DESCRIPCIÓN Y ALCANCE DEL SERVICIO DE NSS S.A.
MITIGACION IPLAN

1. Introducción

Considerando que los Ataques distribuidos de Denegación de Servicio (DDoS) son una amenaza que afecta seriamente los activos de las organizaciones, y existen intentos de hackeos que pueden acceder a la información de las organizaciones a través de estos, IPLAN presenta un servicio de Mitigación acorde a las necesidades del mercado actuales.

El servicio de Mitigación IPLAN está diseñado para prevenir los ataques de denegación de servicio distribuido (DDoS) volumétricos y de protocolo, a través de las conexiones de Internet.

El servicio Mitigación IPLAN es una solución integral que permite la detección y mitigación automática de ataques DDoS sin afectar el tráfico normal de cada Cliente, filtrando el tráfico malicioso sin afectar el normal funcionamiento del servicio de Internet. Posee una infraestructura robusta que, a través de un portal web se podrá realizar revisiones de las alertas de seguridad, el consumo de tráfico normal y el tráfico malicioso.

Mitigación IPLAN cuenta con reglas inteligentes basadas en heurística de alto rendimiento que permite bloquear ataques DDoS de día cero, logrando identificar estos ataques y bloquear automáticamente en cuestión de segundos con un promedio máximo de mitigación de 5 minutos.

A continuación se detallan algunos de los beneficios que este servicio conlleva, sin ser esta lista exhaustiva ni excluyente:

- La mitigación es de forma automática e inmediata.
- Está orientado a ataques de capa 3 y 4.
- Aprendizaje continuo.
- Monitoreo 7x24x365.
- Notificaciones en tiempo real del comportamiento del tráfico de la conexión de Internet con reportes y alarmas vía correo de los ataques y las mitigaciones realizadas.
- Personal altamente capacitado a disposición del Cliente para el monitoreo y administración del servicio.
- Protege las conexiones de Internet contra ataques conocidos y desconocidos, estos últimos llamados usualmente “zero-day attack” ya que no necesita esperar a que se actualicen las firmas de nuevos ataques.

2. Descripción general y Alcance del servicio

El Servicio Mitigación IPLAN únicamente podrá ser contratado por Clientes que tengan contratados con IPLAN servicios de internet de ancho de banda garantizado superior a 100 Mbps, y dichos servicios se encuentren activos, y el ancho de banda de mitigación deberá coincidir con el del enlace de internet contratado y activo.

Brinda una protección de hasta diez veces la capacidad del ancho de banda de Internet contratado. Una vez superada esta capacidad el Cliente irá a blackhole automáticamente para proteger la integridad de su infraestructura. El Cliente podrá traficar su consumo normal automáticamente después de 1hs. (el tiempo estándar que IPLAN sugiere configurar para volver a estado normal es de 1hs, aunque a requerimiento del Cliente durante el aprovisionamiento del servicio se puede configurar más o menos tiempo).

Blackhole: Se redirige el total del tráfico hacia una dirección de "agujero negro" para eliminar el impacto en la red legítima. En este caso, las redes de destino configuran un blackhole para absorber el tráfico no deseado y evitar que sobrecargue la red.

- Los ataques que la plataforma es capaz de detectar/mitigar son ataques volumétricos y únicamente los expresados a continuación, L3/4 Volumetric Protection
    - ACK Attack or ACK-PUSH Flood
    - DNS Amplified (Reflective)
    - DNS Flood
    - Fake Session Attack
    - Fraggle Attack
    - Fragmented ACK Flood
    - ICMP Flood
    - ICMP Fragmentation Flood
    - IP NULL
    - Memcached Attack
    - Non-Spoofed UDP Flood
    - NTP Amplified (Reflective)
    - NTP Flood
    - Ping Flood
    - RST/FIN Flood
    - Same Source/Dest Flood (LAND Attack)
    - Smurf Attack
    - SSDP Amplified (Reflective)
    - SYN Flood
    - SYN-ACK Flood
    - TCP Null
    - TOS Flood
    - UDP Flood
    - UDP Fragmentation

- Protección de la aplicación al inspeccionar el tráfico entrante sin descifrado
    - TCP Connection Flood
    - HTTP Flood
    - HTTP Slow Attack
    - SSL/TLS Malformed
    - SSL/TLS Renegotiation
    - SSL/TLS Session (Per Source IP)
    - SIP Malformed
    - SIP Spoofing
    - SIP REGISTER Request Flooding
    - SIP INVITE Request Flooding
    - Source Half Open Connection
    - Source IP Idle Connection
    - Slow Rate Connection

