ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

1. Descripción del objeto del Servicio.

Las condiciones generales (en adelante, las "CONDICIONES GENERALES"), regulan la prestación de los servicios de seguridad relacionados a continuación (en adelante, el "SERVICIO") prestado por el **Operador**.

El presente anexo describe las características técnicas y de prestación de servicio de:

- SOC – Security Operation Center – Centro de Operaciones de Seguridad
- Seguridad Gestionada
- Tráfico Seguro
- Escudo AntiDDoS

2. Definiciones.

- **SOC:** Centro de operaciones de Seguridad, es el conjunto de servicios y personal encargados de monitorizar la infraestructura interna y externa del **CLIENTE** con el fin de detectar y responder ante los incidentes de seguridad a los que se puede ver expuesta una organización.
- **Seguridad Gestionada:** Conjunto de alternativas en seguridad, cuyo eje fundamental es un dispositivo UTM o cualquier otro dispositivo, o conjunto de dispositivos de seguridad ubicado (s) físicamente en la sede del **CLIENTE** o en la sede del **OPERADOR**, en ambos casos administrado(s) y gestionado (s) por el **OPERADOR**. Es un servicio integral que incluye equipos, software, administración, gestión, monitoreo e informes, en función de las características de la red del cliente.
- **Tráfico:** Es la cantidad de información transferida desde y hacia distintos puntos de la red del **CLIENTE**, medida en bytes durante un intervalo de tiempo determinado.
- **Información:** Son todos los archivos de datos estructurados o no estructurados, programas y aplicativos, cuya responsabilidad recae en el **CLIENTE**, sean de su propiedad o no, alojados en la infraestructura del **CLIENTE** para ser consultados y/o trasmitidos a través de la red.

3. Uso de Software Licenciado.

El **OPERADOR** declara que el software utilizado para la prestación de los Servicios que se utilizan es de propiedad del **OPERADOR** o de sus proveedores o ha sido licenciado a éste o éstos por sus propietarios. En el evento en el que el **OPERADOR** decida suministrar software de su propiedad, de sus proveedores o de terceros licenciantes, para darle cumplimiento a las obligaciones derivadas del presente Anexo, se entenderá que dicho software es licenciado al **CLIENTE** en virtud de este Anexo, y sólo durante la vigencia del mismo, sometiéndose el **CLIENTE** a los términos del licenciamiento otorgado al **OPERADOR** y/o las condiciones de uso que el **OPERADOR** tenga en el momento.

4. Derechos de propiedad intelectual.

Las marcas, avisos, nombres comerciales, propaganda comercial, dibujos, diseños, logotipos, textos, etc., que aparecen en los documentos entregables, son de exclusiva propiedad del **PROVEEDOR**, o de terceros que de manera previa y expresa han autorizado a ésta para su uso. Queda prohibido cualquier uso o explotación por cualquier medio, sin el consentimiento previo y por escrito de **PROVEEDOR**, de las marcas Telefónica, Movistar y Telecom. Los documentos entregables se encuentran protegidos de conformidad con lo establecido por las normas nacionales e internacionales de protección de la Propiedad Industrial y del Derecho de Autor, quedando prohibido: modificar, copiar, distribuir, transmitir, desplegar, publicar, editar, vender, o de cualquier forma explotar los signos distintivos que acompañan los documentos entregables.

5. Obligaciones del CLIENTE.

Será responsabilidad del **CLIENTE**:

- Asignar un interlocutor único como responsable, y definir las personas de contacto autorizadas para realizar consultas.
- Conseguir toda la información necesaria y suministrarla al **OPERADOR**.
- Asignar el personal necesario, experto en las funciones a realizar y con la dedicación suficiente a estas tareas, para ejecutar la coordinación y proporcionar al **OPERADOR** la información necesaria para el análisis y resolución de incidencias.

6. Traslado

La solicitud de traslado del servicio aplica solo para el servicio de seguridad gestionada cuando el equipo Firewall se encuentre en la sede del **CLIENTE**. Este traslado debe solicitarse a través del Call Center o del ejecutivo de cuenta, el cual se realizará dependiendo de la disponibilidad técnica. Si no se cuenta con la disponibilidad técnica en la nueva sede, el **OPERADOR** no estará obligado a prestar el servicio y podrá proceder a la cancelación del servicio, sin sanción alguna para el **CLIENTE**. El precio del traslado será informado en el momento de la solicitud de

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

viabilidad y está compuesto por un precio de instalación más un precio por obras civiles.

