brindará recomendaciones de recursos/contramedidas, si corresponde;
- g. Documentará detalles de CSIs y SIs en el sistema de tickets de IBM; y
- h. Enumerará los CSIs y SIs en el Portal.

#### 4.1.2 Sus Responsabilidades de notificación y monitoreo de eventos

Usted acuerda:

- a. Utilizar el Portal para investigar eventos de auditoría o eventos continuos no considerados como amenazas inmediatas;
- b. Brindarle a IBM documentación global actual de su ambiente;
- c. Actualizar a IBM dentro de los tres días calendario de cambios dentro de su ambiente;
- d. Brindar a IBM la siguiente información, y mantener dicha información actualizada mediante el Portal;
  - (1) Brindar información de servidores críticos (por ejemplo, nombre, plataforma, sistema operativo ("SO"), dirección del protocolo de Internet ("IP") y tipo de segmentos de red);
  - (2) Información de redes monitoreadas;
  - (3) Información de dispositivos utilizando la dirección de redes ("NAT") (por ejemplo, nombre, plataforma, SO, y tipo de segmento de red);
  - (4) Servidores proxy; y
  - (5) Escáneres autorizados;
- e. Brindar y mantener actual una ruta de notificación de contacto lineal, incluidos los números de teléfono y direcciones de e-mail;
- f. actualizar a IBM, mediante el Portal, en un lapso de tres días calendario si existe un cambio en su información de contacto;
- g. Brindar alias de e-mail, según sea necesario, para facilitar la notificación
- h. Asegurarse de disponer de un Contacto de seguridad autorizado o un Contacto de servicios designado especificado en la ruta de notificación 24 horas al día, 7 días a la semana;
- i. Visualizar detalles de los CSI y SIs mediante el Portal;
- j. Trabajar con IBM para optimizar IBM el servicio de monitoreo;
- k. Brindar retroalimentación de los CSI y SIs mediante el Portal;
- l. Y reconocer que:
  - (1) Una vez que IBM haya escalado un SI, usted es el único responsable por todas las respuestas de incidentes de SI, y las actividades de indemnización; y
  - (2) No todas las investigaciones de actividad sospechosa resultarán en la declaración de un SI.

- (3) El monitoreo y la notificación de eventos se aplica solamente a las alarmas de AI resultado de un análisis automatizado realizado en eventos IDS/IPS de red; y
- (4) La no retroalimentación puede resultar en una menor priorización de actividad persistente o recurrente.

## **4.2 Seguridad de contenido**

El Agente puede configurarse para permitir la solución de seguridad de contenido en ciertas plataformas especificadas por IBM. El UTM – Select no soporta soluciones de seguridad de contenido externo.

A pedido suyo, IBM puede brindar soporte para las siguientes funciones de contenido del Agente gestionado:

- Filtrado Web;
- antispam
- Antivirus.

### **4.2.1 Responsabilidades de seguridad del contenido de IBM**

A pedido suyo, y sin costo adicional especificado en el Programa, IBM:

- a. Configuraré al Agente para que soporte una solución de seguridad de contenidos internos en una plataforma especificada por IBM;
- b. Configuraré su política de seguridad de contenidos de filtrado Web específico durante la implementación y activación del Agente, la cual incluye:
  - (1) Listas de categoría – una selección de categorías de contenido para bloquear;
  - (2) Listas blancas de destino – sitios específicos que deberían permitirse si se encuentran en una categoría de contenidos denegada;
  - (3) Listas negras de destino – sitios específicos que deberían bloquearse si se encuentran en una categoría de contenidos permitida;
  - (4) Lista blanca de fuente – direcciones de IP específicas que deberían excluirse del filtrado de contenidos;
- c. Configuraré su política de antispam específica durante la implementación y activación del Agente, la cual incluye:
  - (1) Listas blancas – direcciones de e-mail y/o dominios específicos para ingresar siempre; y
  - (2) Listas negras– direcciones de e-mail y/o dominios específicos que deberían bloquearse.
- d. Brindaré soporte antivirus durante la implementación y activación del Agente;
- e. aplicaré actualizaciones de seguridad de contenido según se describe en la sección de esta Descripción de servicios titulada “Gestión de agentes”; y
- f. Aceptaré y aplicaré cambios a la política de seguridad de contenido según se describe en la sección de esta Descripción de servicios titulada “Gestión de políticas”.