Como mencionamos anteriormente, el servicio Mitigación IPLAN identifica y mitiga, de manera inteligente, automática y proactiva los ataques DDoS, sobre la actividad de monitoreo y detección, aliviando a los Clientes la tarea de dicha gestión y permitiendo la continuidad de su negocio sobre Internet. Este servicio incluye las siguientes capacidades:

(a) Detección y mitigación automática de ataques.
(b) Recepción de alertas automáticas enviadas por email y disponibles en el portal web.
(c) Mitigación de ataques DDoS volumétricos y de protocolo.
(d) Mitigación local en Argentina.
(e) Soporte para múltiples técnicas de mitigación: rápido, normal y por inteligencia artificial.
(f) Acceso al portal web. El portal presentará información sobre sus detalles de tráfico y estadísticas (en tiempo real e históricos de hasta 12 meses), ataques DDoS detectados, alertas y mitigaciones realizadas.
(g) Opción de mitigación manual para desactivar los ataques DDOS volumétricos a través del Centro de

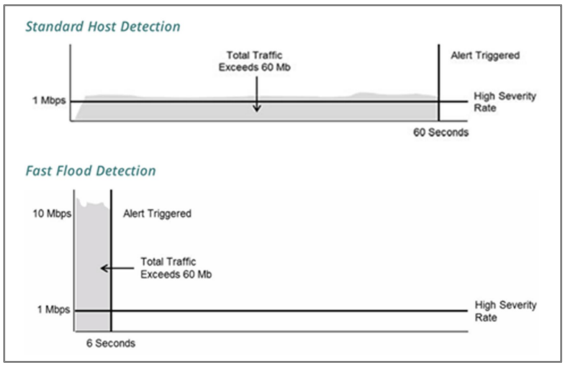
Operaciones de IPLAN

(h) Soporte 7x24x365

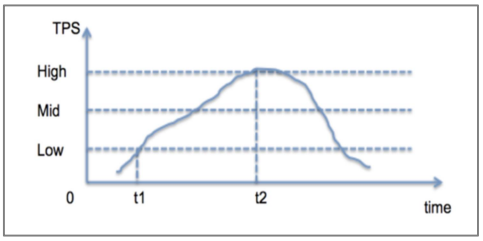
A continuación se detallan las técnicas de mitigación mencionadas anteriormente:

- **Modo rápido:** La alerta de ataque se activa a los pocos segundos a partir que el volumen de tráfico excede el umbral de detección de alto nivel para el ancho de banda contratado.

En este modo, las alertas se generan más rápidamente pero se eleva la tasa de falsos positivos



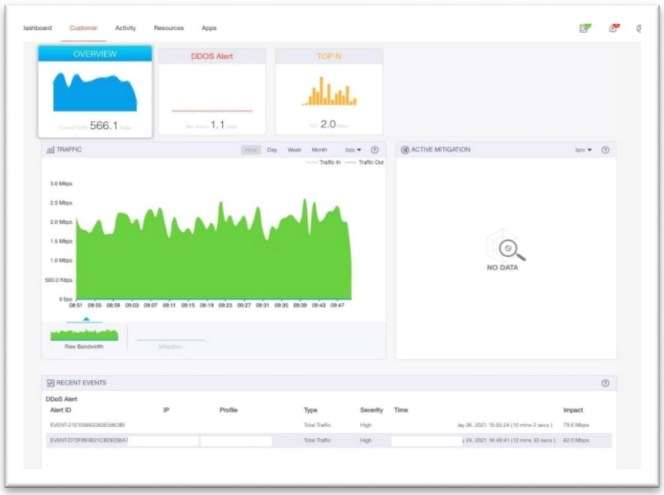
- **Modo normal:** La alerta de ataque se activa cuando el tráfico excede continuamente los umbrales de detección predefinidos durante 3 minutos. Este modo es adecuado para detectar el flujo continuo de tráfico de ataque



