Condiciones particulares del Servicio Tu Empresa Segura

1. CONDICIONES PARTICULARES Y SU ACEPTACIÓN.

Las Condiciones Particulares descritas a continuación (en adelante, las "Condiciones Particulares") regulan las relaciones entre TELEFÓNICA DE ESPAÑA, S.A.U. (en adelante, "Telefónica Empresas"), con CIF A82018474 y domicilio social en C/ Gran Vía nº 28, 28013, Madrid, inscrita en el Registro Mercantil de Madrid al tomo 13.170; libro 0; sección 8ª; hoja M-213.180 y el Cliente del Servicio (en adelante, el "Cliente") en todo lo relativo a prestación del Servicio Tu Empresa Segura (en adelante el "Servicio" o "Tu Empresa Segura"), de conformidad con la modalidad contractual elegida por el Cliente en el Contrato al que se incorporan las presentes Condiciones. La aceptación sin reservas de las presentes Condiciones deviene indispensable para la prestación del servicio "Tu Empresa Segura" por parte de Telefónica Empresas.

El Cliente manifiesta, en tal sentido, haber leído, entendido y aceptado las presentes Condiciones Particulares, puestas a su disposición, en todo momento, con carácter previo a la contratación en la siguiente página web: http://www.movistar.es/rpmm/estaticos/empresas/PDF_Aplicateca/ciberseguridad-empresas/contrato-tu-empresa-segura.pdf

La utilización del Servicio conlleva, asimismo, la aceptación por parte del Cliente de cuantos avisos, reglamentos de uso e instrucciones fueren puestos en su conocimiento por parte de Telefónica Empresas con posterioridad a la aceptación de las presentes Condiciones Particulares; su no aceptación, dentro del plazo al efecto otorgado, conllevará la finalización del Servicio por parte del Cliente.

Las presentes Condiciones completan, en lo no previsto en las mismas, a las Condiciones Generales del servicio Fusión Digital y a las Condiciones Generales de Internet Banda Ancha, y el resto de las condiciones que sean de aplicación a los Servicios contratados

2. DESCRIPCIÓN DEL SERVICIO

El servicio TU EMPRESA SEGURA está formado por un conjunto de tecnologías o herramientas de seguridad, especializadas en la detección y prevención de las principales amenazas de seguridad informática que afectan a dispositivos, redes y aplicaciones en nube.

En las modalidades Básica, Avanzada y Premium cuenta, además, con el soporte y administración en remoto de todas las herramientas incluidas por parte de un grupo de especializado en las mismas, el SOC Pyme.

El SOC Pyme es un grupo de expertos del Centro de Operaciones de Seguridad (SOC, Security Operations Center) dedicados específicamente al segmento pyme y a las necesidades de seguridad de las empresas de este segmento

El servicio se comercializa en un formato de Paquetes de servicio en una de las 4 modalidades existentes.

2.1 Modalidad Paquete Lite

La modalidad **Paquete Lite** incluye una solución para la protección de dispositivos (PCs Windows únicamente) de manera autogestionada por el cliente con los siguientes componentes:

- Suministro de una aplicación software (1 licencia por cada unidad contratada) de protección Antivirus, en tiempo real, que incluye además la funcionalidad de firewall, control de la navegación y protección del correo en el dispositivo en el que se instala.

- Un curso de concienciación en seguridad en la plataforma que ofrece el servicio para tantos usuarios como unidades se contrate.

En el Anexo IV Modalidad Paquete Lite, se encuentra recogida una descripción más detallada de las funcionalidades, el alcance y las condiciones que aplican a la contratación de este paquete de servicio.

2.2 Modalidad Paquete Básico

La modalidad **Paquete Básico**, que incluye el uso de herramientas centradas en la seguridad de los dispositivos fijos y móviles de los usuarios de la empresa. Para ello se proporciona al Cliente:

- Una solución de Antivirus, en tiempo real, que incluye además la funcionalidad de firewall y control de la navegación en los dispositivos en los que se instala (PCs, Smartphones y Tablets)
- Una solución en nube por la que pasará el correo de la empresa y en la que se podrán establecer unas políticas de filtrado. La solución permite detectar correo malicioso y configurar reglas para actuar en consecuencia.