### **4.2.2 Sus Responsabilidades de seguridad del contenido**

Usted acuerda:

- a. Ser responsable de brindar la información suficiente para cada cambio de política solicitado para permitir que IBM realice con éxito dicho cambio;
- b. ser responsable por todos los cargos relacionados con la gestión continua de la solución de seguridad de contenidos; y
- c. Reconocer:
  - (1) Que es responsable por la obtención, el soporte, las licencias, el mantenimiento y otros costos relacionados por la solución de seguridad de contenido; y
  - (2) Que todos los cambios a las políticas de seguridad de contenidos luego de implementar y activar al Agente se contarán en relación con la asignación de cambios de política del presente mes;

### 4.3 Espera en frío

La espera en frío es un sistema de recuperación de desastres en el que un Agente está disponible como sustituto en caso de que el Agente principal tenga una falla de hardware y/o software. Los Agentes de espera en frío no están potenciados o listos para usar, y no contienen actualizaciones de configuración activa, política o contenido.

#### 4.3.1 Responsabilidades de espera en frío de IBM

A pedido suyo, sin costo adicional, IBM:

- a. Trabaja con usted para pasar al Agente de espera en frío a producción y configurar dicho Agente en "activo" si falla el Agente primario;
- b. Aplicará las actualizaciones de contenido requeridas al Agente de espera en frío en caso de que falle el Agente principal; y
- c. Aplicará la configuración activa actual al Agente de fallar el Agente principal.

#### 4.3.2 Sus Responsabilidades de espera en frío

Usted acuerda:

- a. Brindar un Agente secundario para que actúe como Agente de espera en frío;
- b. mantener licencias actuales, además de contratos de soporte y mantenimiento para los Agentes de espera en frío;
- c. Trabajar con IBM para pasar al Agente de espera en frío a producción y configurar dichos Agente en "activo" si falla el Agente primario; y
- d. Y reconocer que:
  - (1) Los Agentes de espera en frío no son gestionados ni mantenidos por IBM a menos que los pasen a "activo";
  - (2) Los agentes de espera en frío requieren de cambios en la configuración para pasar a "activo"; y
  - (3) Los Agentes de espera en frío no pueden generar tráfico para los SOCs a menos que el Agente principal haya fallado y el Agente de espera en frío se haya ubicado en producción y pase a "activo".

### 4.4 Espera en caliente

La espera en caliente es un método de redundancia que puede reducir el tiempo de inactividad por fallas de hardware y/o software de Agentes. La gestión de espera en caliente está diseñada para brindarle la opción de que IBM le gestione y mantenga actualizado un único Agente adicional. Si su Agente principal falla, el Agente adicional o "gusano" estará disponible para restaurar Servicios más rápidamente. Un Agente de espera no podrá generar ningún tráfico para los SOC a menos que se lo coloque en producción y configurado en "activo".

IBM fomenta seriamente el acceso OOB al Agente de espera en caliente según se describe en la sección de esta Descripción de servicios denominada "Acceso fuera de banda".

#### 4.4.1 Responsabilidades de espera en caliente de IBM

A pedido suyo, y sin costo adicional especificado en el Programa, IBM:

- a. Mantendrá el estado de salud y disponibilidad del Agente de espera en caliente según se describe en la sección de esta Descripción de servicios titulada "Monitoreo de salud y disponibilidad del Agente gestionado";
- b. aplicará actualizaciones de contenido a los Agentes de espera en caliente según se describe en la sección de esta Descripción de servicios titulada "Gestión de agentes"; y
- c. Pasará al Agente de espera en caliente a "activo" de fallar el Agente principal.