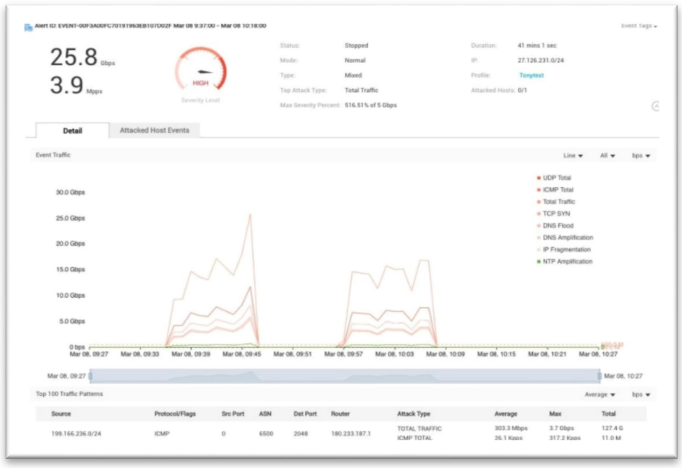
- **Modo Inteligencia Artificial:** La alerta de ataque se genera automáticamente una vez que el tráfico coincide con alguno de los patrones aprendidos por el sistema. Este modo, utiliza múltiples características del tráfico para la detección de los ataques, entre ellas tipo y características del protocolo del tráfico. No es necesario establecer manualmente los umbrales de detección. El tiempo máximo de detección es de 3 minutos.

El Portal Web permitirá la visualización del tráfico de las conexiones de Internet que cuenten con la protección contra ataques de DDoS, y un dashboard con la visualización de las alarmas de seguridad. El Cliente tendrá acceso a esta información a través del mismo y se le asignará un usuario y clave, este es un usuario de solo lectura.

A continuación se detallan algunas pantallas del mismo:



Dashboard del tráfico



Detalle de un ataque mitigado

RECENT EVENTS

DDoS Alert

Alert ID	IP	Profile	Type	Severity	Time	Impact
EVENT-8CF41D7783069E5452DFEA2D2C	45.238.98.81	_45.238.98.0_24	Mixed	High	Apr 23, 2021 11:59:14 - Ongoing	80.0 Mbps
EVENT-FA9882AFAB164C962ABA4C3A4C	138.204.237.100	_138.204.237.0_24	Mixed	High	Apr 23, 2021 11:48:00 - Ongoing	974.3 Mbps
EVENT-0CE5D665B4C5B6777565E1AF72	45.238.98.245	_45.238.98.0_24	Mixed	High	Apr 23, 2021 11:32:48 - Apr 23, 2021 11:54:28 (21 mins 41 secs)	2.1 Gbps
EVENT-9412450C9A4CE46A0E99EA6213	138.204.237.100	_138.204.237.0_24	Mixed	High	Apr 23, 2021 11:14:00 - Apr 23, 2021 11:36:51 (22 mins 52 secs)	2.2 Gbps
EVENT-5B2C7338CC3977AA7DC976D603	45.238.98.245	_45.238.98.0_24	Total Traffic	High	Apr 23, 2021 7:06:13 - Apr 23, 2021 7:20:00 (13 mins 48 secs)	195.6 Mbps
EVENT-FF72CDC4FC03DEA0CFA995C62E	45.238.98.245	_45.238.98.0_24	Mixed	High	Apr 23, 2021 6:11:14 - Apr 23, 2021 6:43:16 (32 mins 3 secs)	1.5 Gbps
EVENT-47149611F6B1E6A92FCDD544FC	45.238.98.245	_45.238.98.0_24	Mixed	High	Apr 23, 2021 4:00:16 - Apr 23, 2021 5:01:16 (1 hour 1 min 1 sec)	636.0 Mbps
EVENT-545F135BFCCF2BA752B91177EF	45.238.98.245	_45.238.98.0_24	Mixed	High	Apr 23, 2021 3:59:15 - Apr 23, 2021 4:11:14 (12 mins)	1.5 Gbps
EVENT-ACD2E1F68FE458E471C448ACC2	45.238.98.245	_45.238.98.0_24	Mixed	Blackhole	Apr 23, 2021 3:25:23 - Apr 23, 2021 3:47:00 (21 mins 38 secs)	2.3 Gbps
EVENT-088D8BB7D467D57380D44FB11E	138.204.237.100	_138.204.237.0_24	Mixed	High	Apr 23, 2021 3:10:00 - Apr 23, 2021 3:31:30 (21 mins 31 secs)	1.1 Gbps

