ISO
9001:2015 | 27001:2013
20000-1:2018
37001:2016

P-SGI-025

Aprovisionamiento y gestión de servicios

Clave del formato de proceso
F-SGI-001

sgi@silent4business.com

Insurgentes Sur #2453, Piso 4, Col, Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

Responsables

Elaboró:	Soporte Técnico
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	24/01/2020	Emisión inicial.
2	07/04/2022	Revisión anual sin actualizaciones
3	23/08/2022	Actualización de formato y revisión general del documento

Contenido

1. Objetivo del proceso

Establecer las actividades para el despliegue y gestión en la provisión de servicios, considerando el aprovisionamiento inicial, afinación inicial de los servicios prestados y afinación continua de los servicios prestados por el SOC.

2. Alcance

El proceso aplica para la provisión de servicios de seguridad y redes a clientes por parte de Silent4business, considerando las fases de aprovisionamiento, instalación y servicios administrados.

3. Diagrama del proceso

No aplica.

4. Descripción de Actividades

4.1 De aprovisionamiento inicial

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Validación de especificaciones.	Líder Operación SOC/NOC	a) Verificación de correspondencia entre los equipos ofertados y los equipos entregados por los fabricantes. b) Signoff de visto bueno para entrega al cliente	No aplica
2.	Plan de logística de entrega	Líder de Entrega de Servicio	a) Reuniones con personal responsable del proyecto por parte de EL CLIENTE para conocer los términos y tramitología relacionada con la entrega de equipamiento. b) Generación de plan para la logística de entrega. c) Formalización de criterios de recepción de soluciones entre el cliente y Silent4Business	No aplica
3.	Desarrollo y Validación del plan por la EL CLIENTE	Líder de Entrega de Servicio	a) Desarrollo del plan de implementación por parte de Silent4Business. b) Presentación del plan al (los) responsable(s) del proyecto por parte de Cliente.	

			c) Validación del plan por parte de EL CLIENTE. d) Asignación de tareas, contrapartes y responsables tanto de SILENT4BUSINESS como de EL CLIENTE.	No aplica
4.	Aprovisionamiento de equipo.	Líder de Entrega de Servicio	a) Ejecución de tramitología para la entrega de equipo. b) Entrega del equipamiento a los sitios designados por EL CLIENTE. c) Recopilación y gestión de documentación de entrega de equipo. d) Entrega a EL CLIENTE de la documentación de entrega de equipo. e) Liberación de entrega Entregables de la etapa de Aprovisionamiento: Plan de logística de aprovisionamiento. El cual incluye: Documentación de entrega de equipo.	No aplica
Fin del procedimiento				

4.2 Instalación del servicio

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Interacción de mesas de trabajo	Líder de Entrega de Servicio /Gerente de Operaciones	a) Sesiones de trabajo con EL CLIENTE y con los líderes del proyecto por parte de EL SILENT4BUSINESS. b) Entrega de requerimientos y de información por parte de SILENT4BUSINESShacia EL CLIENTE para poder concretar la definición de actividades de implementación con base a los requerimientos específicos de EL CLIENTE. c) Recepción y revisión de información complementaria para entendimiento y contextualización de SILENT4BUSINESSsobre cada uno de los servicios solicitados por EL CLIENTE en la presente licitación. Incluyendo:	