Por cada usuario contratado se proporcionará:

- 1 licencia de la solución de antivirus que permite la instalación del software en hasta 5 dispositivos diferentes del usuario.
- Licencia de uso de la plataforma de filtrado de correo para 1 buzón de correo electrónico de 1 dominio del Cliente.

El Cliente contará con el apoyo del SOC Pyme para la puesta en marcha del servicio así como con el soporte, mantenimiento y administración en remoto de estas dos soluciones.

En el Anexo V Modalidad Paquete Básico, se encuentra recogida una descripción más detallada de las funcionalidades, el alcance y las condiciones que aplican a la contratación de este paquete de servicio.

2.3 Modalidad Paquete Avanzado

La Modalidad **Paquete Avanzado** incluye las funcionalidades ya descritas en el párrafo anterior para el Paquete Básico y además equipamiento con funcionalidad de firewall que **se desplegará en la sede del cliente**, en su conexión con Internet, como barrera de control para prevenir, detectar y actuar sobre posibles amenazas de seguridad que llegaran por esta vía.

Se complementa la oferta de este paquete, incluyendo un curso de formación online de concienciación en seguridad para los usuarios del Cliente. El objetivo de este curso es que los empleados adquieran unas nociones básicas en seguridad que después puedan aplicar en el trabajo que desempeñan.

Por cada usuario contratado se proporcionará:

- 1 licencia de la solución de antivirus que permite la instalación del software en hasta 5 dispositivos diferentes del usuario.
- Licencia de uso de la plataforma de filtrado de correo para 1 buzón de correo electrónico de 1 dominio del Cliente.
- Curso de concienciación.

Para la sede se proporcionará:

- Equipamiento firewall UTM desplegado en la sede. El equipamiento se dimensionará de acuerdo con el número de usuarios para los que se ha hecho la contratación del paquete.
  El Cliente tiene la opción de elegir en el momento de la contratación, si desea que el equipamiento sea el modelo inmediatamente superior al incluido por defecto en el paquete para el número de usuarios indicado.

El Cliente también tiene la opción de elegir en el momento de la contratación si desea que se desplieguen 2 dispositivos con el fin de conseguir la funcionalidad de alta disponibilidad en su sede.

El Cliente tendrá que permitir el acceso al técnico de Telefónica para la instalación en dependencias del Cliente del equipamiento hardware incluido en este paquete de servicio.

El Cliente contará con el apoyo del SOC Pyme para la puesta en marcha del servicio, así como con el soporte, mantenimiento y administración en remoto de las soluciones incluidas.

En el Anexo VI Modalidad Paquete Avanzado, se encuentra recogida una descripción más detallada de las funcionalidades, el alcance y las condiciones que aplican a la contratación del Paquete Avanzado del servicio.

2.4 Modalidad Paquete Premium

La modalidad **Paquete Premium**, que incluye todas las funcionalidades ya indicadas en el Paquete Avanzado y además una solución CASB específica para Clientes que tengan licencias E3 de Microsoft y utilicen como aplicaciones corporativas de su empresa los productos cloud: Mail O365, Teams, Sharepoint y Onedrive de la suite de Microsoft de manera que se puedan aplicar políticas de seguridad a medida que se acceda a estos recursos en nube desde cualquier dispositivo.

Por cada usuario contratado se proporcionará:

- 1 licencia de la solución de antivirus que permite la instalación del software en hasta 5 dispositivos diferentes del usuario.
- Licencia de uso de la plataforma de filtrado de correo para 1 buzón de correo electrónico de 1 dominio del Cliente.
- Curso de concienciación.
- 1 licencia de la solución CASB

Para la sede se proporcionará:

- Equipamiento firewall UTM desplegado en la sede. El equipo se dimensionará de acuerdo con el número de usuarios para los que se ha hecho la contratación del paquete.