7. Terminación Anticipada.

Si el **CLIENTE** da por terminado el servicio en forma anticipada a la vigencia del mismo, deberá pagar al **OPERADOR** todos los valores que estén pendientes a la fecha, así Como el monto que faltare del valor total de los servicios.

8. Tarifas del Servicio.

Las partes acuerdan, y así lo acepta **EL CLIENTE**, que durante la vigencia del servicio, **EL OPERADOR** podrá modificar en cualquier momento las tarifas del mismo, siempre que el incremento acumulado en el año no supere la variación del Índice de Precios al Consumidor (IPC) más cinco (5) puntos porcentuales. En todo caso el **OPERADOR** comunicará previamente al **CLIENTE** el incremento a realizar.

Para constancia, se firma en Bogotá D.C. a los_____ días del mes de _____ del año _____, en dos (2) ejemplares de igual tenor literal.

Por el Cliente:

_____
Representante Legal
Nombre:
C: C:

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

ALCANCE DEL SERVICIO DE SOC – Security Operation Center o Centro de Operaciones de Seguridad

En caso de que el **CLIENTE** haya contratado el servicio de SOC, las características de prestación del servicio son las siguientes:

1. Detalles de los servicios que componen el SOC

a. Monitoreo

El monitoreo de los eventos se realiza a través de la recolección de los mismos, usando el protocolo de transmisión SYSLOG para el monitoreo de seguridad y a través del protocolo de SNMP para los eventos de salud de la infraestructura, el cual permite que todos los eventos de los activos de seguridad sean centralizados en un dispositivo donde se crean las reglas y alertas que permitan tener una reacción efectiva y proactiva ante un incidente de seguridad de la información.

Las características del monitoreo son las siguientes:

- Revisión 7x24x365 por personal especializado.
- Análisis de eventos permanente basado en reglas y basado en conocimiento del personal especializado para generar las alertas

b. Correlación

Usando los registros recopilados es posible realizar un análisis de múltiples factores para determinar posibles incidentes de seguridad y la trazabilidad de los eventos sobre los dispositivos implicados, para esto se usa correlación de eventos. Este proceso se basa en reglas creadas por la experiencia del equipo y en análisis de inteligencia artificial que poseen nuestras herramientas, las cuales son permanentemente actualizadas y afinadas para minimizar la detección de falsos positivos o de falsos negativos.

Estos casos de uso dependerán de la cantidad de información que el **CLIENTE**, permita o tenga la necesidad de integrar en el sistema del **OPERADOR**.

c. Informes

Mensualmente el CLIENTE recibirá un informe sobre los eventos detectados tanto en el monitoreo de seguridad como en el monitoreo de salud, donde se evidencia la efectividad del servicio y se relacionan las alertas que se realizaron al equipo de contacto del CLIENTE.

Este reporte tiene una estructura básica con los datos relevantes del monitoreo y donde se evidencia la correcta gestión de las alertas y el escalamiento realizado en cada caso.

2. Características del SOC

- Los eventos del **CLIENTE** se mantendrán seguros en la transmisión y en la recolección.
- Se tiene consola de gestión y monitoreo centralizada.
- Generación de alertas y correlación de eventos a necesidad del **CLIENTE**.
- Alertas tempranas de estado de uso y consumo de hardware.
- Recolección de eventos de múltiples plataformas.
- Soporte especializado 7x24x365.
- Reporte gerencial que permita determinar estadísticamente la efectividad de las alertas y controles que posee la organización.
- Correlación avanzada, usando inteligencia de negocio para determinar los niveles de riesgo de cada evento.

3. Niveles de Servicio del SOC

a. Notificación de Incidentes

El monitoreo de los incidentes de seguridad genera una serie de alertas, las cuales serán reportados el cliente, con el fin de que este pueda tomar las acciones correctivas de forma oportuna y eficaz.