			• Revisión de documentación sobre el sitio en donde será implementada cada solución (diagramas de red, segmentación, direccionamiento IP, protocolos, aplicaciones críticas, componentes de seguridad, etc.). • Conocer los procesos internos de EL CLIENTE asociados al despliegue de los servicios. • Políticas y normatividad que todos los integrantes del personal de SILENT4BUSINESS deberán observar y cumplir durante el desarrollo de sus actividades para este proyecto. Incluyendo horarios, trámites de acceso, códigos de conducta, códigos de vestimenta, códigos o reglamentos de protección civil, entre otros. • Tramitología necesaria para la instalación del equipamiento y despliegue de los servicios. d) Revisión de requerimientos particulares para cada servicio. e) En caso de requerirse, se realizarán visitas físicas a los sitios donde se implementará cada solución tecnológica. f) Especificación de requerimientos hacia EL CLIENTE, para una instalación exitosa y libre de problemas. g) Definición de batería de pruebas de funcionalidad para garantizar que el objetivo de la instalación fue alcanzado. h) Definición de criterios de aceptación y liberación de los trabajos de instalación. i) Definición de planes de comunicación, matrices y mecanismos de escalación.	
2.	Definición de estrategia de instalación.	Líder de Operaciones SOC/NOC /Gerente de Operaciones	A) Diseño detallado de la implementación de la solución tecnológica para cada servicio de EL CLIENTE. Incluyendo líneas base de configuración que cumplan con los objetivos del servicio, las funcionalidades	

			ofertadas, la normatividad aplicable y los requerimientos de niveles de servicio que le apliquen a la solución tecnológica. b) Definición de ruta crítica para la programación de la instalación de cada una de las soluciones y cada uno de los sitios en que serán instalados, de manera que se mantenga el orden y la consistencia en todas las tareas de instalación. c) Generación del plan de trabajo y logística detallada de la implementación.	
3.	Validación de estrategia	Gerente de Operaciones	Una vez que la estrategia de instalación está definida y documentada, EL CLIENTE procederá a la revisión y validación de esta. a) Validación del diseño detallado de la implementación de la solución tecnológica para cada servicio y para cada sitio de EL CLIENTE. b) Validación de la ruta crítica para la programación de la instalación de cada una de las soluciones y cada uno de los sitios en que serán instalados. c) Validación del plan de trabajo y logística detallada de la implementación.	
4.	Instalación, configuración y puesta a punto	Líder Operación SOC/NOC	Las actividades de implementación de la arquitectura tecnológica definida contemplan la instalación física, el aseguramiento y configuración de las tecnologías propuestas, su puesta a punto, pruebas, documentación y liberación a producción. 1.Instalación física. a) Cumplimiento (con apoyo de la EL CLIENTE) de la tramitología relacionada, incluyendo: •Trámites de acceso.	

			•Trámites de acuerdo con procesos de control de cambios, liberaciones, o similares que se encuentren vigentes de acuerdo a la normatividad de EL CLIENTE. •Sujeción, energización y validación de funcionamiento de PDUs. •Inserción del rack en el esquema de cableado de voz y datos del sitio que corresponda. b) Sujeción de los equipos en rack. c) Energización y pruebas de validación de funcionalidades físicas. d) Definición del plan de conectividad y revisión del cableado (ya sea aprovisionado por SILENT4BUSINESSo por EL CLIENTE, según sea el caso). e) Habiltación de patch panels. f) Organización del cableado. g) Documentación de la ubicación, conexiones y consumos. 2. Configuración física y lógica. a) Habilitación de interfaces (de todo tipo). b) Conexión de interfaces de red para conectividad y/o administración. Esto se hace de acuerdo con el plan para conexiones de red, direccionamientos y conectividad en general. c) Configuración de almacenamiento masivo (particiones, unidades lógicas, volúmenes, entre otras). d) Configuración de tarjetas y dispositivos periféricos. e) Preparación de la configuración lógica del equipo: • Análisis de impactos y riesgos sobre las configuraciones propuestas. • Revisión y endurecimiento del equipo propuesto (Hardening, de acuerdo con el análisis de impacto y líneas base definidas). • Configuración de forma segura de sus componentes (Sistema, Contraseñas y servicios asociados).	

