DESCRIPCIÓN Y ALCANCE DEL SERVICIO DE NSS S.A.
SEGURIDAD DIGITAL ESET

1. Introducción

El servicio Seguridad digital ESET ofrece protección completa para endpoints corporativos, datos personales y empresariales y redes a través de distintos bundles de protección.

IPLAN es Partner de ESET, empresa líder en seguridad digital, reconocida mundialmente por su innovación y soluciones avanzadas para proteger a usuarios y organizaciones de amenazas digitales. Con una sólida reputación en la industria.

ESET utiliza tecnologías de vanguardia y una inteligencia artificial de alto rendimiento para ofrecer una protección integral frente a virus, malware, ransomware y otras amenazas emergentes.

2. Servicio

La plataforma ESET PROTECT funciona en la nube sobre infraestructura administrada por ESET. Cualquier cambio, actualización o trabajo sobre su infraestructura estará a cargo de ESET.

IPLAN funciona como revendedor autorizado de los productos ESET.

2.1. Variantes del Servicio

El servicio Seguridad digital ESET contempla las siguientes opciones:

- ESET PROTECT Entry
- ESET PROTECT Advanced
- ESET PROTECT Complete
- ESET PROTECT Elite

Cada uno de estos productos constituye un bundle de seguridad que comprende varios componentes.

La siguiente tabla resume los principales componentes y funcionalidades de los bundles de protección ESET PROTECT:

Componentes / Funcionalidades	PROTECT ENTRY	PROTECT ADVANCED	PROTECT COMPLETE	PROTECT ELITE
Consola de gestión basada en la nube	✔	✔	✔	✔
Protección moderna de endpoints	✔	✔	✔	✔
Seguridad para servidores	✔	✔	✔	✔
Defensa contra amenazas móviles		✔	✔	✔
Cifrado de disco completo		✔	✔	✔
Defensa avanzada contra amenazas		✔	✔	✔
Gestión de vulnerabilidades y parches			✔	✔
Seguridad del servidor de correo			✔	✔
Protección de aplicaciones en la nube			✔	✔
Detección y respuesta extendida (XDR)				✔
Autenticación en múltiples factores				✔

A su vez, se encuentra disponible el servicio ESET Cloud Office Security (ECOS), el cual ofrece protección de aplicaciones en la nube. Proporciona protección preventiva avanzada para aplicaciones de Microsoft 365 y Google Workspace.

Comprende funcionalidades como:

- Antispam
- Anti-phishing
- Antimalware
- Defensa avanzada contra amenazas 0 day
- Protección automática
- Administración de cuarentena

Componentes/ Funcionalidades	ECOS
Consola de gestión basada en la nube	✔
Protección para Exchange on line y Gmail	✔
Protección para Onedrive y Google Drive	✔
Protección para Sharepoint on line	✔
Protección para Teams	✔

2.2. Descripción de Funcionalidades:

Consola de gestión remota basada en la nube: ESET PROTECT es una herramienta remota multifuncional basada en la nube para la administración de la seguridad de red de los productos de seguridad corporativos de ESET en todos los sistemas operativos. Permite implementar la seguridad fácilmente y suministra visibilidad de la red sin necesidad de tener hardware adicional, lo que reduce el costo total de propiedad.

Protección moderna de endpoints: Brinda múltiples capas de protección y es capaz de detectar malware antes, durante y después de su ejecución. El machine learning, el análisis de comportamiento avanzado, los macrodatos y la experiencia humana, equilibran el rendimiento, la detección y los falsos positivos. Incluye:

- Antivirus de próxima generación
- Protección contra ataques de red bloqueando el tráfico de red malicioso directamente en los endpoints.
- Control de dispositivos: permite restringir el uso de dispositivos no autorizados.
- Anti-Phishing:

Protección para servidores: Protección avanzada en tiempo real para todos los servidores generales de almacenamiento de archivos de red y servidores multipropósito para garantizar la continuidad del negocio. Incluye protección contra Ransomware, prevención de fuga de datos y protección ante botnets.

Defensa contra amenazas móviles: Seguridad para todos los dispositivos móviles Android e IOS dentro de la organización

Cifrado de disco: Solución de cifrado de discos de sistema, particiones o dispositivos completos que permiten el cumplimiento de normas legales. El cifrado de disco completo aumenta la seguridad de los datos de su organización y lo ayuda a cumplir con las normativas de protección de datos.

Gestión de vulnerabilidades y parches: Rastrea y corrige de forma activa las vulnerabilidades de los sistemas operativos y las aplicaciones en todos los endpoints.

