

Servicios de seguridad gestionados por IBM (Computación en la nube)

-

Hosted Security Event and Log Management - Select

Índice

1.	<i>Alcance de los servicios</i>	3
2.	<i>Definiciones</i>	3
3.	<i>Servicios</i>	3
3.1	Centros de operaciones de seguridad	4
3.2	Portal	4
3.3	Contactos de servicio	5
3.4	Inteligencia de seguridad	7
3.5	Implementación y activación	8
3.6	Recopilación y Archivado	13
3.7	Análisis automatizado	15
3.8	Monitoreo de salud y disponibilidad del OA	15
3.9	Gestión de OA	17
3.10	Informes de seguridad	17
4.	<i>Servicios opcionales</i>	18
4.1	Monitoreo y notificación de eventos	18
4.2	Acceso fuera de banda	19
4.3	Integración del sistema de Tickets	20
4.4.	Entrega de eventos y logs de seguridad	20
5.	<i>Acuerdos de nivel de servicio</i>	21
5.1	Disponibilidad de SLA	21
5.2	Recursos de SLA	22

Descripción de Servicios

Servicios de seguridad gestionados por IBM (Computación en la nube) - Hosted Security Event and Log Management - Select

1. Alcance de los servicios

Los servicios de seguridad gestionados por IBM (Computación en la nube) - Hosted Security Event and Log Management - Select (called "Hosted SELM - Select" or "Services") están diseñados para brindar una solución basada en la Web para la recopilación, consolidación, análisis, correlación, alerta, el análisis de tendencias y el archivado de datos de eventos y logs de seguridad de dispositivos soportados (denominados "Agentes").

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").

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.

sistema de prevención de intrusos ("IPS") – dispositivo de seguridad o aplicación de software de 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.

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

<u>Función de servicio</u>	<u>Métrica o cantidad</u>	<u>Acuerdos de nivel de servicio</u>
<u>Disponibilidad de servicios</u>	<u>100%</u>	<u>Disponibilidad de servicios</u>
<u>Disponibilidad del Portal IBM MSS</u>	<u>99.9%</u>	<u>SLA de disponibilidad del Portal IBM MSS</u>
<u>Contactos de seguridad autorizados</u>	<u>3 usuarios</u>	<u>N/A</u>
<u>Archivado de log/evento</u>	<u>5 Gb/año por cada año del contrato (hasta 7 años)</u>	<u>N/A</u>
<u>Identificación de incidentes de seguridad</u>	<u>100%</u>	<u>Identificación de incidentes de seguridadn</u>
<u>Notificación de alertas de incidentes de seguridadn</u>	<u>60 minutos</u>	<u>SLA de alerta de incidentes de seguridadn</u>
<u>Alertas del agredador en sitio</u>	<u>15 minutos</u>	<u>SLA de monitoreo del sistema</u>
<u>Notificación de incidentes de seguridad (Agregado de servicios opcionales)</u>	<u>15 minutos</u>	<u>SLA de notificación de incidentes de seguridad</u>

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 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 COMERCIALIZACIÓN, 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) conciencia y alerta de inteligencia de seguridad;
 - (2) Información sobre el incidente de seguridad y el ticket de servicios;
 - (3) Iniciación y actualizaciones de tickets y flujo de trabajo;
 - (4) conversación en vivo y colaboración con analistas de SOC;
 - (5) un panel de informes de planillas;
 - (6) acceso a logs y eventos de Agentes archivados y en tiempo real;
 - (7) Autorización para descargar datos de log;
 - (8) capacidades interrogación de log y eventos de seguridad granular; y

- (9) acceso a Materiales educativos de acuerdo con los terminos 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 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 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) Envío de solicitudes de servicios a los SOC;
 - (d) 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;
 - (e) Creación de tickets relacionados con servicios internos y asignación de dichos tickets a usuarios de Portal;
 - (f) análisis, visualizaciones y actualización de tickets relacionados con Servicios;
 - (g) Visualización y edición de detalles de Agentes;
 - (h) Visualización de políticas de agentes (de aplicarse);
 - (i) Creación y edición de listas de observación de vulnerabilidad;
 - (j) El monitoreo de eventos en vivo;
 - (k) Análisis de datos de eventos y log de seguridad;
 - (l) Programación de descargas de datos de log y eventos de seguridad;
 - (m) 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.

Nota: Las actividades de implementación y activación se realizan una vez durante la realización de los servicios. Si decide reemplazar 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, mejoras 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.