Los reportes se realizarán a través de correo electrónico y/o llamada telefónica según la matriz de escalabilidad que se coordine con el cliente, realizando este proceso el personal de operación de SOC en el menor tiempo posible tras la detección de un incidente.

b. Gestión de Requerimientos y/o Solicitudes

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

El servicio de SOC contará con una línea de atención a través del esquema de soporte tradicional para las solicitudes que tenga el cliente, las cuales se contemplan a continuación:

- Modificaciones sobre la plataforma monitoreada.
- Recuperación de eventos almacenados.
- Reporte de detección de incidente por parte del cliente como verdadero negativo

TIPO DE CAMBIO	DESCRIPCIÓN DEL CAMBIO	TIEMPO DE RESPUESTA
EMERGENCIAL	Cualquier cambio, bloqueo o modificación en configuración que requiere ser ejecutado de inmediato debido a la interrupción o pérdida del servicio. Este proviene de un incidente.	2 horas
NORMAL	Cualquier cambio temporal o permanente que pueda generar afectación de servicio y requiera ser revisado en comité **Ejemplo:** (ventanas de mantenimiento, implementación de nuevas interfaces, cambio de direccionamiento, enrutamiento, cambios en los parámetros de configuración del servicio),	Según aprobación de **CLIENTE** y comité de cambios
ESTANDAR	Cualquier cambio que no genere alguna afectación de servicio **Ejemplo:** regla del SIEM	4 horas

c. Horarios de Atención y Tiempos de atención

CASO TIPO	ATENCION	RESPUESTA
REQUERIMIENTOS - RFS	5x8 08:00 A 17:00	4 Horas Hábiles
CAMBIOS - RFC	5x8 08:00 A 17:00	1 Dia Hábil
INCIDENTES	7X24	2 Horas - 30 Min Iniciales Diagnostico

ALCANCE DEL SERVICIO DE SEGURIDAD GESTIONADA

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

En caso de que el **CLIENTE** haya contratado el servicio de Seguridad Gestionada, las características de prestación del servicio son las siguientes:

1. Componentes del Servicio de Seguridad Gestionada

a. IPS (Intrusion Prevention System): Es un software de seguridad que se instala sobre el Firewall encargado de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión, esto es, cualquier intento de comprometer la confidencialidad, integridad o disponibilidad de un sistema informático, o de eludir los mecanismos de seguridad de éste. Las intrusiones se pueden producir de varias formas:

- Atacantes que acceden a los sistemas desde Internet.
- Usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados.
- Usuarios autorizados que hacen un mal uso de los privilegios o recursos que se les ha sido asignados.

b. Gestión de VPN´s: Configuración del módulo de VPN, junto con usuarios y reglas de acceso a servicios. SITE to SITE, conexión vía VPN con otros firewalls del mismo fabricante u otro fabricante o implementación de VPNs CLIENTE-Servidor, donde se crean conexiones remotas en PCs o Móviles para conectarse a un terminador de VPNs para acceder de manera segura a un servicio interno.

c. Integración con antivirus: Software adicional compatible con el firewall, para inspección de diferente tipo de tráfico como smtp ó web asegurando la integridad de la información transmitida, la cual se puede ver alterada a causa de código malicioso. Detección y eliminación de virus en el correo electrónico entrante y saliente.

d. Integración con antispam: Software adicional compatible con el firewall con la opción de control de spam como recurso dentro de los servicios, se ofrece:

- Filtro para los tipos de archivos no deseados
- Gestión de los archivos de gran tamaño
- Gestión de los datos del correo electrónico

e. Filtro de contenidos: Software adicional compatible con el firewall cuya función es vigilar y/o filtrar el acceso de los empleados a los servicios conforme a la política definida por el CLIENTE controlando el adecuado uso del ancho de banda. El software observa todo el tráfico entre la red del CLIENTE e Internet y almacena información con base a las reglas definidas. Este log incluye información de los usuarios de la red, el tipo de servidores Web visitados, el ancho de banda consumido y los intentos de violación de la Política de Acceso a Internet.

f. Diseño estructural de las políticas de seguridad: es una actividad conjunta en cuya definición participan las partes del contrato. En dicha actividad se definen los servicios que requieren ser accedidos desde y hacia las redes protegidas por el Firewall. En esta fase se incluye el análisis de la topología de la red y servicios asociados a la misma. El OPERADOR hace las recomendaciones pertinentes para que el grupo de reglas definidas correspondan a las necesidades específicas de seguridad del CLIENTE.