			• Modificación de parámetros por omisión. • Aplicación de últimos parches y/o actualizaciones (De acuerdo con el análisis de impacto y líneas base definidas). • Configuración de parámetros y variables de ambiente (De acuerdo con el análisis de impacto y líneas base definidas). f) Configuración de la solución tecnológica de acuerdo con las líneas base definidas y los cambios que apliquen de acuerdo con el análisis de impactos y riesgos. g) Configuración y Afinación de políticas de seguridad (reglas o filtros), o bien configuraciones de red, funcionalidades o módulos ofertados en cada servicio. h) Pruebas de conectividad hacia el Centro de Operaciones de EL SILENT4BUSINESS a través de los medios definidos en mesas de trabajo. i) Configuración e integración con las diferentes consolas de monitoreo y gestión. j) Puesta a punto de la consola de administración centralizada para que la infraestructura recién instalada pueda ser gestionada desde nuestro Centro de Operaciones y tomen efecto desde el inicio de las operaciones de monitoreo y administración. 3. Pruebas de funcionalidad de la solución y aceptación de los servicios en producción. a) Se probará de forma integral el correcto funcionamiento de la solución tecnológica, así como la NO afectación negativa de los servicios y/o aplicaciones de cada sitio. Todo esto se realizará de acuerdo con lo definido en las mesas de trabajo para la etapa de definición de estrategia de instalación.	

			b) Se dará la aceptación de los servicios al validar y cumplir con los criterios de aceptación definidos en mesas de trabajo de la etapa de definición de estrategia de instalación. c) Se proporcionarán los accesos de "solo lectura" al personal designado por EL CLIENTE, de acuerdo con lo definido en términos de referencia para cada servicio. Entregables de la etapa de Instalación i. Memoria Técnica Actualizada de la solución tecnológica, incluyendo: ii. Diagrama actualizado de red, incluyendo la información del(los) equipo(s) instalado(s) a detalle (localidad, direcciones IP, equipamiento, etc). iii. Descripción de configuración física y lógica del equipo instalado. iv. Matriz de escalación para atención a fallas y/o incidentes. v. Procedimiento de Help Desk (para problemas y requerimientos). vi. Protocolo de pruebas firmadas por el(los) responsable(s) por parte de la EL CLIENTE, que este último designe. Las actividades antes mencionadas se estarán aplicando para el ingreso de los equipos Data colector en las instalaciones de EL CLIENTE (Corporativo y/o Centro de Datos).	
Fin del procedimiento				

4.3 Servicios Administrativos

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Líder Operación SOC/NOC	Aprovisionamiento de enlaces EL SILENT4BUSINESS - EL CLIENTE	1. Para llevar a cabo las tareas de monitoreo y soporte, el SOC contará con un enlace de datos (RPV-MPLS), así como todo el equipamiento necesario, hacia alguna parte de la red corporativa de EL CLIENTE, con el fin de estar integrado de alguna manera al backbone de datos donde pueda tener acceso únicamente a la información generada por los equipos que serán monitoreados. Para ellos EL SILENT4BUSINESS realizará lo siguiente: a) Revisión de documentación sobre el sitio en donde se adecuará en el enlace de datos. EL CLIENTE deberá proporcionar las facilidades para la instalación, configuración y adecuación del enlace en sus instalaciones. b) Configuración de los ruteadores que conforman el enlace de datos, aplicando para ambos sitios EL SILENT4BUSINESS - EL CLIENTE. c) Validación de comunicación entre EL CLIENTE y EL SILENT4BUSINESS, revisando que la información de prueba fluya de un sitio a otro dentro de los umbrales solicitados por EL CLIENTE para el cumplimiento de disponibilidad, desempeño, latencia y pérdida de paquetes. d) EL SILENT4BUSINESS proporcionará una solución de seguridad, compuesta por Firewalls perimetrales para la protección de la información que fluye entre el centro de operaciones SOC y EL CLIENTE. e) EL SILENT4BUSINESS habilitará la comunicación con la red de EL CLIENTE por medio del Servicio Administrado de Red Privada Virtual (RPV-MPLS) con	