Histórico de ataques

3. Otras Obligaciones Generales

3.1 El Cliente deberá cumplir con todas las leyes, regulaciones, normas, ordenanzas y órdenes aplicables relacionadas con sus actividades. El Cliente garantiza y acuerda que los Servicios no se proporcionarán en relación con ninguna actividad que:

i) Esté en violación de cualquier ley, código o regulación aplicable, incluyendo, entre otros, infracción de marcas, derechos de autor y otros derechos de propiedad intelectual, difamación, robo, fraude, tráfico de drogas, lavado de dinero, terrorismo, juego ilegal, violación de derechos de datos y privacidad, o la realización de dichas actividades;

ii) Pueda incitar a la violencia, el sadismo, la crueldad o el odio racial;

iii) Sea pornográfica, obscena, indecente, abusiva, ofensiva o amenazante;

iv) Pueda, directa o indirectamente, promover juegos de azar, loterías o actividades similares; o

v) Manipule el enrutamiento de la red o los servicios de nombres de dominio de manera que oculte la identidad del remitente o implique la suplantación de otro sistema informático.

4. Actividades Prohibidas

4.1 El Cliente no participará en prácticas comerciales engañosas, ilegales o poco éticas, y cumplirá con todas las leyes aplicables, incluyendo, entre otras, la Ley de Prácticas Corruptas en el Extranjero de los EE. UU. de 1977, según sea modificada.

4.2 El Cliente no utilizarán ni proporcionarán los Servicios de ninguna manera para enviar correos electrónicos no solicitados, recopilar, usar, extraer o transferir datos personales de individuos (ni permitirán que otros lo hagan) sin el consentimiento previo por escrito de dichos individuos de acuerdo con la Ley de Protección de Datos Personales.25.326

4.3 El Cliente no transmitirá ni cargará, ningún gusano, troyano, virus, spyware, código, script, adware o cualquier forma de malware que pueda impedir, degradar o afectar negativamente el rendimiento de la Red o de los Servicios, ni permitirá que terceros lo hagan. El Cliente garantiza que mantiene y seguirá manteniendo una protección antivirus actualizada y conforme a los estándares de la industria con respecto al contenido, material, información o datos que transmite.

4.4 El Cliente se compromete a no abusar ni hacer un uso fraudulento de los Servicios, incluyendo, sin limitación:

i) Intentar o realmente obtener, acceder, alterar o destruir los archivos de datos, programas, procedimientos y/o información de IPLAN;

ii) Ayudar a otros a realizar los actos prohibidos;

iii) Usar los Servicios (o permitir su uso) de manera que interfiera con el uso, rendimiento, seguridad e integridad de los Servicios.

4.5 El Cliente se compromete a mantener su Información de Acceso, nombres de inicio de sesión, contraseñas y otra información confidencial relacionada con el acceso a los Servicios de manera confidencial. El Cliente reconoce y acepta que es el único responsable de la integridad y seguridad de sus propios sistemas y asume todo el riesgo por el uso fraudulento o no autorizado de su Información de Acceso, nombres de inicio de sesión, contraseñas y otra información confidencial relacionada. El Cliente entiende que la falta de protección de su Información de Acceso, nombres de inicio de sesión, contraseñas y otra información confidencial relacionada puede permitir que una persona o entidad no autorizada acceda a los Servicios y/o haga que los Servicios sean menos efectivos o ineficaces. La falta de seguridad adecuada por parte del Cliente anulará las obligaciones de IPLAN bajo este acuerdo.

4.6 El Cliente reconoce que la Red de IPLAN y los Servicios son meramente un conducto electrónico y que IPLAN no tiene control sobre el contenido, material, información o datos que pasan a través de la Red de IPLAN y los Servicios, y, por lo tanto, IPLAN no acepta responsabilidad alguna por dicho contenido, material, información o datos. El Cliente es el único responsable y está obligado por su propio contenido, material, información o datos que pasen a través de la Red de IPLAN.

5. Indemnización

El Cliente defenderá e indemnizará a IPLAN frente a cualquier pérdida, daño, responsabilidad, acuerdo, costo y gasto (incluyendo, sin limitación, gastos legales y de otros profesionales) incurridos como resultado de cualquier reclamación, demanda, juicio o procedimiento presentado contra IPLAN por un tercero que surja de un incumplimiento de este Acuerdo por parte del Cliente, o que alegue que los datos del Cliente, o el uso de los Servicios por parte del Cliente en violación de este Acuerdo, infringen o se apropian indebidamente de los derechos de propiedad intelectual de un tercero o violan la ley aplicable. El Cliente deberá indemnizar a IPLAN por cualquier daño, honorarios de abogados y costos finalmente adjudicados contra IPLAN como resultado de, o por cualquier monto pagado por IPLAN.

