Alcance y descripción del servicio

ANTIVIRUS IPLAN

1. Introducción.

El servicio de Antivirus IPLAN ofrece una amplia cobertura contra distintos tipos de detecciones, permitiendo de forma cotidiana, efectiva y sencilla proteger proactivamente de amenazas conocidas y desconocidas que circulan en la red.

2. Descripción General y Alcance.

El cliente podrá adquirir cualquiera de las soluciones de ESET Latinoamérica y de acuerdo al producto no tendrá restricciones de uso sobre el mismo.

2.1 Componentes del servicio

Los componentes básicos

- Antivirus : ESET NOD32 Antivirus 5 (Mandatorio)
- Antivirus + Firewall : ESET Smart Security 5 (Mandatorio)

2.1.1 ESET NOD32 Antivirus 5 (Mandatorio)

Está orientado a mantener protegido de virus, spyware, troyanos, robo de contraseñas y otras amenazas informáticas, logrando detener nuevas amenazas de forma proactiva, permitiendo explorar y limpiar el tráfico del correo electrónico, con actualizaciones que son muy livianas y de forma automáticas, logrando un alto rendimiento del sistema.

- Antivirus
- Antispyware

2.1.2 ESET Smart Security antivirus 5 (Mandatorio)

Este servicio permitie obtener mayor control del contenido inapropiado que pueda estar circulando en la red, logrando un control parental que proteja de cierta información inapropiada, con protección en línea logrando limpiar en contenido de internet y el correo electrónico, deteniendo posibles amenazas que intenten ingresar mediante dispositivos portátiles, permitiendo compartir con confianza distintos tipos de archivos.

- Antivirus
- Antispyware
- Firewall
- Antispam
- Control parental

2.1.3 Resumen

COMPONENTES	Mandatorio/Opcional
ESET NOD32 Antivirus	Mandatorio
ESET Smart Security	Mandatorio

2.2 ESPECIFICACIONES

2.2.1 ADMINISTRACIÓN

Para lograr una mejor administración el cliente podrá encontrar en el mail de bienvenida un link con videos explicativos.

2.2.2 INSTALACIÓN.

El cliente podrá ingresar al sitio web indicado en el mail de bienvenida con el usuario y password provistos por IPLAN y descargar el software que aplique a la versión de su sistema operativo.

IPLAN proveerá:

- ✓ Las credenciales que permitan descargar el producto.
- ✓ Contacto técnico.
- ✓ Los instructivos de primeros pasos para la puesta en marcha del servicio.

2.2.2.1 Credenciales

IPLAN proveerá usuario y password para descargar el software y será responsabilidad del cliente evitar divulgarla con el fin de mantener la privacidad de la información, siendo su absoluta responsabilidad que terceros no puedan acceder.

3 Activación del Servicio

IPLAN pondrá a disposición el servicio con las condiciones correspondientes a la opción contratada.

IPLAN notificará vía mail al cliente sobre la disponibilidad del servicio contratado, el/los nombres de usuario generados y sus password respectivos, formas de interacción con la plataforma y demás características que hagan a cuestiones operativas del servicio en cuestión.

A partir de la comunicación, y transcurridas 48 hs de efectuada, si el cliente no reclamase a cualquier efecto sobre problema alguno del servicio en cuanto a las características contratadas, IPLAN considerará al servicio como activo y aceptado.

4 Documentación adicional

Centro de Atención al Usuario.

El cliente dispone de acceso al centro de atención al usuario para efectuar reclamos de tipo técnico o administrativo.

Para el acceso a dicho servicio el cliente deberá disponer de su código de gestión personal disponible en su factura.

En caso de ser un cliente nuevo, que aún no haya recibido su primera factura, el cliente podrá gestionar el mismo vía la web de IPLAN.

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.