			el que cuenta actualmente la convocante, para el cifrado de la comunicación se estará definiendo en conjunto con el proveedor de la RPV-MPLS conforme a las características soportadas en la topología actual, de forma inicial se propone un cifrado del tipo IPSEC.	
2.	Líder Operación SOC/NOC	Afinación de infraestructura	Al inicio de las actividades de arranque del centro de operaciones SOC, se hace un levantamiento del inventario de equipos y sus respectivas configuraciones para contar con todo el detalle necesario para el diagnóstico de fallas. b) Se realiza la activación y configuración de comunidades SNMP para la comunicación con la herramienta de monitoreo del SOC. c) Se hace una revisión de diagramas y arquitectura, y al mismo tiempo se identifica como se integra cada una de la tecnología a los servicios críticos de EL CLIENTE. d) Se hace levantamiento de información de servicios e infraestructura para el levantamiento de tickets con terceros en caso de existir. e) Adecuación preparación de la infraestructura dentro del SOC tales como: i. Sistemas de levantamiento de incidentes. ii. teléfono: 55 7823 3000 para el levantamiento de ticktes, incidentes y cambios, requerimientos, etc. f) Se realiza la preparación de la infraestructura de monitoreo del centro de Operaciones, especificando los parámetros de monitoreo, según aplique para cada servicio particular: • Tiempos de poleo. • Comunidades SNMP. • Recolecciones de datos.	

			• Recolección de log. g) Activación de dispositivos en consolas de monitoreo, se realizan pruebas de conectividad entre las consolas de monitoreo y los dispositivos que serán parte del alcance de monitoreo y soporte. • Arranque de métricas para niveles de servicio. a) Adecuación y afinación de los SLAs (Niveles de Servicio) requeridos EL CLIENTE b) Revisión y afinación de la infraestructura tecnológica para cumplir con los niveles de servicio establecidos. • Adecuación de Proceso de atención. a) Adecuación de los procedimientos de atención. b) Los procedimientos de atención que entregamos son: • Procedimiento de levantamiento y cierre de tickets • Procedimiento de atención a eventos de soporte • Procedimiento de atención a solicitudes de requerimientos • Procedimiento de notificación c) Se personalizan los procedimientos de acuerdo con los requerimientos de EL CLIENTE, tomando en cuenta las matrices de escalación que se definan en los niveles de servicio, la interacción del SOC-NOC con EL CLIENTE, o de un tercero.	
Fin del procedimiento				

4.4 Operación Continua.

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Monitoreo	Operación (SOC/NOC)	Para llevar a cabo las tareas de monitoreo y soporte, el SOC contará con un enlace de datos (RPV-MPLS), así como todo el equipamiento necesario, hacia alguna parte de la red corporativa de EL CLIENTE, con el fin de estar integrado de alguna manera al backbone de datos donde pueda tener acceso únicamente a la información generada por los equipos que serán monitoreados. Para ellos EL SILENT4BUSINESS realizará lo siguiente: Revisión de documentación sobre el sitio en donde se adecuará en el enlace de datos. EL CLIENTE deberá proporcionar las facilidades para la instalación, configuración y adecuación del enlace en sus instalaciones. b) Configuración de los ruteadores que conforman el enlace de datos, aplicando para ambos sitios EL SILENT4BUSINESS - EL CLIENTE. c) Validación de comunicación entre EL CLIENTE y EL SILENT4BUSINESS, revisando que la información de prueba fluya de un sitio a otro dentro de los umbrales solicitados por EL CLIENTE para el cumplimiento de disponibilidad, desempeño, latencia y pérdida de paquetes. d) EL SILENT4BUSINESS proporcionará una solución de seguridad, compuesta por Firewalls perimetrales para la protección de la información que fluye entre el centro de operaciones SOC y EL CLIENTE.	