6. Responsabilidad

6.1 El Cliente reconoce y acepta que IPLAN no tiene control sobre Internet, ya que esta consiste en diferentes entidades y redes que son propiedad, operación y control independientes, y que, en ocasiones, los Servicios pueden no estar disponibles debido a interrupciones, fallas o ceses de los servicios de Internet proporcionados por otros proveedores de servicios de Internet o por cualquiera de las redes que conforman Internet, incluyendo, sin limitación, cualquier evento de fuerza mayor.

6.2 El Cliente reconoce y acepta que IPLAN no será responsable por los daños incurridos cuando los Servicios estén temporal o permanentemente no disponibles, incluyendo, sin limitación, debido a interrupciones, fallas o ceses de servicios de Internet por factores externos fuera del control de IPLAN, o debido a cualquier accidente, mal uso o abuso por parte del Cliente, o por un evento de fuerza mayor. Además, el Cliente reconoce que IPLAN puede, a su discreción, modificar o suspender los Servicios en cualquier momento, siempre que IPLAN informe al Cliente con treinta (30) días de aviso previo por escrito.

6.3 Salvo por cualquier incumplimiento, IPLAN no será responsable ante ninguna parte por cualquier violación de seguridad en cualquier red del Clientes, ni por cualquier pérdida, robo o mal uso de información (incluyendo, sin limitación, la Información Confidencial del Clientes), ya que Internet es inherentemente una red insegura y fuera del control de IPLAN. IPLAN no será responsable ante el Cliente por cualquier acceso no autorizado, divulgación o uso de dichas claves de cifrado, ni por la pérdida, robo o mal uso de cualquier información cifrada (incluyendo, sin limitación, la Información Confidencial del Clientes), ya que IPLAN no puede garantizar la seguridad de dichas claves de cifrado.

6.4 SIN PERJUICIO DE LO ANTERIOR, SALVO QUE SE INDIQUE EXPRESAMENTE EN ESTE ACUERDO, IPLAN NO HACE NINGUNA DECLARACIÓN O GARANTÍA DE NINGÚN TIPO EN RELACIÓN CON LOS SERVICIOS, SU USO O NO USO, O LA RED IPLAN (O CUALQUIER PARTE DE ESTA), INCLUYENDO, ENTRE OTROS, COMERCIABILIDAD, IDONEIDAD PARA UN USO PARTICULAR Y NO INFRACCIÓN. EN LA MEDIDA MÁXIMA PERMITIDA POR LA LEY, SE EXCLUYE CUALQUIER DECLARACIÓN O GARANTÍA, YA SEA EXPRESA O IMPLÍCITA, ESTATUTARIA O DE OTRO TIPO, EN RELACIÓN CON LOS SERVICIOS, SU USO O NO USO, O LA RED IPLAN (O CUALQUIER PARTE DE ESTA). EXCEPTO COMO SE ESTABLECE EXPLÍCITAMENTE AQUÍ, IPLAN NO GARANTIZA QUE LOS SERVICIOS Y LA RED IPLAN (O CUALQUIER PARTE DE ESTA) SERÁN PRECISOS, OPORTUNOS, SEGUROS, LIBRES DE INTERRUPCIONES O ERRORES, O DE INTERFERENCIAS EXTERNAS DE CUALQUIER NATURALEZA, O QUE CUALQUIER DEFECTO IDENTIFICADO SERÁ CORREGIDO. SIN LIMITAR LO ANTERIOR, IPLAN ESPECÍFICAMENTE RENUNCIA A CUALQUIER GARANTÍA SOBRE LA PRECISIÓN, OMISIONES, INTEGRIDAD O ACTUALIDAD DE LOS DATOS U OTROS CONTENIDOS PROPORCIONADOS A TRAVÉS DE LOS SERVICIOS. EL CLIENTE RECONOCE QUE, AUNQUE IPLAN UTILIZA ESFUERZOS COMERCIALMENTE RAZONABLES PARA PROPORCIONAR LOS SERVICIOS, LA PRESTACIÓN DE LOS SERVICIOS INVOLUCRA LA POSIBILIDAD DE ERRORES HUMANOS Y DE MÁQUINAS, RETRASOS, INTERRUPCIONES Y PÉRDIDAS, INCLUYENDO, SIN LIMITACIÓN, LA PÉRDIDA INVOLUNTARIA DE DATOS.