Completion Criteria:

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

Deliverable Materials:

Ninguno

Actividad 2 - Requisitos de acceso a la red

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. Dichas reimplementaciones se brindarán a un costo adicional según lo especificado en el Programa.

Completion Criteria:

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

Deliverable Materials:

Documento de Requisitos de acceso a la red

Actividad 3 - Evaluación

El propósito de esta actividad es evaluar su ambiente actual, y sus metas de negocios y tecnología.

Tarea 1 - Reunir datos

IBM:

- a. Le brindará un Punto de Contacto con un formulario de recuperación de datos en el que deberá documentar:
 - (1) Nombres de miembros del equipo, información de contacto, roles y responsabilidades;
 - (2) Requisitos únicos para países y sitios;
 - (3) Su infraestructura de red existente;
 - (4) Servidores críticos;
 - (5) Cantidad y tipo de usuario finales; e
 - (6) Impulsores y/o dependencias comerciales clave que podrían influir en la entrega o los plazos de los Servicios.

Tarea 2 - Evaluar entorno

IBM:

- a. Determinará si la recopilación de datos de agentes se implementará mediante el Agente de inicio de sesión universal ("ULA") o vía SYSLOG; y
- b. Si se aplica, brinde recomendaciones para ajustar la política de un Agente.

Completion Criteria:

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

Deliverable Materials:

Ninguno

Actividad 4 - Implementación del agente de inicio de sesión universal

El ULA es un agente basado en software que se ejecuta en un Agente suscripto a los Servicios, y recopila logs basados en textos. El ULA recopila dichos logs a nivel local del Agente y los envía al agregador en sitio ("OA"). Luego, el OA envía los logs a la infraestructura de IBM para su recopilación, almacenamiento a largo plazo, y visualización en el Portal.

Las funciones básicas del ULA son:

- a. recopilar eventos/logs a nivel local del Agente;
- b. comprimir los datos de eventos/logs;
- c. codificar los datos de eventos/logs; y
- d. Transmitir los eventos/logs de manera segura al OA.

Las principales funciones del ULA son:

- a. Recopilar datos de archivos de texto genéricos;
- e. Recopilar eventos/logs;
- f. Recopilar información del sistema, la cual puede incluir:
 - (1) Versión del sistema operativo ("SO");
 - (2) memoria;
 - (3) CPU;
 - (4) Cuentas de usuario local;
 - (5) Detalles de la interface de red;
 - (6) Procesos en ejecución; y
 - (7) Conexiones de red abiertas;
- g. Realizar transmisión unidireccional de log. La comunicación del OA se realiza por medio de conexiones SSL/TCP-443 de salida;
- h. Restringir mensajes, si está configurado. Esto limita el ancho de banda del ULA al OA, en mensajes por segundo, para preservar el ancho de banda; y

- i. 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.

Tarea 1 - Instalación del ULA

IBM:

- a. Le brindará una lista de Agentes que requieren de la instalación de ULA;
- b. Le brindará instrucciones para descargar el ULA en el Agente mediante un servidor Web configurado en el OA;
- c. Le brindará instrucciones activar la sesión a auditorías/sistema para que el Agente introduzca datos útiles; y
- d. A pedido suyo, y por un costo adicional, le brindará servicios de instalación física del ULA.

Tarea 2 - Configuración del ULA

IBM le brindará instrucciones sobre cómo iniciar sesión al Portal y confirmar al Agente.

Completion Criteria:

Esta actividad estará finalizada cuando IBM le haya presentado una lista de Agentes que requieren de la instalación del ULA.

Deliverable Materials:

Instrucciones para la instalación del ULA

Actividad 5 - Implementación de la recopilación sin agentes

El propósito de esta actividad es facilitar la recopilación de logs sin Agentes cuando no sea técnicamente posible instalar el ULA en un Agente.

IBM le brindará instrucciones para dirigir las secuencias de SYSLOG del Agente al OA.

Completion Criteria:

Esta actividad habrá finalizado cuando IBM le haya brindado instrucciones para dirigir las secuencias de SYSLOG del Agente al OA.

Deliverable Materials:

Instrucciones de configuración de SYSLOG

Actividad 6 - Implementación del Agregador en sitio

El propósito de esta actividad es configurar el OA.

El OA es un dispositivo que debe brindar y que se implementa en su sitio y es gestionado y monitoreado por IBM MSS por un costo adicional, según se especifica en el Programa.