			e) EL SILENT4BUSINESS habilitará la comunicación con la red de EL CLIENTE por medio del Servicio Administrado de Red Privada Virtual (RPV-MPLS) con el que cuenta actualmente la convocante, para el cifrado de la comunicación se estará definiendo en conjunto con el proveedor de la RPV-MPLS conforme a las características soportadas en la topología actual, de forma inicial se propone un cifrado del tipo IPSEC.	
2.	Administración de la seguridad	Operación (SOC/NOC)	1. Control y administración de cambios, esta actividad tiene como objetivo la reconfiguración del software de los equipos, que son los filtros y/o reglas de los dispositivos de seguridad. Este procedimiento se ejecuta cada vez que es necesario, ya sea por un requerimiento del cliente o debido a una eventualidad que implica cambios inmediatos en configuraciones. 2. El control de cambios tiene el propósito de agregar, remover o modificar debidamente todas las partes de configuraciones que lo necesiten con el fin de permitir el flujo adecuado de las aplicaciones del negocio, y bloquear toda aquella actividad o flujo ajeno o perjudicial para el mismo. Todo cambio realizado es debidamente documentado para su posterior consulta y así mantener una base o memoria técnica actualizada al día de las configuraciones que se tienen en los dispositivos. Esta documentación contiene los cambios que se han realizado y el por qué de cada uno, las personas implicadas, fechas, horas, etc. Los	

			cambios pueden ser de dos tipos: Inmediatos por un incidente, ataque o requerimiento urgente que así lo amerite; y los cambios programados para que durante una ventana de tiempo acordada en conjunto con el cliente, se lleven a cabo todos los cambios establecidos en el requerimiento, previo análisis de impacto. El número de cambios es ilimitado durante la duración del contrato. •Administración de Configuraciones, permite mantener la base de datos de configuraciones (CMDB) de todos los elementos involucrados en la operación del SOC, así como de proveer información a las demás funciones sobre dichos elementos para su correcta ejecución.	
3.	Notificación de alertas	Operación (SOC/NOC)	1. Si los valores monitoreados rebasan alguno de los umbrales predefinidos, entonces se dispara una notificación hacia los administradores responsables de los sistemas afectados para que tomen las acciones necesarias. • En forma continua, un grupo de especialistas de SILENT4BUSINESS está monitoreando los principales sitios de Internet que notifican sobre nuevas vulnerabilidades y la liberación de nuevos virus y sus variantes. Cuando se detecta una nueva vulnerabilidad o virus, se realiza un análisis para conocer si afectará el ambiente de EL CLIENTE, y si es viable, realizar cambios a las configuraciones (incluyendo parches) o definir soluciones alternas, y hacer la notificación al personal adecuado de EL CLIENTE.	

4.	Manejo de Incidentes	Líder Operación SOC/NOC	1. Dentro del Manejo de Incidentes tenemos varios procesos que tienen por objetivo el evitar de manera proactiva, rápida y eficiente que una actividad sospechosa pueda causar algún impacto a los activos de la EL CLIENTE. A continuación, se enlistan estos procesos: Identificación, el principal objetivo de este procedimiento es el de llevar a cabo la comparación de los eventos registrados contra un patrón de incidentes ya establecido para confirmar la existencia o no de una actividad sospechosa como incidente. La importancia de este procedimiento radica en evitar: i. El no poder determinar la extensión y daño ocasionado por el incidente. ii. La utilización de la infraestructura tecnológica para generar ataques o daños en contra de otros sistemas de otras organizaciones. iii. La pérdida de oportunidades de negocio en conjunto con la pérdida de reputación. • Contención Inicial, el objetivo de este procedimiento es el de llevar a cabo las acciones iníciales necesarias para limitar el alcance e impacto de la actividad sospechosa / incidente. La contención consiste en la aplicación de tácticas, definidas en el corto plazo, para detener el acceso del intruso al dispositivo violado, limitar la extensión del incidente y prevenir daños adicionales y futuros que pudiera causar el atacante.	