6.5 IPLAN no será responsable en ningún caso por interferencias o daños a cualquier dispositivo o los datos contenidos en ellos, en relación con cualquier acceso, uso o participación en los Servicios y la Red IPLAN (o cualquier parte de esta). Además, IPLAN renuncia completamente a cualquier garantía, declaración y responsabilidad en relación con cualquier aspecto de los Servicios y la Red IPLAN (o cualquier parte de esta) que pueda ser proporcionado por terceros, incluyendo, entre otros, proveedores de servicios de banda ancha y telecomunicaciones, y no será responsable bajo ninguna circunstancia por el incumplimiento, falta de acción o negligencia de dichos proveedores externos.

6.6 EN LA MÁXIMA MEDIDA APLICABLE SEGÚN LA LEY, BAJO NINGUNA CIRCUNSTANCIA IPLAN, SUS ACCIONISTAS, DIRECTORES, EMPLEADOS O AGENTES SERÁN RESPONSABLES ANTE EL CLIENTE O CUALQUIER OTRA PERSONA O ENTIDAD POR CUALQUIER RECLAMACIÓN DERIVADA O RELACIONADA CON EL OBJETO DE ESTE ACUERDO, LOS SERVICIOS, SU USO O NO USO O LA RED IPLAN, BAJO CUALQUIER TEORÍA LEGAL O EQUITATIVA, POR: (I) CUALQUIER DAÑO INCIDENTAL, ESPECIAL, CONSECUENTE O INDIRECTO O PÉRDIDAS DE BENEFICIOS, O (II) CUALQUIER MONTO, INDIVIDUAL O EN CONJUNTO, QUE EXCEDA LA SUMA TOTAL AGREGADA DE LOS PAGOS REALIZADOS POR EL CLIENTE EN LOS TRES (3) MESES ANTERIORES A LA FECHA EN QUE SURGIÓ LA RECLAMACIÓN O RECLAMACIONES, INDEPENDIENTEMENTE DE SI IPLAN HA SIDO INFORMADO O NO DE TAL POSIBILIDAD. ESTA SECCIÓN NO LIMITA LA RESPONSABILIDAD DE NINGUNA PARTE POR LESIONES CORPORALES O LA MUERTE DE UNA PERSONA.

LAS LIMITACIONES DE RESPONSABILIDAD ESTABLECIDAS EN EL PRESENTE SE APLICARÁN INDEPENDIENTEMENTE DE SI ALGÚN RECURSO PREVISTO EN ESTE ACUERDO FALLA EN SU PROPÓSITO ESENCIAL Y SIN IMPORTAR SI LA RECLAMACIÓN SURGE EN AGRAVIO (INCLUYENDO, SIN LIMITACIÓN, NEGLIGENCIA), CONTRATO, GARANTÍA, RESPONSABILIDAD ESTRICTA U OTRO.

7 Centro De Atención Al Usuario

El Cliente dispone de acceso al Centro de Ayuda IPLAN, donde encontrará los manuales de uso de los servicios y una guía de preguntas técnicas y administrativas frecuentes para resolver las distintas necesidades que se presenten. A su vez, dispone de la Zona de Clientes donde podrá descargar su factura, generar las solicitudes y reclamos técnicos o administrativos y gestionar los servicios contratados. Para el acceso a dicho servicio el Cliente deberá disponer de su código de gestión personal (CGP), disponible en su factura. En caso de ser un Cliente nuevo, el mismo podrá gestionar dicho código a través de la Zona de Clientes en la Web de IPLAN.

Asistencia técnica y reclamos: a través del portal Web www.iplan.com.ar, o bien en forma telefónica al Centro de Atención al Cliente a los teléfonos: 5032-0000 y 0800-345-0000 las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

El Cliente es responsable de mantener actualizada su información de contacto en el sistema que IPLAN pone a disposición de forma tal que eficientice cualquier necesidad de comunicación por parte de IPLAN.

..... **.....**

Firma del Cliente **Aclaración**

FECHA __/__/__