#### 4.4.2 Sus Responsabilidades de espera en caliente

Usted acuerda:

- a. mantener licencias actuales, además de contratos de soporte y mantenimiento para las plataformas de espera en caliente;

- b. ser responsable por todos los cargos relacionados con la gestión continua del Agente de espera en caliente;
- c. Brindar direcciones de IP secundarias;
- d. Cumplir con, y realizar, sus Responsabilidades de monitoreo de salud y disponibilidad de Agentes gestionados según se describe en la sección de esta Descripción de servicios titulada “Monitoreo de salud y disponibilidad de Agentes gestionados”;
- e. Cumplir con, y realizar, sus Responsabilidades de gestión de Agentes según se define en la sección de esta Descripción de servicios titulada “Gestión de agentes”;
- f. Y reconocer que:
  - (1) Los cambios de políticas realizados al Agente principal no se verán reflejados en el Agente de espera en caliente;
  - (2) Los Agentes de espera no podrán generar tráfico para los SOC a menos que se los haya colocado en producción y configurado en “activo”; y
- g. 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

#### **4.5 Alta disponibilidad**

Para ayudar a protegerlo de fallas en el hardware y/o software y brindar una alta disponibilidad (“HA”), se pueden configurar e implementar Agentes de protección gestionados; uno completamente operacional y el otro en espera como copia de seguridad que entre en funcionamiento si falla el primer Agente. Algunos Agentes también pueden implementarse como clústeres para que los Agentes múltiples operen y compartan la carga de red.

##### **Implementaciones de activo/pasivo**

En esta configuración, se configura un segundo Agente, listo para comenzar brindando el servicio de red si el Agente principal experimenta una falla crítica de hardware o software. En dicho escenario, la recuperación es automática y se espera que sea inmediata.

##### **Implementaciones activo/activo**

Los clústeres activo/activo usan dos o más Agentes para manejar el tráfico en red simultáneamente. En esta configuración, cada Agente maneja una parte de los paquetes de red, determinados por un algoritmo de equilibrio de peso. Si falla un Agente, el o los otros Agentes están diseñados para manejar automáticamente todo el tráfico hasta que se haya restaurado al Agente.

IBM fomenta seriamente el acceso OOB a todos los Agentes de la configuración de alta disponibilidad, según se describe en la sección de esta Descripción de servicios denominada “Acceso fuera de banda”.

#### **4.5.1 Responsabilidad de alta disponibilidad de IBM**

A pedido suyo, y sin costo adicional especificado en el Programa, IBM:

- a. Configuraré a un Agente secundario ya sea en una configuración activo/pasivo o activo/activo, según lo que usted especifique;
- b. Realizaré configuraciones activo/activo utilizando tres Agentes o más (“clúster”) en modo unicast (es decir, comunicación entre un único remitente y un único receptor por una red);  
Nota: IBM no soporta configuraciones activo/activo en modo multicast.
- c. Gestionaré y monitorearé la solución HA;
- d. mantendrá el estado de salud y disponibilidad del Agente secundario según se describe en la sección de esta Descripción de servicios titulada “Monitoreo de salud y disponibilidad del Agente gestionado”;
- e. aplicará actualizaciones de contenido al o los Agentes secundarios según se describe en la sección de esta Descripción de servicios titulada “Gestión de agentes”; y
- f. Actualizaré la política de Agentes secundarios según se describe en la sección de esta Descripción de servicios titulada “Gestión de políticas”.