Para garantizar lo anterior, el **OPERADOR** estudia la topología de la red juntamente con el **CLIENTE** y verifica los servicios que requieren ser accedidos para diseñar las políticas de seguridad correspondientes.

Una vez finalizada la etapa de definición conjunta, el **OPERADOR** implementa la solución y genera el Acta de Entrega del Servicio, con la cual el **CLIENTE** da por aceptado el servicio y a partir de este momento se inicia la fase de operación en la cual los cambios, adiciones o modificaciones entrarán bajo el esquema de mantenimiento dependiendo de la modalidad de servicio contratado.

En el Acta de Entrega del Servicio se consigna el resultado de la solución implementada incluyendo la topología de red, políticas de seguridad y observaciones / recomendaciones generales.

g. Gestión del equipo firewall: La gestión del equipo firewall incluye: (i) Actualizaciones de aplicación de seguridad y/o Sistema Operativo y (ii) Monitoreo 7 x 24.

2. Solicitud de Actividades

a. Operación Remota: Consiste en la ejecución de los requerimientos o acciones a ejecutar de acuerdo con el procedimiento de solicitud de cambios y/o adiciones. Adicionalmente, la operación remota, permite resolver eventos de soporte.

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

- Se actúa con la operación remota cuando:

  - El **CLIENTE** solicita alguna modificación en las políticas de seguridad o en los alcances del servicio basados en el procedimiento de control de cambios.
  - Ocurre un evento crítico en horas no hábiles (o de no operación por parte del **CLIENTE**) y simultáneamente se notifica al cliente del evento y de la acción tomada.

- Cualquier acción y modificación realizada en la operación remota bien sea por solicitud del **CLIENTE**, o por acción proactiva, preventiva o correctiva ante un evento crítico, es notificada al **CLIENTE** de forma inmediata y es registrada en el reporte mensual al **CLIENTE.**

b. Mantenimiento de políticas de seguridad: Correcciones y/o adiciones a las políticas de seguridad (hasta 5 solicitudes al mes), teniendo como base el registro de los del Firewall y servicios adicionales que el CLIENTE requiera.

c. Informes de servicio: Informe Mensual de la Bitácora de eventos y/o solicitudes sobre el elemento de seguridad, incluido en las dos modalidades de servicio. Este informe es un registro periódico de los cambios, adiciones, modificaciones efectuadas sobre el firewall del cliente tanto por solicitud del mismo ó por gestión proactiva del **OPERADOR.**

d. Procedimiento para solicitud de cambios y/o adiciones en políticas

La solicitud de cambio y/o adiciones de políticas, se hará mediante un Formato establecido por el **OPERADOR** para este efecto, del cual se llevará un registro de las políticas establecidas. Igualmente se tiene implementado un cronograma de ejecución en horario de bajo impacto para evitar eventuales problemas con el servicio contratado.

e. Política de cambios

- El **CLIENTE** debe tener una persona de contacto para él envió de políticas y servicios (solicitud y soporte).
- Toda política y servicio se enviará bajo el formato definido para tal fin.
- Solo se recibirán políticas a través del Formato oficial.
- El Formato debe ser diligenciar con los datos de la persona contacto e información para en caso de confirmación o duda sobre la política o servicio que se instalará.
- Estas son políticas que se envían por nuevos servicios, cambios en los puertos o modificaciones controladas debido a nuevos productos o instalaciones por parte del cliente.
- Toda tiene un soporte de 24 horas.