  El Cliente tiene la opción de elegir en el momento de la contratación, si desea que el equipamiento sea el modelo inmediatamente superior al incluido por defecto en el paquete para el número de usuarios indicado.
  El Cliente también tiene la opción de elegir en el momento de la contratación si desea que se desplieguen 2 dispositivos con el fin de conseguir la funcionalidad de alta disponibilidad en su sede.

El Cliente tendrá que permitir el acceso al técnico de Telefónica para la instalación en dependencias del Cliente del equipamiento hardware incluido en este paquete de servicio.

El Cliente contará con el apoyo del SOC Pyme para la puesta en marcha del servicio así como con el soporte, mantenimiento y administración en remoto de las soluciones incluidas.

En el Anexo VII Modalidad Paquete Premium, se encuentra recogida una descripción más detallada de las funcionalidades, el alcance y las condiciones que aplican a la contratación de este Paquete Premium del servicio.

El Cliente podrá elegir el paquete de servicio que mejor se ajuste a sus necesidades asociado a su sede. Si el Cliente tiene varias sedes, podrá contratar paquetes en distintas modalidades para cada una de sus sedes.

2.5 Módulos Adicionales

Además del paquete de servicio, se ofrecen 4 módulos contratables adicionales, que el Cliente puede añadir a su contrato si lo desea

- **Firma Digital.** Es una solución que permite la firma digital de documentos pdf mediante firma biométrica y firma por OTP (contraseña de un solo uso).
  Por cada unidad contratada se pone a disposición del Cliente un paquete de hasta 250 firmas al año.
  Este módulo adicional puede contratarse en cualquier momento durante la vigencia del servicio y tantas unidades como el cliente desee. Es compatible con las modalidades de paquete Básico, Avanzado y Premium.

- **Buzones adicionales de correo limpio.** Permite la contratación de licencias adicionales de la solución de filtrado de correo. Por cada unidad contratada se da licencia de uso de la plataforma de filtrado de correo para 1 buzón adicional de correo electrónico de un dominio del Cliente.
  Este módulo adicional puede contratarse en cualquier momento durante la vigencia del servicio y tantas unidades como el cliente desee.
  Es compatible con las modalidades de paquete Básico, Avanzado y Premium.

- **Puesta en marcha.** 1 unidad de este opcional incluye la instalación y configuración inicial de hasta 5 aplicaciones de las incluidas en el servicio. Como aplicación se entiende:
  - Antivirus/Antiransomware y Navegación Segura. Instalación en 1 dispositivo de 1 usuario (aplicaría a todos los paquetes)
  - Acceso remoto VPN. Instalación y configuración del acceso de 1 usuario a la sede de la empresa (aplicaría a paquetes Avanzado y Premium)

  Incluye también la configuración del Correo Limpio, así como un recorrido por el portal del servicio y explicación de los informes del mismo.
  Este módulo adicional puede contratarse en cualquier momento durante la vigencia del servicio y tantas unidades como el cliente desee.
  Es compatible con las modalidades de paquete Básico, Avanzado y Premium.

- **Visita.** Es la visita de un técnico en domicilio del cliente para una actuación sobre el equipo firewall UTM que se incluye en las modalidades Paquete Avanzado y Premium.

  Este módulo adicional puede contratarse en cualquier momento durante la vigencia del servicio (no en el alta del servicio donde la visita ya está incluida) y tantas veces como sea necesario.
  Es compatible con las modalidades de paquete Avanzado y Premium.
- **Protección de la identidad.** Es un servicio de detección de filtraciones de datos en la *Dark Web* (“Web oscura”) de elementos que forman parte de la identidad de la pyme, (nombre, CIF, IPs, dirección postal, teléfonos y direcciones de correo del dominio asociado a la pyme)
  Este módulo adicional puede contratarse en cualquier momento durante la vigencia del servicio como una única unidad asociada a una sede.
  Es compatible con las modalidades de paquete Básico, Avanzado y Premium.