			• Recuperación de los sistemas de Seguridad, el objetivo de este procedimiento es verificar que se lleven a cabo las acciones necesarias para el restablecimiento de la operación de los servicios de seguridad perimetral de los dispositivos contratados, es decir, garantizar que los servicios de seguridad implicados en la administración del SOC que hayan sido afectados (en caso de ser así) por un incidente, operen de manera similar a como lo venían haciendo hasta antes del incidente y continúen ofreciendo la seguridad dentro del perímetro contratado. Dentro de las principales actividades de este procedimiento están las de verificar todas aquellas tareas de contención realizadas para disminuir o detener el impacto del incidente ocurrido para que los dispositivos regresen a su operación normal. Toda esta tarea se realiza en caso de haber: i. Pérdida de configuraciones de los dispositivos / elementos de seguridad, se llevará a cabo la restauración de las mismas a partir de los respaldos realizados con anterioridad. ii. Desconexión o desconectado de equipos, se llevará a cabo la conexión de los mismos. iii. Baja de servicios, se procede a darlos de alta nuevamente. iv. Ejecución de cambios temporales, a través de la ejecución del proceso de "rollback" de los mismos. • Seguimiento, el objetivo de esta fase es apoyar en la ejecución de	

			los procedimientos que conforman a las siguientes fases: i. Detección ii. Respuesta iii. Mejora Continua El objetivo del procedimiento de seguimiento es garantizar el correcto flujo del proceso de manejo de incidentes, facilitando y verificando que el proceso avanza de manera óptima y sin contratiempos. Y en el caso que exista un cuello de botella o un problema durante un incidente, reportarlo y garantizar que se tomen las líneas de acción necesarias para resolverlo. • Documentación, se refiere a registrar y documentar las actividades realizadas para mitigar y contener el impacto a lo largo del proceso de manejo de incidentes, garantizando así el contar con las lecciones aprendidas de los eventos ocurridos. Las características de los reportes son las siguientes: i. Fecha y hora del incidente ii. Tiempo de duración iii. Naturaleza / Origen del Problema iv. Vulnerabilidad o Método Explotado para dar origen al Incidente v. IP Origen vi. Equipos Afectados vii. Descripción del Incidente viii. Fecha y Hora de la última modificación / actualización sobre el equipo / sistema	
5.	Servicios recurrentes y de soporte	Líder Operación SOC/NOC	1. Actualización de Software de seguridad, incluye la incorporación de nuevas versiones, fixes, parches al equipo	

			que vaya liberando el fabricante, previo análisis de impacto. Actualización de Memoria Técnica, EL SILENT4BUSINESS realizará la actualización de la memoria técnica de los dispositivos de seguridad cada vez que exista un cambio y será entregada a EL CLIENTE de acuerdo con lo requerido en términos de referencia. Respaldo de configuraciones, el SOC hará respaldo de configuraciones a los dispositivos de seguridad bajo contrato. La periodicidad del respaldo se realizará de acuerdo con las necesidades y requerimientos de cada servicio. Soporte Técnico (Help Desk), EL SILENT4BUSINESS cuenta con una Mesa de Ayuda que se encuentra regida por procesos adaptados y mejores prácticas como lo es ITIL para brindar toda la ayuda necesaria para EL CLIENTE. Esta mesa de ayuda se encuentra establecida en un esquema 7x24x365 con equipos de ingenieros capacitados y experimentados que apoyarán en los requerimientos solicitados. La mesa de ayuda como punto único de contacto entre EL SILENT4BUSINESS y EL CLIENTE tiene entre sus actividades realiza lo siguiente: i. Atención telefónica para asesoría, dudas y/o levantamiento de requerimientos. ii. Análisis y canalización de requerimientos iii. Soporte 1er y 2do nivel telefónico y primeros diagnósticos	