Tipos de Cambios:

Cambios Normales: Cualquier cambio temporal o permanente con determinado nivel de riesgo o afectación o modificación del Servicio.
Cambios Estándar: Cambios que no afectan el servicio de los cuales están predefinidos y aprobados contractualmente.
Cambios Emergencial: Cambios, bloqueos o modificaciones en configuración que debe realizarse tan pronto sea posible debido a la interrupción o pérdida de un servicio. Este proviene de un incidente.

f. VPNs Client to Site o Site to Site

Estas son solicitudes de configuraciones de VPNs para conectar usuarios móviles o conectarse con otra entidad para intercambiar información de forma privada y segura. Se debe caracterizar por: (i) El **CLIENTE** debe facilitar los datos y persona de contacto remota en VPNs Site to Site. (ii) El **CLIENTE** debe facilitar la información del agente (VPNs Client to Site) para que pueda ser creado el perfil según los datos. En ambos casos, se debe llenar el formato de solicitudes, opción fuente any y destino el usuario o nombre de la persona que lo utilizará, el puerto o servicio que se configurará en la VPNs.

Los tiempos para VPNs Cliente son de 48 horas. Las solicitudes de VPNs Site to Site. Que implican configuración con otros firewalls serán analizadas y estudiadas determinando un tiempo de configuración no mayor a 2 semanas.

Toda solicitud debe ser registrada a través del callcenter. No se aceptarán solicitudes dirigidas a correos corporativos ni comunicaciones dirigidas a nombre de los colaboradores del **OPERADOR**. La solicitud debe estar soportada por el Formato de Solicitud de Políticas de Seguridad avalado por el **OPERADOR**.

g. Instalación de Servicio de Seguridad Gestionada:

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

La instalación de los equipos y software necesarios para prestar el servicio de Seguridad Gestionada será de exclusiva responsabilidad del **OPERADOR**. Este instalará los equipos y software necesarios para prestar el servicio de Seguridad Gestionada para que opere de acuerdo con los estándares y especificaciones técnicas. El **OPERADOR** programará los elementos de conectividad del Centro de Datos, como se establezca en la Orden de Servicio. Será responsabilidad exclusiva del **OPERADOR** la operación y manejo de los equipos y software necesarios para prestar el servicio de Seguridad Gestionada, así como su mantenimiento físico y lógico. Estas actividades se realizan de conformidad con el Manual del Fabricante.

En los casos donde el equipo Firewall se instale en el lado del **CLIENTE**, éste es responsable de suministrar la infraestructura necesaria, para la instalación de los equipos y bienes requeridos en la solución de seguridad gestionada con el objeto de garantizar la buena prestación del servicio.

Infraestructura Física:

- Espacio en gabinetes para instalación de bandejas donde se alojará el equipo firewall.
- Suministro de aire acondicionado o refrigeración para mantener la temperatura constante del salón donde están ubicados los equipos. Se requiere una temperatura ambiente máxima de veinticuatro (24) grados centígrados.

Infraestructura Eléctrica:

- Suministro de energía AC Regulada e ininterrumpida o energía DC con su correspondiente rectificador/conversor asociado. El suministro de energía debe llegar hasta el lugar en el cual se van a instalar los diferentes equipos y ésta será suministrada a través de una protección sobre tensiones y sobre corrientes (breaker) exclusiva para dichos equipos.
- Se debe proveer un barraje de tierra en el salón de equipos el cual estará conectado a un sistema de tierra independiente al del pararrayos con resistividad menor a cinco ohmios o de un nivel adecuado para la protección de los equipos.

3. Niveles de Servicio de Seguridad Gestionada

Instalación de Equipos

Estos tiempos dependerán, si se cumplen con los requerimientos estipulados en el numeral **2g Instalación de Servicio de Seguridad Gestionada,** así como que los mismos ya hayan cumplido su proceso de importación que dependerá de cada fabricante.

Nivel de Servicio	Métrica	Índice
Ciudades Principales	Días	<= 4 días
Ciudades Intermedias	Días	<= 7 días
Ciudades y Municipios Remotos	Días	<= 10 días

Requerimientos y/o Solicitudes

TIPO DE CAMBIO	DESCRIPCIÓN DEL CAMBIO	TIEMPO DE RESPUESTA
EMERGENCIAL	**Cualquier cambio, bloqueo o modificación en configuración que requiere ser ejecutado de inmediato debido a la interrupción o pérdida del servicio. Este proviene de un incidente.**	**2 horas**
NORMAL	**Cualquier cambio temporal o permanente que pueda generar afectación de servicio y requiera ser revisado en comité** **Ejemplo: (ventanas de mantenimiento, implementación de nuevas interfaces, cambio de direccionamiento, enrutamiento, cambios en los parámetros de configuración del servicio)**	**Según aprobación de cliente y comité de cambios**
ESTANDAR	**Cualquier cambio que no genere alguna afectación de servicio** **Ejemplo: regla del SIEM**	**4 horas**

Horarios Estipulados para Requerimientos y/o Solicitudes.