#### **4.5.2 Sus Responsabilidad de alta disponibilidad**

Usted acuerda:

- a. Proveer un Agente secundario;

- b. Realizar cualquier cambio requerido para licencias de software;
- c. Brindar direcciones de IP secundarias;
- d. ser responsable por todos los cargos relacionados con la gestión continua del Agente secundario;
- e. Cumplir con, y realizar:
  - (1) Sus Responsabilidades de monitoreo de salud y disponibilidad de Agentes gestionados según se define en la sección de esta Descripción de servicios titulada “Monitoreo de salud y disponibilidad de Agentes gestionados”;
  - (2) Sus Responsabilidades de gestión de Agentes según se define en la sección de esta Descripción de servicios titulada “Gestión de agentes”;
  - (3) Sus Responsabilidades de gestión de políticas según se define en la sección de esta Descripción de servicios titulada “Gestión de políticas”;
- f. ser responsable por la configuración en forma remota y la resolución de problemas, si decide no implementar una solución OOB en Agentes tanto principales como secundarios, o si la solución OOB no está disponible por alguna razón; y
- g. Y reconocer que:
  - (1) que los Servicios no soportan soluciones de HA no integradas;
  - (2) IBM soporta configuraciones activo/activo utilizando tres Agentes o más únicamente en modo unicast.

#### 4.6 Agregador en sitio

El Agregador en sitio (“OA”) es un dispositivo que usted brinda y es implementado en su sitio. El propósito del OA es centralizar la recopilación de datos de eventos de log y seguridad cuando cuenta con Agentes múltiples que se suscriben a IBM MSS y transmitir estos datos de manera segura a IBM MSS para continuar el procesamiento y el almacenamiento a largo plazo.

Las funciones básicas del OA son:

- a. Recopilar o combinar los datos de eventos de seguridad y log;
- b. Comprimir los datos de eventos y log de seguridad;
- c. Codificar los datos de eventos y log de seguridad; y
- d. Transmitir los datos de eventos de seguridad y log a la infraestructura de IBM MSS.

Las principales funciones del OA son:

- a. Realizar colas locales agregando los eventos en forma local cuando no se dispone de una infraestructura de IBM MSS;
- b. Realizar transmisión unidireccional de log. La comunicación del OA se realiza por medio de conexiones SSL/TCP-443 de salida;
- c. Restringir mensajes, si está configurado. Esto limita el ancho de banda del OA a la infraestructura de IBM MSS (en mensajes por segundo) para preservar el ancho de banda; y
- d. Proveer de ventanas de transmisión, de estar configurado. Las ventanas de transmisión activan/desactivan la transmisión de eventos a la infraestructura de IBM MSS durante el marco de tiempo que usted especificó en el Portal.

IBM fomenta seriamente el acceso OOB al OA según se describe en la sección de esta Descripción de servicios denominada “Acceso fuera de banda”.

##### 4.6.1 Responsabilidades del Agregador en sitio de IBM

A pedido suyo, y sin costo adicional especificado en el Programa, IBM brindará los siguientes servicios:

###### **Actividad 1 - Configuración**

El propósito de esta actividad es configurar el OA.

IBM:

- a. Brindará soporte en vivo, por teléfono o e-mail, y lo asistirá en la ubicación de los documentos de proveedores aplicables detallando los procedimientos de instalación y configuración para el sistema

- b. Le brindará las especificaciones de hardware para la plataforma de OA;
- c. Le brindará la configuración y el software de OA;
- d. Le brindará soporte por teléfono e e-mail para asistirlo con la instalación del software de OA en la plataforma de hardware que usted brinde. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- e. A pedido suyo, y sin costo adicional especificado en el Programa, brindará servicios de instalación de software:
- f. En el caso de plataformas existentes:
  - (1) Evaluará las configuraciones existentes de hardware para asegurarse de que cumplan con la especificación de IBM; e
  - (2) Identificará actualizaciones de hardware requeridas que usted deberá brindar e instalar.

### **Actividad 2 - Instalación**

El propósito de esta actividad es instalar el OA.

IBM:

- a. Brindará soporte en vivo, por teléfono e e-mail, y lo asistirá en la ubicación de documentos de proveedores aplicables detallando los procedimientos de instalación y cableado físicos del OA. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;

Nota: Puede contratar por separado para que IBM brinde servicios de instalación y cableado físicos.