3. INICIO DEL SERVICIO Y DURACIÓN.

El contrato entrará en vigor el día siguiente de su firma y tendrá una vigencia indefinida.

En el caso de Modalidad Paquete Básico, no existe ningún periodo de vigencia mínima, en caso de los Paquetes Avanzados y Premium tendrán una vigencia mínima de 12 meses, aplicándose la penalización correspondiente según la modalidad contratada si el Cliente causa baja anticipada en el servicio o reduce el número de usuarios durante este periodo de vigencia.

La fecha de inicio de aplicación de las Condiciones será la del día siguiente a la fecha de puesta en servicio del Paquete o Módulo adicional.

El alta efectiva del Paquete se notificará al Contacto Técnico proporcionado en el momento de la contratación de TU EMPRESA SEGURA, informándole de la disponibilidad del Servicio y dándole acceso en ese momento al portal web en el caso de las modalidades paquete Básico, Avanzado o Premium o a la licencia del paquete Lite en caso de contratar esta modalidad.

El alta efectiva del servicio de Módulo adicional, en caso de haberlo contratado, se producirá también mediante notificación vía correo electrónico al Contacto Técnico.

4. OBLIGACIONES DEL Cliente

4.1 Precio del Servicio

Como contraprestación por el Servicio el Cliente vendrá obligado a satisfacer el precio correspondiente a cada paquete y unidades de los módulos adicionales de conformidad con los precios vigentes en cada momento. Los precios actuales, están reseñados en el cuadro de Precios que figura en el Anexo I.

4.2 Modificaciones de precios.

Cualquier modificación en los precios aplicables, será comunicada por Telefónica Empresas al Cliente a través de cualquiera de los medios previstos en la cláusula 11. Comunicaciones de las presentes Condiciones Particulares con un (1) mes de antelación. En tal supuesto, el Cliente tendrá derecho a resolver la relación de prestación de servicio regulada en las presentes Condiciones Particulares sin penalización alguna por este concepto, sin perjuicio de otros compromisos adquiridos por el propio Cliente.

4.3 Facturación y Pago

Telefónica Empresas facturará al Cliente las sumas previstas conforme al Anexo I

- Todos los conceptos facturables en virtud de la prestación del Servicio se facturarán a mes vencido, con carácter mensual y se incorporarán en la factura correspondiente a la prestación por Telefónica Empresas del servicio Fusión Digital o Servicio Internet Banda Ancha.

- El pago correspondiente al Servicio será exigible desde el momento que se presente al cobro la factura correspondiente al servicio de Fusión Digital o Servicio Internet Banda Ancha de que dispusiere el Cliente, y se realizará a través de la cuenta del mismo en la Entidad Bancaria o Caja de Ahorros que para tal efecto señale o, en su defecto, en lugar habilitado por Telefónica Empresas, a su presentación al cobro, que constará expresamente en el aviso de pago enviado al Cliente.

- La primera cuota será prorrateada en función de la fecha de entrada en vigor del Servicio.

- la baja anticipada de todo o parte del SERVICIO con compromiso de permanencia (paquetes Avanzado y Premium), obliga al Cliente a satisfacer a Telefónica Empresas las cuotas pendientes de lo estipulado en el contrato inicial hasta completar las cuotas comprometidas, las cuales serán pasadas a cobro mediante la emisión de una factura adicional.

Asimismo, en el supuesto de impago, los datos relativos a la deuda podrán ser comunicados a las siguientes entidades dedicadas a la gestión de sistemas de información crediticia: ASNEF, sistema gestionado por la mercantil EQUIFAX IBERICA S.L. y BADEXCUG, sistema gestionado por la mercantil Experian Bureau de Crédito, S.A. y cualesquiera otra que sea comunicada oportunamente al Cliente.