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;
- 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; y

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

Tarea 1 - Configuración del 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 operativo de OA y software de OA brindado por IBM. Dicho respaldo debe estar programado por adelantado para asegurar la disponibilidad de un especialista en implementación de IBM;
- 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 mejoras de hardware requeridas que usted deberá brindar e instalar.

Tarea 2 - Instalación del 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. Confirmaré que la infraestructura de IBM MSS reciba la comunicación del OA.

Completion Criteria:

Esta actividad habrá finalizado cuando el OA quede instalado y configurado, e IBM haya confirmado que la infraestructura de IBM MSS reciba las comunicaciones del OA.

Deliverable Materials:

Ninguno

Actividad 7 - Actividad 5 – 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.

Completion Criteria:

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

Deliverable Materials:

Ninguno

Actividad 8 - Actividad 6 – Activación de servicios

El propósito de esta actividad es activar los Servicios.

IBM:

- a. Asumirá el soporte del Agente;
- b. Configuraré al Agente en “activo”; y
- c. Trasladaré al Agente a los SOC para soporte continuo.

Completion Criteria:

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

Deliverable Materials:

Ninguno

3.5.2 Sus Responsabilidades de Implementación y activación

Actividad 1 - Inicio del proyecto

Usted acuerda:

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

Actividad 2 - Requisitos de acceso a la red

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. Será responsable único por cualquier costo incurrido como resultado del uso de IBM de una VPN de sitio a sitio para conectarse a su red.

Actividad 3 - Evaluación

Tarea 1 - Reunir 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 - Evaluar entorno

Para esta actividad no se le requiere ninguna responsabilidad adicional.

Actividad 4 - Implementación del agente de inicio de sesión universal

Tarea 1 - Instalación del ULA

Usted acuerda:

- a. Descargar el software de ULA del servidor Web alojado en el OA;
- b. Instalar el ULA en uno o más Agentes suscriptos al servicio; y
- c. Y reconocer que es el único responsable por todas las tareas de instalación de ULA.

Tarea 2 - Configuración del ULA

Usted acuerda:

- a. Establecer el ULA con la configuración adecuada y una dirección IP configurada en el OA,
- b. Configurar al Agente de acuerdo con las especificaciones de inicio de sesión de auditoría/sistema recomendadas por IBM (según sea necesario);
- c. Iniciar sesión al Portal y confirmar al Agente en tres días hábiles después de la instalación y configuración de ULA; y
- d. Y reconocer que es el único responsable por todas las tareas de configuración de ULA.

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

Actividad 5 - Implementación de la recopilación sin agentes

Usted acuerda:

- a. configurar al Agente para marcar secuencias de SYSLOG al OA bajo la guía de IBM; y
- b. Iniciar sesión al Portal y confirmar al Agent en tres días hábiles.

Actividad 6 - Implementación del Agregador en sitio

Tarea 1 - Configuración del OA

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. Mantener las licencias actuales y los contratos de soporte y mantenimiento por el hardware en el que el OA se encuentra instalado;
- d. Instalar el software de OA brindado por IBM en el hardware que se le entregó, guiado por IBM;
- e. Configurar una dirección de IP externa junto con la configuración de OA relacionada;
- f. 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
- g. En el caso de plataformas existentes, obtener e instalar las mejoras de hardware solicitadas por IBM

Tarea 2 - Instalación del OA

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.

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

Actividad 7 - Actividad 5 – 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 8 - Actividad 6 – 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).

Los Servicios brindan hasta cinco Gb de almacenamiento por cada año del término del contrato. En el primer día del contrato, IBM hará disponible todo el espacio de almacenamiento según el término del contrato (5 Gb x n en el que "n" equivale al término del contrato). Por un costo adicional, se puede adquirir espacio de almacenamiento adicional especificado en el Programa.

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 almacenamiento por hasta cinco Gb de datos de logs y eventos por cada año del término del contrato;
- 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 de primero en entrar, primero en salir ("FIFO"):
 - (1) Según los períodos de retención que usted definió;
 - (2) Cuando se excede su espacio de almacenamiento; o
 - (3) 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.