5. Soluciones y funcionalidades.

A) **ESET NOD32 Antivirus 5 (Antivirus, Antispyware)**

Reputación basada en la nube – Ahora el cliente podrá analizar archivos utilizando una base que se encuentra disponible en la red, esta base registra los archivos analizados, por lo tanto cuando el cliente analice un archivo que previamente fue analizado, el tiempo de análisis se reducirá considerablemente. Adicionalmente podrá determinar si un archivo representa o no una amenaza antes de descargarlo.

Modo de juego – El modo de juego es una característica para los jugadores, que requiere utilizar el software en forma ininterrumpida, no desean que las ventanas emergentes los molesten y quieren minimizar el uso de la CPU. El modo de juego también se puede usar como modo para pasar presentaciones, cuando una presentación no se puede interrumpir por la actividad del programa antivirus.

Sistema de prevención de intrusiones (HIPS) – El Sistema de prevención de intrusiones basado en el host (HIPS) protege su sistema de malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS utiliza el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro, y así bloquear y prevenir en forma activa los intentos de dichas actividades maliciosas.

Exploración más inteligente – Las amenazas no siempre ingresan de la manera que uno espera. ESET NOD32 Antivirus examina los canales de comunicación cifrada SSL como HTTPS y POP3S, y explora en forma inteligente los archivos comprimidos para detectar amenazas que otros productos pasan por alto. La detección proactiva comienza en la etapa más temprana del inicio del sistema para asegurar que su computadora esté siempre protegida.

Correo electrónico limpio y seguro – Explora Microsoft Outlook, Outlook Express, Mozilla Thunderbird, Windows Live Mail, Windows Mail, y otros clientes de correo electrónico POP3/IMAP, asegurando que su correo permanezca libre de virus y otras amenazas.

Control avanzado de medios removibles – Ofrece la posibilidad de definir excepciones para bloquear medios extraíbles según el tipo de medio, el número de serie, el fabricante, el modelo, los parámetros del dispositivo (tamaño, cantidad de cabezales, sectores, etc.) o basándose en la ubicación de un archivo cifrado que identifique el dispositivo. Pueden configurarse los permisos como bloqueados, con acceso de solo lectura o con acceso de lectura y escritura, y también pueden definirse para un usuario específico o para grupos de usuarios.

Herramientas para el sistema – ESET SysInspector simplifica el diagnóstico del sistema permitiendo la exploración profunda de los procesos del sistema para encontrar amenazas ocultas, ESET SysRescue facilita la limpieza de sistemas infectados creando unidades de arranque de rescate en CD, DVD o USB que lo ayudará a reparar una computadora infectada.

Tecnología de Autodefensa – ESET NOD32 Antivirus incluye una tecnología integrada para prevenir que los programas maliciosos lo corrompan o deshabiliten, por lo tanto el cliente podrá estar tranquilo de que su computadora permanecerá siempre protegida.

B) **ESET Smart Security 5 (Antivirus, Antispyware, Firewall, Antispam y Control Parental)**

Control parental – Le permite controlar que sitios web se pueden acceder o no, en forma individual para cada cuenta de Windows. Los usuarios tendrán la posibilidad de establecer un "rol" para cada cuenta. Cada rol tiene opciones predeterminadas de configuración para las categorías de URL que pueden mostrarse (o no) al usuario. Además, el usuario puede establecer listas negras y blancas para cada cuenta de Windows.

Modo de juego – El modo de juego es una característica para los jugadores, que requieren utilizar el software en forma ininterrumpida, no desean que las ventanas emergentes los molesten y quieren minimizar el uso de la CPU. El modo de juego también se puede usar como modo para pasar presentaciones, cuando una presentación no se puede interrumpir por la actividad del programa antivirus.

Reputación basada en la nube – Ahora el cliente podrá analizar archivos utilizando una base que se encuentra disponible en la red, esta base registra los archivos analizados, por lo tanto cuando usted analice un archivo que previamente fue analizado, el tiempo de análisis se reducirá considerablemente. Adicionalmente podrá determinar si un archivo representa o no una amenaza antes de descargarlo.

Sistema de prevención de intrusiones (HIPS) – El Sistema de prevención de intrusiones basado en el host (HIPS) protege el sistema del cliente de malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS utiliza el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro, y así bloquear y prevenir en forma activa los intentos de dichas actividades maliciosas.