4.4 Requisitos necesarios durante la contratación del servicio.

- Mantener el presente contrato durante el periodo establecido en la cláusula 3 de estas Condiciones.
- Abonar a Telefónica Empresas el precio del Servicio. En caso de impago, será de aplicación lo dispuesto en la cláusula 5.2 de las presentes Condiciones.
- Si el cliente da de baja la sede, se dará de baja también todo lo que tenga contratado en dicha sede del servicio Tu Empresa Segura.
- No está permitido contratar paquetes en modalidades diferentes en una misma sede.
- Cada paquete incluye unos servicios por defecto sin posibilidad de contratar sólo alguno de ellos ni de modificarlos.
- El número de usuarios contratados por paquete (sede) debe estar obligatoriamente entre 4, como mínimo, y 200 como máximo, excepto en la modalidad paquete Lite en donde el número de unidades contratables empieza en 1.
- Para la instalación del software que protege los dispositivos éstos deben cumplir con los siguientes requisitos:

    - Modalidad Paquete Lite:
        - Dispositivos con Sistema Operativo: Windows 7 con Service Pack 1, Windows 8.1, Windows 10 y Windows 11
        - 2GB de RAM (como mínimo)
        - 2,5GB de espacio libre en disco (como mínimo)
        - Internet Explorer versión 11 (como mínimo)

    - Modalidad Paquete Básico, Avanzado y Premium:
        - En PCs:
            - Procesador a 2GHz y 3 GB de RAM (como mínimo)
              Los sistemas operativos soportados pueden consultarse en cualquier momento en la web: https://www.movistar.es/empresas/soluciones-digitales/ciberseguridad-empresas, en el apartado ***Preguntas frecuentes***
        - En dispositivos móviles
            - Versión 5 o posterior en caso de Sistema Operativo Android
            - versión 10 o posterior en caso de Sistema Operativo iOS.

- El cliente debe tener un dominio de correo propio para poder hacer uso de la

plataforma de Correo Limpio que se incluye en los paquetes Básico, Avanzado y Premium.

- La modalidad paquete Básico, Avanzado o Premium tiene que contratarse para la totalidad de usuarios del dominio o dominios de correo a analizar con la plataforma. Si con la contratación de los paquetes para los usuarios, no se cubre la totalidad de los buzones de correo, el Cliente deberá contratar adicionalmente tantas unidades del módulo de Correo Limpio como sea necesario hasta llegar a incluir todos los buzones existentes en el dominio o dominios dados de alta en el SERVICIO.
- En este sentido, Telefónica monitorizará activamente el número de buzones protegidos comparándolo con lo especificado en este contrato, en caso de detectarse una desviación superior a lo estipulado en el contrato de forma continuada, Telefónica notificará al Cliente dicha situación anómala para que tome medidas o regularice la situación. En caso de un incumplimiento repetido (2 meses) que no se resuelva por parte del Cliente, telefónica se reserva el derecho de la cancelación total o parcial del presente servicio.
- Para la contratación de los paquetes Avanzado y Premium el cliente debe tener una dirección IP fija.

- Dado que en la contratación de los paquetes Avanzado y Premium se dimensiona el modelo de dispositivo a desplegar en la sede del Cliente en función del número de usuarios contratados en el paquete, podrían verse mermadas las prestaciones del servicio al Cliente en caso de que el número de usuarios que trabajen en dicha sede (utilicen la conectividad) sea superior al indicado. Cualquier problema derivado de un incorrecto dimensionamiento por esta causa será responsabilidad exclusiva del Cliente.

Para la instalación del equipamiento incluido en el Paquete Avanzado y en el Paquete Premium, será responsabilidad del Cliente

- Gestionar las autorizaciones de entrada del personal de Telefónica a las dependencias del Cliente en caso de que sea necesario para la ejecución del proyecto contratado.
- Asignar un interlocutor único como responsable del proyecto, y definir las personas de contacto autorizadas para realizar consultas
- Tener preparado todo lo necesario para la instalación. Puede consultarse en el Anexo VI y VII.