3.6.2 Sus Responsabilidades de Recopilación y Archivado

Usted acuerda:

- a. Brindarle a IBM los períodos de retención de eventos y logs de seguridad para no exceder los cinco Gb de almacenamiento por cada año del término del contrato;
- 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. Asegurarse de que se conserve un contrato activo de MSS para la Gestión de eventos y logs de seguridad – Select por cada evento de seguridad único y fuente de log;
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) Todos los datos de log y eventos se transmitirán a los SOC por Internet;
 - (2) El viaje de datos en Internet se codifica con algoritmos de codificación específica estándares en la industria siempre que sea posible;
 - (3) IBM solo puede recopilar y archivar datos de log y eventos que lleguen con éxito a la infraestructura de IBM MSS;
 - (4) 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;

- (5) IBM tiene el derecho de restringir flujos de eventos generados por el Agente que excedan los 100 EPS (de ser requerido);
- (6) ;
- (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 [“Sacudos 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 Monitoreo de salud y disponibilidad del OA

IBM monitoreará el estado de salud y la disponibilidad del OA. Dicho monitoreo está diseñado para asistir en la cada vez mayor disponibilidad y tiempo de actividad del OA.

3.8.1 Responsabilidades de monitoreo de salud y disponibilidad de IBM

Actividad 1 - Monitoreo basado en Agentes

El propósito de esta actividad es monitorear la salud y el rendimiento del OA.

IBM:

- a. instalará software de monitoreo en el OA;
- 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 el OA no se desempeña 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 OA o un posible problema en la salud del OA;
- b. Comenzará estudiando e investigando los problemas documentados;
- c. Si se identifica al OA como posible fuente de un problema relacionado con la red, examinará la configuración y funcionalidad del OA por posibles problemas; y
- d. Desplegará la salud del OA y el ticket de parada en el Portal.

Actividad 3 - Notificación

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

IBM:

- a. Lo notificará si el OA 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 OA, después de la iniciación de notificación telefónica; y
- c. desplegará la salud del OA y los tickets de parada en el Portal.

3.8.2 Sus Responsabilidades de monitoreo de salud y disponibilidad

Actividad 1 - Monitoreo basado en Agentes

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 OOB, o si la solución OOB no está disponible por alguna razón
- c. reconocer que si se elimina a un OA 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.

3.9 Gestión de OA

IBM actualizará las aplicaciones y la seguridad del OA.

3.9.1 Responsabilidades de gestión del OA de IBM

IBM:

- a. Será el único proveedor de gestión a nivel de software para el OA;
- b. Conservará información sobre el estado del sistema;
- c. Instalará nuevas actualizaciones del contenido de aplicaciones y seguridad en el OA, a medida que se hacen disponibles;
- d. instalará parches y actualizaciones de software para mejorar el rendimiento, permitir una funcionalidad adicional, o resolver un problemas de aplicación;
- e. Declarará por adelantado una ventana de mantenimiento de actualizaciones del OA 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 de un mantenimiento programado en el OA y sus requisitos específicos.

3.9.2 Sus Responsabilidades de gestión del OA

Usted acuerda:

- a. Realizar mejoras especificadas por IBM en el hardware para soportar al software y firmware actuales;
- b. Trabajar con IBM para realizar actualizaciones del OA (según se requiera);
- c. Ser responsable de todos los cargos relacionados con las mejoras 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 mejoras de software solicitadas por IBM puede resultar en la suspensión de entrega de servicios y/o SLA; y
 - (4) El no cumplimiento con las mejoras de hardware solicitadas por IBM puede resultar en la suspensión de entrega de servicios y/o SLA.

3.10 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.

3.10.1 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 sensores IDS/IPS que incluyen métricas de ataque, ataques evitados, impacto de vulnerabilidad, conteos/tendencias de eventos;
- f. Correlación y análisis de eventos (según se aplique); y
- g. Informes de firewall que incluyen resumen, análisis de tráfico, uso de protocolo y uso de IP específico y reglas (según se aplique).

3.10.2 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

Durante cualquier período en el que se haya suscripto al Monitoreo y notificación de eventos, y por un costo adicional especificado en un Programa, IBM:

- a. Lo notificará vía e-mail al comenzar y finalizar la ventana de monitoreo y notificación de eventos que le hace saber que el monitoreo ha comenzado/finalizado;
- b. 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;
- c. Realizará una investigación y análisis de alarmas de AI;
- d. Le solicitará que implemente la modificación a la configuración IDS/IPS del agente, si la política actual no permite que el SOC procese datos de eventos satisfactoriamente;
- e. Cuando sea posible, eliminará los positivos falsos y disparadores benignos y los clasificará como incidentes de seguridad comentados ("CSI");
- f. 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;
- g. 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

[servicios](#)”, “Notificación de incidentes de seguridad”;

- h. Brindará recomendaciones de recursos/contramedidas, si corresponde;
- i. Documentará detalles de CSIs y SIs en el sistema de tickets de IBM; y
- j. Las investigaciones que resultan en una clasificación de alta prioridad (i.e., Prioridad 1) requieren de una acción defensiva inmediata.