Exploración más inteligente – Las amenazas no siempre ingresan de la manera que uno espera. ESET Smart Security examina los canales de comunicación cifrada SSL como HTTPS y POP3S, y explora en forma inteligente los archivos comprimidos para detectar amenazas que otros productos pasan por alto. La función de Optimización Inteligente de ESET hace que la exploración de archivos sea más veloz que nunca.

Firewall personal – El Modo de Aprendizaje ahorra tiempo ya que crea automáticamente reglas de firewall tras observar cómo los usuarios finales utilizan la red, también cuenta con la opción de Modo Avanzado para usuarios más experimentados. Además, permite que el usuario seleccione perfiles personalizados de firewall para zonas de red confiables y que se apliquen reglas adecuadas automáticamente según la red detectada.

Autenticación de zonas de confianza – Esta función permite identificar las zonas de red confiables por medio de las configuraciones de red (una combinación configurable de la dirección IP del servidor principal / DNS/ DHCP, red inalámbrica SSID, el perfil de conexión, etc.) y realizar la autenticación segura para el acceso a una red usando el Servidor de Autenticación de ESET.

Antispam mejorado – ESET Smart Security ahora se encarga de los molestos mensajes de correo no deseados con un filtro para spam más pequeño, veloz y eficaz. Se integra con los clientes de correo electrónico más populares, Windows Mail, Windows Live Mail y Mozilla Thunderbird.

Control avanzado de medios removibles – Ofrece la posibilidad de definir excepciones para bloquear medios extraíbles según el tipo de medio, el número de serie, el fabricante, el modelo, los parámetros del dispositivo (tamaño, cantidad de cabezales, sectores, etc.) o basándose en la ubicación de un archivo cifrado que identifique el dispositivo. Pueden configurarse los permisos como bloqueados, con acceso de solo lectura o con acceso de lectura y escritura, y también pueden definirse para un usuario específico o para grupos de usuarios.

Herramientas para el sistema – ESET SysInspector simplifica el diagnóstico del sistema permitiendo la exploración profunda de los procesos del sistema para encontrar amenazas ocultas, ESET SysRescue facilita la limpieza de sistemas infectados creando unidades de arranque de rescate en CD, DVD o USB que lo ayudará a reparar una computadora infectada.

Tecnología de Autodefensa – ESET Smart Security incluye una tecnología integrada para prevenir que los programas maliciosos lo corrompan o deshabiliten, por lo tanto podrá estar tranquilo de que su computadora permanecerá siempre protegida.

6 Actualizaciones.

Las mismas serán gratuitas y se podrán descargar de manera automática o manual.

En caso de clientes Business podrán crear un mirror de actualización desde la consola de administración ESET Remote Administrator.

7 Acuerdo de servicio.

Los siguientes puntos muestran el detalle de los servicios.

- Se brindara soporte ante incidentes de la plataforma de ANTIVIRUS IPLAN y conectividad en modalidad 7 x 24 x 365.
- Disponibilidad comprometida de la plataforma de ANTIVIRUS IPLAN.

8 Limitaciones del Servicio.

IPLAN no se hace responsable por la integridad, inconsistencia y/o pérdida de los datos que puedan ocasionar las fallas que involucren a los componentes del equipo adquiridos (hardware o software) ni errores humanos de terceros ajenos a IPLAN.

IPLAN no se hace responsable ante el caso fortuito de pérdida de datos y su respectivo Backup.

IPLAN no admite prácticas de SPAM por parte de sus clientes. Si IPLAN detectara tal situación, se procederá a dar de baja los servicios contratados. El cliente manifiesta y se compromete a no efectuar prácticas de SPAM a través de los servicios que contrata con IPLAN.

Ante cualquier duda el cliente deberá contactarse con el Centro de Atención al Cliente en iplan.com.ar/contacto

…… ……

Firma del Cliente Aclaración

Fecha _ _/_ _/_ _