Cambios Normales y Cambios Estándar: Estos son registrados por correo en horario 7*24 pero serán atendidas en horario de: 8:00a.m. a 5:00pm de Lunes a Viernes.

Los cambios serán evaluados por Telefónica y podrán ser recategorizados según el riesgo y el impacto que presente dicho cambio sobre la infraestructura, los cuales serán socializados con el cliente.

Cobertura Soporte Servicio

Alcances	Cobertura
Soporte Técnico Telefónico – 1er Nivel	7x24
Soporte Técnico Telefónico – 2do Nivel (Ingenieros Especialistas de Seguridad)	7x24

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

Soporte Técnico Telefónico – 3er Nivel (Fabricante)	7x24

En todos los casos se contempla que podrán existir tiempo de demoras justificadas, en cuyo caso se sale de los tiempos de respuesta indicados.

En resumen, a lo anterior:

CASO TIPO	ATENCION	RESPUESTA
REQUERIMIENTOS – RFS	5x8 08:00 A 17:00	4 Horas Hábiles
CAMBIOS – RFC	5x8 08:00 A 17:00	1 Dia Hábil
INCIDENTES	7X24	2 Horas – 30 Min Iniciales Diagnostico

****

ALCANCE DEL SERVICIO DE TRAFICO SEGURO

En caso de que el **CLIENTE** haya contratado el servicio de Trafico Seguro, las características de prestación del servicio son las siguientes:

1. **Alcance del Servicio de Trafico Seguro**

El Servicio ofrece protección perimetral al acceso de Internet dedicado del **CLIENTE** en el equipo de seguridad implementado en la red del **OPERADOR**. Las funcionalidades de seguridad perimetral y de contenidos que se definen como parte del alcance del servicio del servicio son:

- Firewall

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

- IPS
- Antivirus de Gateway
- AntiSpam
- Filtro de Contenido web
- Conexión teletrabajo VPN SSL

Algunas de las consideraciones que se deben tener con respecto al servicio de Trafico Seguro:

- La infraestructura sobre la cual se presta el servicio es propiedad del **OPERADOR**.
- El servicio permite al **CLIENTE** que la conexión y la navegación a Internet se realicen con un alto nivel de seguridad y rendimiento, permitiendo la escalabilidad de todos sus componentes.
- El servicio permite al cliente controlar la Navegación de Internet de sus usuarios y mediante el uso de Firewall impide el acceso de tráfico no deseado.
- El servicio se ofrece sobre una plataforma muy flexible y escalable
- Se entregarán reportes del comportamiento de la solución por cliente de manera mensual
- La administración de los IPS es hecha por el **OPERADOR** y no puede ser compartida con el **CLIENTE**.
- El filtro de contenido web tiene la capacidad de hacer filtrado por:
  - Lista personal de sitios permitidos
  - Lista personal de sitios bloqueados
  - Categorías a bloquear
  - Archivos prohibidos para download
- Solo se bloquea tráfico que está saliendo del **CLIENTE** por el **OPERADOR**
- No se bloquea cuando el **CLIENTE** está con el laptop de la empresa en algún otro sitio diferente
- No se bloquea si el **CLIENTE** tiene un enlace con otro ISP y está accediendo a Internet por ese enlace.
- Los servicios que el antivirus perimetral ofrecido en tráfico seguro soporte son los siguientes:
  - Http, Https: controla la entrada de virus del contenido consultado a Internet y la descarga a través de estos medios.
  - FTP: Controla la entrada de virus que pudiera penetrar al descargar información de servidores FTP.
  - SMTP, IMAP, POP: Puede revisar el correo para detectar anomalías, gusanos, o contenido malicioso.
- **El OPERADOR** es responsable por configurar/Implantar la configuración del Antivirus para el **CLIENTE**.