4.5 Uso correcto del SERVICIO

El Cliente se compromete a utilizar el Servicio de conformidad con la ley, la moral, las buenas costumbres generalmente aceptadas y el orden público, así como a abstenerse de utilizar el Servicio y/o los demás servicios con fines o efectos ilícitos, prohibidos en las presentes Condiciones Generales, lesivos de los derechos e intereses de terceros, o que de cualquier forma puedan dañar, inutilizar, sobrecargar o deteriorar los servicios, los equipos informáticos de otros Clientes o de otros usuarios de Internet (hardware y software) así como los documentos, archivos y toda clase de contenidos almacenados en sus equipos informáticos (hacking), o impedir la normal utilización o disfrute de dichos Servicios, equipos informáticos y documentos, archivos y contenidos por parte de los demás Clientes y de otros usuarios de Internet.

Telefónica se reserva la facultad de adoptar las medidas que estime oportunas en caso de que existan indicios de un uso fraudulento del Servicio, incluyendo la adopción de las acciones legales oportunas. Asimismo, la utilización del Servicio podrá exclusivamente destinarse al ámbito profesional o privado. Queda expresamente prohibida la realización de

actos de reventa o comercialización del Servicio a terceros ajenos a la prestación del Servicio.

En caso de incumplimiento de la presente condición, Telefónica podrá suspender la prestación del Servicio, de conformidad a lo dispuesto de las presentes Condiciones Particulares. El Cliente será responsable frente a Telefónica del uso incorrecto de los servicios contratados. El Cliente responderá de los daños y perjuicios de toda naturaleza que Telefónica pueda sufrir como consecuencia del incumplimiento de cualquiera de las obligaciones a las que queda sometido por virtud de las presentes Condiciones Particulares o de la ley en relación con la utilización del Servicio.

4.5.1 Uso correcto del equipamiento incluido en las modalidades Paquete Avanzado y Paquete Premium

- El suministro del equipamiento hardware, para los casos de Paquete Avanzado y Premium, se realizará en la sede indicada por el cliente en el momento de la contratación
- La propiedad del dispositivo (o dispositivos) que se despliega en casa del Cliente en estos paquetes será en todo momento de Telefónica, siendo la responsabilidad del Cliente, el cuidado y la guarda del Hardware. El dispositivo se cede en régimen de alquiler y en caso de sufrir algún daño, pérdida o robo, el Cliente deberá restituirlo.
- Tendrá la obligación de comunicar de inmediato a Telefónica cualquier novedad dañosa, así como cualquier reclamación, acción, demanda o embargo que se produzca en relación con el equipamiento que tiene alquilado. Asimismo, deberá manifestar que el equipamiento no es de su propiedad sino que es alquilado a Telefónica frente a los terceros que pretendan embargarles o entablar cualquier acción, demanda o reclamación sobre su propiedad o posesión.

4.6 COMPROMISO DE PERMANENCIA

Los paquetes Avanzado y Premium tienen una permanencia de 12 meses desde el momento del alta efectiva de dicho paquete.

Si el cliente causara baja anticipada o una reducción en el número de usuarios antes de finalizar este periodo, se facturará el último mes en el que el Cliente esté dado de alta en el servicio, la cuota mensual correspondiente y prorrateada hasta el día de la baja efectiva y se emitirá una factura adicional con el resto del importe restante adeudado hasta cubrir el periodo de permanencia.

Para el cómputo de lo adeudado se utilizará como base la cuota del contrato inicial del paquete correspondiente.

5. CONDICIONES DE ACCESO Y BAJA DEL SERVICIO

5.1 Cliente titular y usuarios del Servicio

Para contratar el Servicio, el Cliente ha de ser un cliente Fusión Digital o Cliente de Servicio de Internet Banda Ancha en cualquiera de las modalidades de la oferta vigente en el momento de contratación del Servicio Fusión Digital o Servicio Internet Banda Ancha. Asimismo, se requiere que el Cliente disponga de los requisitos necesarios tal y como ya se ha indicado en la Cláusula 4.4 de estas Condiciones. Por lo que el titular del servicio Fusión

Digital o Servicio Internet banda Ancha será el único responsable de la gestión comercial del Servicio, es decir de la activación o baja del mismo.