- b. Configuraré de manera remota el OA para incluir su registro con la infraestructura de IBM MSS y comenzará con el proceso de intervención de implementación y gestión del OA; y
- c. Confirmará que la infraestructura de IBM MSS reciba la comunicación del OA.

### **Actividad 3 – Gestión y soporte continuos**

El propósito de esta actividad es brindar una gestión y soporte continuos del OA.

IBM:

- a. Establecerá el OA en “activo” en los SOC’s para el soporte y la gestión continuos;
- b. mantendrá el estado de salud y disponibilidad del OA según se describe en la sección de esta Descripción de servicios titulada “Monitoreo de salud y disponibilidad del Agente gestionado”;
- c. aplicará actualizaciones de software al OA según se describe en la sección de esta Descripción de servicios titulada “Gestión de agentes”; y
- d. Será responsable por la gestión y monitoreo del OA por el término del contrato y durante cualquier período de renovación.

## **4.6.2 Sus Responsabilidades del Agregador en sitio**

### **Actividad 1 - Configuración**

Usted acuerda:

- a. Brindarle a IBM la dirección de IP externa para el OA;
- b. Brindarle el hardware para la plataforma de OA, según las recomendaciones y requerimientos de IBM;
- c. Instalar el software de OA brindado por IBM en el hardware que se le entregó, guiado por IBM;
- d. Configurar una dirección de IP externa junto con la configuración de OA relacionada;
- e. Brindarle a IBM la dirección de IP de OA, el nombre del servidor, la plataforma de la máquina, la versión de la aplicación y el uso horario del Agente; y
- f. En el caso de plataformas existentes, obtener e instalar las actualizaciones de hardware solicitadas por IBM.

## **Actividad 2 - Instalación**

Usted acuerda:

- a. Ser responsable por la instalación y el cableado físicos del OA; y
- b. Programar soporte en vivo con un especialista de implementación de IBM.

## **Actividad 3 – Gestión y soporte continuos**

Usted acuerda:

- a. Ser responsable de obtener e instalar las actualizaciones de hardware requeridas en la plataforma de OA por el término del contrato;
- b. Cumplir con, y realizar, sus Responsabilidades de monitoreo de salud y disponibilidad de Agentes gestionados según se describe en la sección de esta Descripción de servicios titulada “Monitoreo de salud y disponibilidad de Agentes gestionados”; y
- c. Cumplir con, y realizar, sus Responsabilidades de gestión de Agentes según se describe en la sección de esta Descripción de servicios titulada “Gestión de agentes”;

### **4.7 Integración del sistema de Tickets**

Si desea que sus inversiones en tickets con problemas y gestión de casos rindan, IBM le brindará una interfaz de programas de aplicación (“API”) que permite una integración personalizada con sistemas de tickets externos.

#### **4.7.1 Responsabilidades de integración del sistema de tickets de IBM**

A pedido suyo, y por un costo adicional especificado en el Programa, IBM le brindará un API que le permitirá realizar una integración personalizada con sistemas de tickets externos.

#### **4.7.2 Sus Responsabilidades de integración del sistema de tickets**

Usted acuerda:

- a. Ser responsable por todos los costos adicionales relacionados con la integración de tickets de API;
- b. Utilizar el paquete de API del Portal para facilitar la integración de tickets;
- c. Ser responsable por todas las cuestiones de ingeniería y desarrollo relacionadas con la integración de tickets; y
- d. Reconocer que IBM no le brindará asistencia ni consultoría por su integración del sistema de tickets.

### **4.8 Entrega de eventos y logs de seguridad**

A pedido suyo, IBM recuperará datos de log y eventos de la infraestructura de IBM MSS y dispondrá de su descarga desde un servidor de IBM asegurado. Cuando IBM considere que la cantidad de datos de log y eventos es demasiada para hacerla disponible por descarga, IBM almacenará los datos en medios codificados y la enviará a una ubicación que usted especifique. La posibilidad de entrega por descarga se evaluará caso por caso.