2. Niveles de Servicio de Trafico Seguro

a. Disponibilidad por componente de la solución

COMPONENTE DEL SERVICIO	INDICE DE DISPONIBILIDAD
Firewall	99,6%
Filtro de Navegación	99,6%
Prevención de Intrusión	99,6%
VPN	99,6%
Anti-Virus	99,6%
Anti-Spam	99,6%
Firewall Aplicación WEB	99,6%
Proxy de Navegación	99,6%
Anti-DDoS	99,6%
Sandbox	99,6%

b. Servicio de Soporte

NIVEL DE SOPORTE	ALCANCE DEL SOPORTE	DISPONIBILIDAD
NIVEL 1	Soporte telefónico (GICS) que recibe los casos y da solución a casos básicos solicitados	7x24x365

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

NIVEL 2	Soporte telefónico realizado por ingenieros especializados en seguridad, que cubren casos específicos del cliente	7x24x365
NIVEL 3	Soporte telefónico del fabricante para casos de soporte avanzados	7x24x365

CASO TIPO	ATENCION	RESPUESTA
REQUERIMIENTOS - RFS	5x8 08:00 A 17:00	4 Horas Hábiles
CAMBIOS - RFC	5x8 08:00 A 17:00	1 Dia Hábil
INCIDENTES	7X24	2 Horas - 30 Min Iniciales Diagnostico

****

ALCANCE DEL SERVICIO DE ESCUDO ANTIDDoS

En caso de que el **CLIENTE** haya contratado el servicio de Escudo AntiDDoS, las características de prestación del servicio son las siguientes:

1. Alcance del Servicio de Escudo AntiDDoS

a. Detección, Mitigación y Reportes

La solución desplegada está monitorizando continuamente el tráfico de la red, permitiendo obtener datos estadísticos de uso de la misma y pudiendo detectar Ataques de volumen masivo que saturan el enlace del cliente (volumetric attacks).

En el panorama actual de la seguridad informática, los ataques de denegación de servicio (DoS) y los ataques de denegación de servicio distribuidos (DDoS) son una de las principales amenazas a la disponibilidad de las redes. Los ataques DDoS pueden

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

provenir de hacktivistas que buscan dar visibilidad a una causa, defraudadores que intentan obtener ilegalmente datos o fondos, o incluso eventos geopolíticos. En cualquier caso, está claro que estos ataques pueden ser un arma de destrucción cibernética. Los gobiernos y las empresas de servicios públicos, servicios financieros y comercio sufren ataques a diario.

Los ataques se tornan cada vez más sofisticados y graves, al punto que burlan los servicios tradicionales de protección CDN y protección en la nube para atacar la infraestructura informática y las aplicaciones críticas de una organización.

b. Componentes de la solución.

- Prevención DDoS: Prevención de ataques de denegación de servicio.
- IPS: Previene contra exploits de capa de aplicación.
- NBA: Previene contra el uso inadecuado de recursos, ataques Zero-Day.

2. Descripción de los planes

El servicio Anti-DDoS se define como un servicio de protección frente a ataques DDoS gestionado según el modelo In-Cloud y que no requiere instalación de equipamiento en la red del cliente. El tráfico del cliente se monitoriza y los ataques se mitigan antes de que lleguen a su red.
El servicio se comercializa según la modalidad del servicio y el ancho de banda del canal a proteger.

Se definen dos planes posibles para la contratación; Plan Básico y Plan Avanzado.