			iv. Asignación de ingenieros a sitio en caso de ser necesario v. Asesoría ante dudas y requerimientos acerca del proyecto. vi. Levantamiento, seguimiento, cierre y verificación de tickets. El servicio de soporte técnico es permanente durante todo el contrato de administración desde el SOC-NOC, cualquier día y en cualquier horario. Ante una falla nuestros ingenieros capacitados apoyan todas las actividades para restablecer o corregir el servicio o elemento de seguridad a su actividad normal. Dentro del soporte se tienen actividades como: i. Soporte de los Fabricantes ii. Procedimientos para soporte y Matriz de escalación Para el monitoreo de los dispositivos EL SILENT4BUSINESS cuenta con un sistema de monitoreo licenciado (PRTG) el cual permite conocer en tiempo real la disponibilidad, estado de salud, el uso de los recursos y su capacidad permitiendo detectar comportamientos de forma anticipada conforme a los datos históricos almacenados. 1. El monitoreo de la disponibilidad de la infraestructura se enfoca a vigilar que los elementos estén funcionando (activos y operando normalmente), en caso de que algún dispositivo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio en conjunto con el	

			cliente para reactivar y/o restaurar el servicio lo antes posible a cómo funcionaba antes de la falla o eventualidad. Adicional al monitoreo de la disponibilidad EL SILENT4BUSINESS ejecutara el monitoreo de los dispositivos respecto a la utilización de los recursos y su desempeño. De esta forma, se están monitoreando variables dentro del dispositivo como nivel de utilización (canal, CPU, disco, memoria), que determinan el rendimiento del elemento o dispositivo. Si los valores monitoreados rebasan alguno de los umbrales predefinidos, entonces se dispara una notificación vía correo hacia los administradores del sistema en cuestión, ya sea dentro del mismo SOC y/o al cliente, para que tomen las acciones necesarias. Dentro de este monitoreo se determinan los parámetros siguientes: Disponibilidad de Equipos. Pérdida de Paquetes. Latencia. Tiempo de respuesta y carga de páginas web Desempeño de Equipos: Uso y carga de CPU, uso y disponibilidad de RAM, espacio en disco duro. Ancho de banda: utilización de entrada y salida de las interfaces monitoreadas. Disponibilidad de servicios: Aplicativos publicados por diferentes protocolos/Puertos (http, https, FTP, POP, IMAP, SMTP etc). Estado del hardware.	

			En caso de presentarse fallas de monitoreo en los dispositivos y con el fin de verificar su estado y tomar las acciones necesarias se proporcionará el seguimiento correspondiente hasta su resolución, las siguientes actividades describen las acciones a ejecutar por parte del SOC: Recepción continua de alarmas y alertas a través de SNMP traps por medio de la herramienta de monitoreo PRTG. Detección, registro, aislamiento y seguimiento de eventos. Notificación y escalamiento (de acuerdo con SLA's y procedimientos definidos previamente). SILENT4BUSINESS realiza un monitoreo proactivo el cual permite el análisis de los mismo basado en los umbrales definidos minimiza las ocurrencias de caídas y/o degradaciones del servicio, las siguientes actividades describen las acciones a ejecutar por parte del SOC: Monitoreo de desempeño de los dispositivos a través de SNMP traps por medio de la herramienta de monitoreo PRTG. Registro proactivo de eventos al detectarse alguna excepción en el comportamiento de la infraestructura monitoreada o con base en la tendencia, es decir, aunque no se rebase un umbral con el respectivo seguimiento. La plataforma de monitoreo PRTG se encontrará en las instalaciones de EL SILENT4BUSINESS realizando el monitoreo remoto por medio de la RPV-MPLS entre las	

			instalaciones del SOC y EL CLIENTE. Los umbrales de monitoreo se estarán definiendo en conjunto conforme a las necesidades de la operación como mejor practica se estará utilizando el protocolo SNMP V3 el cual permite la autenticación y encriptación de la información de vuelta por los dispositivos permitiendo la validación y la autenticidad de la solicitud.	
Fin del procedimiento				