4.1.2 Sus Responsabilidades de notificación y monitoreo de eventos

Usted acuerda:

- a. Utilizar el Portal para programar el monitoreo y la notificación de eventos;
- b. Implementar los cambios de políticas del pedido de MSS al Agente con anterioridad al siguiente período de monitoreo;
- c. Utilizar el Portal para investigar eventos de auditoría o eventos continuos no considerados como amenazas inmediatas;
- d. Brindarle a IBM documentación global actual de su entorno;
- e. Actualizar a IBM dentro de los tres días calendario de cambios dentro de su ambiente;
- f. 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) Escaners autorizados;
- g. Brindar y mantener actual una ruta de notificación de contacto lineal, incluidos los números de teléfono y direcciones de e-mail;
- h. actualizar a IBM, mediante el Portal, en un lapso de tres días calendario si existe un cambio en su información de contacto;
- i. Brindar alias de e-mail, según sea necesario, para facilitar la notificación;
- j. 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;
- k. Visualizar detalles de los CSI y SIs mediante el Portal;
- l. Trabajar con IBM para optimizar IBM el servicio de monitoreo;
- m. Brindar retroalimentación de los CSI y SIs mediante el Portal;
- n. 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;
 - (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; y
 - (5) Si no realiza las modificaciones de política solicitadas antes del siguiente período de monitoreo, el SLA de Notificación de incidentes de seguridad establecido en la sección de esta Descripción de servicios titulada “Acuerdos de nivel de servicios” será nula;

4.2 Acceso fuera de banda

El acceso OOB es una función muy recomendada que asiste a los SOC si se pierde la conectividad al OA. Si se dan dichos problemas de conectividad, los analistas del SOC pueden discar en el módem

para verificar si el OA está funcionando adecuadamente para determinar la fuente de la parada antes de que le llegue a usted.

4.2.1 Responsabilidad de acceso fuera de banda de IBM

A pedido suyo, sin costo adicional, IBM:

- a. 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;
- b. Configuraré el dispositivo OOB para acceder al OA; o
- c. Trabjará de buena fe con usted para utilizar una solución OOB existente aprobada por IBM.

4.2.2 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 OA;
 - (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 al OA gestionado; 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

4.3 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.

4.3.1 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.

4.3.2 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.

4.4. 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.

4.4.1 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.

4.4.2 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 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”.

- 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. Si no realiza las modificaciones de política solicitadas antes del siguiente período de monitoreo, el SLA de Notificación de incidentes de seguridad establecido en la sección de esta Descripción de servicios titulada “Acuerdos de nivel de servicios” será nula; Este SLA se aplica únicamente al

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 incidente de seguridad (disponible durante cualquier período en el que se suscribió para el monitoreo y notificación de eventos) – Durante el período de monitoreo de SOC, IBM comenzará la notificación de todos los incidentes de seguridad identificados dentro de los 15 minutos de dicha notificación. 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. Monitoreo proactivo de sistemas – IBM lo notificará en un lapso de 15 minutos después de determinar que su OA es inalcanzable mediante la conectividad en banda estándar.
- e. Disponibilidad de servicios – IBM brindará 100% de disponibilidad de servicios para los SOC.
- f. 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 alertas de incidentes de seguridad, notificación de incidentes de seguridad, monitoreo de sistema 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

<u>Acuerdos de nivel de servicio</u>	<u>Recursos de disponibilidad</u>
<u>Identificación de incidentes de seguridad</u>	<u>Crédito por un mes, una semana, o un día por el Agente inicial que reportó el evento, según lo especificado anteriormente</u>
<u>Monitoreo de sistema proactivo</u>	<u>Crédito por un día del cargo mensual de monitoreo por el OA afectado</u>
<u>Notificación de alarma de incidentes de seguridad</u>	
<u>Notificación de incidentes de seguridad</u>	<u>Crédito por un día del cargo mensual de monitoreo por el Agente afectado</u>
<u>Disponibilidad de servicios</u>	
<u>Disponibilidad del Portal</u>	