Seguridad del servidor de correo: Ofrece una capa adicional de seguridad a los servidores de correo Exchange. Cuenta con funciones avanzadas antiphishing, antimalware y antispam. Evita el ransomware.

Protección de aplicaciones en la nube: Protección avanzada para apps Microsoft 365 y Google Workspace, con defensa proactiva de amenazas.

Detección y respuesta extendida (XDR): Capacidad adicional de la plataforma para detectar proactivamente amenazas, identificar de manera efectiva comportamientos anómalos en la red y realizar una remediación oportuna, previniendo brechas de datos y alteraciones en el negocio.

Autenticación en múltiples factores: Autenticación basada en el móvil con un solo toque que protege a las organizaciones de contraseñas débiles y accesos no autorizados.

3. Requisitos técnicos

Para una correcta elección del servicio, el cliente deberá verificar previamente a la instalación de las licencias el cumplimiento de los requisitos de sistema operativos que se encuentran detallados a

continuación para cada uno de los bundles.

- **ESET PROTECT Entry**

  Para computadoras:
  - Microsoft Windows 11, 10, 8.1, 8, 7, SP1
  - macOS 10.12 y posterior
  - Ubuntu Desktop 20.04 LTS y 18.04 LTS 64-bit
  - RedHat Enterprise Linux 7, 8 64-bits (RHEL) Desktop
  - SUSE Linux Enterprise Desktop 15 64-bits

  Para smartphones y tablets:
  - Android 5 (Lollipop) y posterior
  - iOS 9 y posterior

  Para servidores de archivos:
  - Microsoft Windows Server 2022, 2019, 2016, 2012, 2008, R2 SP1
  - Microsoft Windows Server Core 2012, 2008R2
  - Microsoft Windows Small Business Server 2011
  - RedHat Enterprise Linux (RHEL) 7, 8, 9
  - CentOS 7
  - Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS
  - Debian 10, 11
  - SUSE Linux Enterprise Server (SLES) 12, 15
  - Oracle Linux 8
  - Amazon Linux 2

- **ESET PROTECT Advanced**

  Para computadoras:
  - Microsoft Windows 11, 10, 8.1, 8, 7
  - ARM64: Algunas funcionalidades o características no están soportadas en Microsoft Windows sobre ARM.
  - macOS 10.12 y posteriores. ESET Endpoint Antivirus para macOS version 7 y posteriores, proveen soporte nativo para dispositivos Apple con chips ARM
  - Ubuntu Desktop 18.04 LTS 64-bit and RedHat Enterprise Linux (RHEL) Desktop 7 64-bit

  Para smartphones y tablets:
  - Android 5 (Lollipop) y posterior
  - iOS 9 y posterior

  Para servidores de archivos:
  - Microsoft Windows Server 2022, 2019, 2016, 2012, 2008, R2 SP1
  - Microsoft Windows Server Core 2012, 2008R2
  - Microsoft Windows Small Business Server 2011
  - RedHat Enterprise Linux (RHEL) 7, 8, 9
  - CentOS 7
  - Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS
  - Debian 10, 11
  - SUSE Linux Enterprise Server (SLES) 12, 15
  - Oracle Linux 8
  - Amazon Linux 2

- **ESET PROTECT Complete**

  Para computadoras:
  - Microsoft Windows 11, 10, 8.1, 8, 7
  - ARM64: Algunas funcionalidades o características no están soportadas en Microsoft Windows sobre ARM.
  - macOS 10.12 y posteriores. ESET Endpoint Antivirus para macOS version 7 y posteriores, proveen soporte nativo para dispositivos Apple con chips ARM
  - Ubuntu Desktop 18.04 LTS 64-bit and RedHat Enterprise Linux (RHEL) Desktop 7 64-bit

  Para smartphones y tablets:
  - Android 5 (Lollipop) y posterior
  - iOS 9 y posterior

  Para servidores de archivos:
  - Microsoft Windows Server 2022, 2019, 2016, 2012, 2008, R2 SP1
  - Microsoft Windows Server Core 2012, 2008R2
  - Microsoft Windows Small Business Server 2011
  - RedHat Enterprise Linux (RHEL) 7, 8, 9
  - CentOS 7
  - Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS
  - Debian 10, 11
  - SUSE Linux Enterprise Server (SLES) 12, 15
  - Oracle Linux 8
  - Amazon Linux 2

  Para servidores de correo:
  - Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007
  - Microsoft Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008 SP2
  - Microsoft Small Business Server 2011