5. Indicadores

Indicador	Descripción	Meta	Frecuencia
Cumplimiento en el aprovisionamiento y gestión del servicio de acuerdo los Niveles establecidos	Garantizar el cumplimiento del aprovisionamiento y gestión del servicio.	95%	Mensual

6. Políticas

i. Para la atención, registro y seguimiento se estará realizando con la herramienta BMC Remedy Service Desk en la cual se proporcionará el acceso al personal de EL CLIENTE para la consulta y generación de tickets via WEB. A continuación, se describen las actividades que estará ejecutando el SOC de forma enunciativa:

ii. Respaldos de configuración: El SOC proactivamente y de forma periódica generara los respaldos de las configuraciones para los equipos administrados. Los cuales pueden ser utilizados en caso de una contingencia o para recuperar una línea base de los equipos, estos respaldos se almacenan en un repositorio de forma segura obteniendo el HASH correspondiente para mantener la integridad de la información con una periodicidad semanal o cuando se ejecute algún cambio en los activos.

iii. Actualización de los activos: El SOC estará realizando una revisión constante de las versiones y/o parches con los que cuentan los activos para la ejecución de un análisis conforme a las recomendaciones de los fabricantes, permitiendo realizar las actualizaciones que apliquen conforme a la tecnología y configuración con la que se cuenta.

iv. Mantenimiento Operativo: Estas actividades se estarán ejecutando de forma continua por parte del

SOC, como son optimización y/o depuración de configuraciones, respaldos, depuración de logs entre otros.

v. Remediación de Vulnerabilidades: EL SILENT4BUSINESS estará realizando el análisis de vulnerabilidades y su remediación de la plataforma gestionada, estas actividades se estarán ejecutando de forma continua previa aprobación por parte de EL CLIENTE y alineado al proceso de control de cambios.

vi. Memoria Técnica: Como parte de los entregables EL SILENT4BUSINESS estará entregando la memoria técnica para la habilitación del servicio considerando su actualización de forma anual o cada que se ejecute un cambio mayor en la solución

7. Definiciones

- **SOC:** Security Operation Center (Centro de Operación para monitorear la Seguridad).
- **NOC:** Network Operation Center (Centro de Operación para monitoreo de Redes).
- **Aprovisionamiento:** Dentro de este grupo de actividades tenemos aquellas que tienen que ver con la logística de adquisición y entrega a nuestros clientes del equipamiento tecnológico necesario para entregar nuestros servicios. Sólo se compone de una fase.
- **Instalación:** Dentro de este grupo se encuentran aquellas actividades requeridas para la puesta en funcionamiento de todo el equipamiento tecnológico necesario para la provisión de nuestros servicios. Está compuesto por sólo una fase.
- **Servicios administrados:** Este grupo comprende todas aquellas actividades necesarias para la entrega de nuestros servicios de Centro de Operación de Seguridad (SOC, por sus siglas en inglés – Security Operations Center), y aquellos servicios adicionales y recurrentes que cumplan con las necesidades y especificaciones de nuestros clientes.
- **Operación de los servicios:** ejecución de los servicios de administración, monitoreo y soporte de infraestructura de seguridad de un proyecto.

8. Documentos relacionados

- P-SGI-002 Gestión Comercial.
- P-SGI-008 Gestión de Proveedores.
- P-SGI-010 Gestión de la Capacidad.
- P-SGI-011 Gestión de la Continuidad.
- P-SGI-012 Gestión de la Disponibilidad.
- P-SGI-013 Gestión de Niveles de Servicio.
- P-SGI-014 Gestión de Informes del Servicio.
- P-SGI-015 Gestión de Seguridad de la Información.
- P-SGI-017 Gestión de Incidentes del Servicio.
- P-SGI-018 Gestión de Incidentes de Seguridad.
- P-SGI-022 Gestión de Cambios.
- P-SGI-024 Gestión de la Demanda.
- PR-ENS-001Gestión de Proyectos.