El detalle de los planes según alcance de protección es el siguiente:

Plan Básico – Protección contra ataques volumétricos Capa 4. **Análisis de comportamiento Basado en Red**
Protección en tiempo real contra los ataques:
• TCP SYN Floods
• TCP SYN+ACK Floods:
• TCP FIN Floods
• TCP RESET Floods
• TCP Out of state Floods
• TCP Fragment Floods
• UDP Floods
• ICMP Floods
• IGMP Floods
• Paquetes Anómalos

Plan Avanzado – Protección contra Capa 7. **Análisis de Comportamiento en Capa 7.**
Incluye los servicios prestados en el Plan Básico más:
Protección en tiempo real contra ataques de desafíos de autenticación y ataques de robo de información:
• Ataques HTTP – Orientados a la Conexión
• Escaneos de Vulnerabilidades Web
• Herramientas de Ataques con Live CD (Backtrack, Metasploit, etc)
• Enumeración y Escaneo Capa 3 y Capa 4
• Botnets y HTTP Floods
• Ataques de consumo de ancho de Banda HTTP
• Ataques de Fuerza Bruta y Diccionario
• Ataques SIP
• Ataques a Servidores SMTP/IMAP/POP3
• Ataques dirigidos a Servidores de Transferencia de Archivos (FTP, etc)
• Ataques a aplicaciones DNS (Query, Recursive Floods)
• Intrusiones

3. Entregables del Servicio

Plan Básico	**Plan Avanzado**
	Lo entregado en el **Plan Básico**
Detecciones de Ataques Capa 4	Detección de Ataques Capa 7 limitado
Mitigaciones de Ataques Capa 4	Mitigación de Ataques Capa 7 limitado
Configuración y puesta en marcha de la política asignada.	Reportes personalizados mensuales y bajo demanda. Análisis y enriquecimiento por parte de Analista del SOC

ANEXO DE SERVICIOS DE SOC, SEGURIDAD GESTIONADA, TRÁFICO SEGURO Y ESCUDO ANTIDDoS

	Configuración de protección de Server Protection hasta 5 Server

4. Modelo de Atención

Dado el carácter confidencial de la información tratada y reportada, Telefónica propone la existencia de un contacto único dentro del Cliente al cual se le notificará cualquier grado de avance y, en particular, aquellos puntos relativos al tratamiento de incidencias.

A su vez, el Cliente tendrá a su disposición los siguientes puntos de contacto dentro del servicio:

El SOC será el contacto principal del Cliente y atenderá cualquier aspecto relacionado con la prestación del servicio (consultas, peticiones, aclaraciones, incidencias etc.) en horario 7x24.

Las incidencias deberán ser siempre notificadas a Telefónica por parte del interlocutor autorizado por el cliente para tales fines, y a través de las vías establecidas. Por lo tanto, no se gestionará ningún tipo de consulta o incidencia que no sea debidamente solicitada y procesada.

5. Niveles de Servicio de Escudo AntiDDoS

a. Servicio de Soporte

NIVEL DE SOPORTE	ALCANCE DEL SOPORTE	DISPONIBILIDAD
NIVEL 1	Soporte telefónico (GICS) que recibe los casos y da solución a casos básicos solicitados	7x24x365
NIVEL 2	Soporte telefónico realizado por ingenieros especializados en seguridad, que cubren casos específicos del cliente	7x24x365
NIVEL 3	Soporte telefónico del fabricante para casos de soporte avanzados	7x24x365

CASO TIPO	ATENCION	RESPUESTA
REQUERIMIENTOS - RFS	5x8 08:00 A 17:00	4 Horas Hábiles
CAMBIOS - RFC	5x8 08:00 A 17:00	1 Dia Hábil
INCIDENTES	7X24	2 Horas - 30 Min Iniciales Diagnostico

Incidencia Plataforma	El SOC cuenta con 30 minutos para diagnosticar el incidente escalado. • uando un caso supere los tiempos de diagnostico (70 Min a 120 Min) y según el tipo de falla, se debe iniciar las actividades por el proceso de EMP-PO-01050604 Gestión crisis DC tras notificación de SOC al Incident Manager
Notificación de Incidencias	• El SOC cuenta con 15 minutos para diagnosticar el incidente escalado
Actividades Programadas	• Esta actividad es notificada a través de un RFC, confirmando la fecha y hora del mantenimiento, una vez aprobada la actividad el gestor de cambio notifica avances cada 15 minutos hasta concluir el tiempo de la ventana de mantenimiento.
Requerimientos y Solitudes (Reglas, Consultas, Modificaciones de Configuración, etc)	• El SOC cuenta con un tiempo de 4 horas para dar respuesta a este tipo de solicitudes de Consulta

****