  Para la protección de aplicaciones en la nube:
  - Suscripciones para Microsoft 365 o Google Workspace para conectar con su instancia (exchange Online, OneDrive, SharePoint Online, Teams, Gmail, Google Drive)

- **ESET PROTECT Elite**

  Para computadoras:
  - Microsoft Windows 11, 10, 8.1, 8, 7
  - ARM64: Ten en cuenta que en Microsoft® Windows® en ARM, algunas características y funcionalidades no son compatibles. Más información
  - macOS 10.12 y posterior. ESET Endpoint Antivirus para macOS versión 7 en adelante brinda soporte nativo para chips Apple basados en ARM.
  - Ubuntu Desktop 18.04 LTS 64-bit y RedHat Enterprise Linux (RHEL) Desktop 7 64-bit

  Para smartphones y tablets:
  - Android 5 (Lollipop) y posterior
  - iOS 9 y posterior

  Para servidores de archivos:
  - Microsoft Windows Server 2022, 2019, 2016, 2012, 2008, R2 SP1

- Microsoft Windows Server Core 2012, 2008R2
- Microsoft Windows Small Business Server 2011
- RedHat Enterprise Linux (RHEL) 7, 8, 9
- CentOS 7
- Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS
- Debian 10, 11
- SUSE Linux Enterprise Server (SLES) 12, 15
- Oracle Linux 8
- Amazon Linux 2

Para servidores de correo:

- Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008 SP2
- Microsoft Small Business Server 2011
- IBM Domino 6.5.4 y posterior
- HCL Domino 11

Para la protección de aplicaciones en la nube:

- Suscripciones para Microsoft 365 o Google Workspace para conectarse con el tenant (Exchange Online, OneDrive, SharePoint Online, Teams, Gmail, Google Drive

- **ESET CLOUD OFFICE SECURITY**

Navegadores compatibles:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome
- Opera
- Safari

Requisitos:

- Un plan de suscripción compatible a Microsoft 365
- Acceso a Azure Active Directory (Azure AD) con permisos de administrador
- Servicios en la nube de Azure – Exchange | OneDrive | Sharepoint | Teams
- Una cuenta en ESET PROTECT Hub
- Planes de suscripción de Google Workspace compatibles
- Acceso de administrador a la cuenta de Google Workspace
- Una cuenta en ESET PROTECT Hub

4. Instalación

IPLAN proporcionará al cliente, mediante un correo de activación:

- Las credenciales necesarias para gestionar las licencias adquiridas.
- Instructivos con los primeros pasos para la puesta en marcha del servicio.
- Información de contacto para soporte técnico.

Responsabilidad del cliente:

- Definir los dispositivos que desea proteger con el servicio.
- Realizar la instalación y activación de las licencias correspondientes, siguiendo las instrucciones provistas y considerando la versión de su sistema operativo.

También es responsabilidad del cliente evitar divulgar las credenciales enviadas por IPLAN con el fin de mantener la privacidad de la información, siendo su absoluta responsabilidad que terceros no puedan acceder.

5. 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 formas de interacción con la plataforma y demás características que hagan a cuestiones operativas del servicio en cuestión.

A partir de que IPLAN comunique la disponibilidad del servicio contratado se dará por activado y comenzará a ser facturado. En el transcurso de las 72 hs posteriores el cliente podrá comunicarse con el implementador a cargo, para recibir asistencia ante eventuales consultas.

6. Actualizaciones.

Los productos ESET PROTECT incluyen una función configurable para mantener los productos de seguridad actualizados a la versión más reciente.

7. Limitaciones del servicio

Las funciones y prestaciones específicas del servicio las define ESET directamente y no son modificables por IPLAN.

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 producto adquirido (hardware o software) ni errores humanos de terceros ajenos a IPLAN.

El Cliente al contratar el servicio expresamente acepta que la prestación del servicio se regirá por las condiciones generales y particulares de prestación de servicios de NSS S.A., así como también por los términos de uso de los productos, sitios web y servicios de ESET que en forma previa leyó y comprendió y en virtud de ello aceptó, y que se encuentran publicados en los siguientes links https://help.eset.com/protect_cloud/es-CL/terms_of_use.html?terms_of_use.html,

https://help.eset.com/protect_cloud/es-CL/agent_eula.html y/o los que en el futuro los reemplacen y sean dispuestos por ESET para la prestación de sus servicios.

8. Centro de Atención al Usuario

El Cliente 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.

A su vez, podrá solicitar asistencia técnica y/o realizar reclamos a través del portal Web www.iplan.com.ar, vía Whatsapp escribiendo al 1150320000, o en forma telefónica al Centro de Atención al Cliente al teléfono 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 / /