#### **4.8.1 Responsabilidades de entrega de eventos y logs de seguridad de IBM**

A pedido suyo, y sin costo adicional especificado en el Programa, IBM:

- a. recuperará (vía el Portal) datos específicos de la infraestructura de IBM MSS y se los hará disponibles para que los descargue en un servidor de IBM asegurado; y
- b. Le informará de los cargos adicionales por el tiempo y los materiales utilizados para recuperar y preparar los datos.

#### **4.8.2 Sus Responsabilidades de entrega de eventos y logs de seguridad**

Usted acuerda:

- a. Solicitar la entrega de logs de eventos de seguridad por medio del Portal;
- b. Descargar los datos solicitados desde un servidor de IBM asegurado;
- c. Y reconocer que los pedidos de recuperación de cantidades excesivas de datos pueden requerir que éstos sean almacenados en medios codificados y enviados a una ubicación especificada por usted; y

- d. Ser responsable por todos los costos de tiempo, materiales y envío (según corresponda) relacionados con la entrega de logs.

## 5. Acuerdos 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 Agente 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 ninguna garantía para los Servicios entregados de conformidad con esta Descripción de servicios. Los únicos recursos por incumplir con los valores por defecto de SLA se especifican en la sección de esta Descripción de servicios titulada “Recursos de SLA”.

- a. Identificación de incidentes de seguridad – IBM identificará todos los eventos según los considere como incidentes de seguridad de nivel de Prioridad 1, 2 y 3 en datos de eventos de IDS/IPS del Agente recibidos por los SOC.
  - (1) Incidentes de Prioridad 1: Eventos de alto riesgo con el potencial para causar daños severos a sus sistemas o ambientes requieren de una acción defensiva inmediata. Los ejemplos de incidentes de Prioridad 1 incluyen compromisos de sistema o datos, infecciones/propagación de gusanos y masiva negación de ataques a servicios (“DOS”).
  - (2) Incidentes de Prioridad 2: Eventos de menor riesgo que pueden impactar en sus sistemas o ambientes y precisan de una acción dentro de un lapso de 12-24 horas de la notificación. Los ejemplos de incidentes de Prioridad 2 incluyen actividades de escaneo local y ataques apuntados a servidores o estaciones de servicio específicos.
  - (3) Incidentes de Prioridad 3: Eventos de bajo riesgo o confiabilidad con el potencial de impactar en sus sistemas o ambientes. Esta categoría de investigación comprende una actividad en una red o servidor que debe investigarse más en un lapso de 1-7 días, aunque no puede accionarse directamente. El escaneo de descubrimiento, las programaciones de recopilación de datos y otros sondeos de reconocimiento se agrupan en esta categoría.

Nota: IBM será el único que pueda determinar si un evento de seguridad se considera un incidente de seguridad o no.

- b. Notificación de alerta de incidentes de seguridad (no disponible durante ningún período en el que el Cliente se suscribió al monitoreo y la notificación de eventos) – Si la notificación de alertas del Sistema de Protección de X-Force fue configurada por usted en el Portal y se generó una alerta, IBM enviará un e-mail de notificación por hora al Contacto de servicios designado, resumiendo las alarmas de AI del sistema de protección X-Force. Este SLA se aplica únicamente al envío inicial de la notificación de alarmas del Sistema de protección X-Force; no a la entrega confirmada al o los receptores finales.

Con el propósito de aclarar, se enviará un e-mail de notificación solamente si se generó una alarma durante la hora anterior.

- c. Notificación de incidentes de seguridad - IBM responderá a todos los incidentes de seguridad identificados en un lapso de 15 minutos desde la implementación, si contrató el servicio opcional agregado de “Monitoreo de eventos y notificación”. IBM iniciará la notificación de todos los incidentes de seguridad identificados en un lapso de 15 minutos de dicha identificación. Se notificará a su Contacto de seguridad autorizado o Contacto de servicios designado por teléfono en caso de incidentes de seguridad de Prioridad 1 y vía e-mail para incidentes de Prioridad 2 y 3. Durante una notificación de incidentes de seguridad de Prioridad 1, IBM continuará tratando de contactar al Contacto de seguridad autorizado o el Contacto de servicios designado hasta que se alcance dicho contacto o se hayan utilizado todos los contactos de notificación.

Las actividades operacionales relacionadas con incidentes de seguridad y respuestas se documentarán y se les realizará el sellado de tiempo en el sistema de tickets con problemas de

IBM. Dicha documentación y sellado de tiempo se utilizarán como la única fuente de información autoritativa para los propósitos de este SLA.

- d. Reconocimiento de solicitudes de cambio de política – IBM reconocerá la recepción de su solicitud de cambios de política en un lapso de dos horas después de la recepción de IBM. El SLA está disponible solamente para solicitudes de cambio de políticas emitidas por un Contacto de seguridad autorizado o un Contacto de servicios designado de conformidad con los procedimientos establecidos y documentados en el Portal.
- e. Implementación de solicitud de cambios de política – IBM implementará sus solicitudes de cambio de política en un lapso de ocho horas después de la recepción, a menos que el pedido haya quedado en estado de “espera” por falta de información necesaria para implementar la solicitud de cambio de política enviada. El SLA está disponible solamente para solicitudes de cambio de políticas emitidas por un Contacto de seguridad autorizado o un Contacto de servicios designado de conformidad con los procedimientos establecidos y documentados en el Portal.
- f. 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.
- g. Actualización de contenidos de seguridad proactivos – IBM comenzará con la aplicación de nuevas actualizaciones de contenido de seguridad en un lapso de 48 horas después de publicada dicha actualización como disponible generalmente por el proveedor aplicable.
- h. Disponibilidad de servicios – IBM brindará 100% de disponibilidad de servicios para los SOC.
- i. 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”.

## 5.2 Recursos de SLA

- a. Recurso de identificación de incidentes de seguridad – Si IBM no cumple con este SLA en un mes calendario particular, se enviará un crédito de la siguiente forma;
  - (1) Incidentes de Prioridad 1: La no identificación del o los eventos de seguridad como incidentes de seguridad resultará en un crédito de un mes para el Agente inicial que reportó el o los eventos.
  - (2) Incidentes de Prioridad 2: La no identificación del o los eventos de seguridad como incidentes de seguridad resultará en un crédito de una semana para el Agente inicial que reportó el o los eventos.
  - (3) Incidentes de Prioridad 3: La no identificación del o los eventos de seguridad como incidentes de seguridad resultará en un crédito de un día para el Agente inicial que reportó el o los eventos.
- b. Notificación de alarma de incidentes de seguridad, notificación de incidentes de seguridad reconocimiento de solicitudes de cambio de política, implementación de solicitudes de cambio de política, monitoreo de sistema proactivo, actualización de contenido de seguridad proactivo, créditos de disponibilidad de servicios y disponibilidad del Portal – Si IBM no cumple con cualquiera de estos SLA, se emitirá un crédito por los cargos aplicables por un día de cargos de monitoreo mensuales para el Agente afectado, por el que no se cumplió con el SLA respectivo.

### **Resumen de los SLA y los Recursos**

Acuerdos de nivel de servicio	Recursos de disponibilidad
Identificación de incidentes de seguridad	Crédito por un mes, una semana, o un día por el Agente inicial que reportó el evento, según lo especificado anteriormente
Notificación de alarma de incidentes de seguridad	Crédito por un día del cargo mensual de monitoreo por el Agente afectado
Notificación de incidentes de seguridad (opcional)	

Reconocimiento de solicitud de cambio de política	
Implementación de solicitud de cambio de política	
Monitoreo de sistema proactivo	
Actualización del contenido de seguridad proactivo	
Disponibilidad de servicios	
Disponibilidad del Portal	