Para su contratación, el Cliente ha de haber aceptado las presentes Condiciones del servicio Tu Empresa Segura.

El acceso al portal web del servicio TU EMPRESA SEGURA se realizará mediante unas credenciales que se proporcionarán exclusivamente al contacto técnico del Cliente. Será con estas credenciales de acceso con las que pueda establecer contacto con el equipo de soporte para solicitar modificaciones en las configuraciones de los servicios, notificar incidencias, tener información sobre los servicios contratados, ver informes y modificar su perfil de acceso.

Uso y custodia. El Cliente se compromete a hacer un uso diligente de las Claves de Acceso al portal web. En todo caso, el Cliente responderá de la mala utilización de las mismas por cualquier tercero que haya conseguido dichas claves por un error o negligencia imputable exclusivamente al Cliente.

5.2 Baja del Servicio

El presente contrato se resolverá por decisión del propio Cliente una vez comunicado a Telefónica Empresas por cualquier medio fehaciente.

En caso de baja anticipada por parte del Cliente del SERVICIO con un producto con compromiso de permanencia vigente, se incluirá en la última factura la mensualidad prorrateada según la fecha efectiva de baja y un importe adicional de acuerdo con las cuotas restantes adeudadas hasta cubrir el período total de permanencia.

La solicitud de baja por parte del Cliente del servicio (o de la sede) FUSIÓN DIGITAL o Servicio Internet Banda Ancha, al que esté asociada la contratación de este servicio, causará automáticamente la baja del servicio **TU EMPRESA SEGURA**, así como de los diferentes productos contratados y asociados al mismo, lo que no exime al cliente del pago de la permanencia, si la tuviera.

La solicitud de baja por parte del Cliente de este Servicio, no afectará a los restantes productos Fusión, que mantendrán sus vigencias y compromisos de permanencia.

Asimismo, el presente contrato se resolverá por cesación de Telefónica Empresas en la prestación del Servicio, previa comunicación a los Clientes con (1) mes de antelación sobre la fecha prevista para dicha cesación, lo que eximirá al Cliente del pago de las penalizaciones por permanencia si las tuviera.

En especial, Telefónica Empresas podrá resolver el presente contrato:

1. Por impago del servicio contratado.
2. Por incumplimiento del uso correcto del servicio de acuerdo con lo indicado en el presente documento.

3. Por impedir el Cliente o retrasar en más de 2 meses la instalación del equipo necesario para la prestación del Servicio TU EMPRESA SEGURA en las modalidades Avanzada y Premium.

4. Por detectarse un uso abusivo de la herramienta de Correo Limpio por parte del Cliente y no regularizar la situación tras pasar dos meses desde la notificación de Telefónica Empresas

Terminada la prestación del Servicio **TU EMPRESA SEGURA**, Telefónica EMPRESAS facturará, en su caso, el importe correspondiente a la parte proporcional de la última cuota mensual, en función de la fecha de efectividad de la baja y, en su caso, en factura adicional el importe por las cuotas restantes hasta la finalización del periodo de permanencia comprometido por el cliente.

El cambio de titular Fusión también implica la baja automática del servicio Tu Empresa Segura, pudiendo el nuevo titular solicitar la contratación mediante solicitud expresa.

5.3 Retirada y suspensión del servicio

Telefónica podrá retirar o suspender cautelarmente, la prestación de los servicios a aquellos Clientes que incumplan lo establecido en estas Condiciones, comunicándolo debidamente, con 1 mes de antelación.

6. OBLIGACIONES DE TELEFONICA EMPRESAS

6.1 Utilidad y fiabilidad de los servicios y contenidos accesibles a través del Servicio.

El servicio se soporta en proveedores reconocidos en protección frente a amenazas informáticas y ataques maliciosos, lo que acompaña de herramientas avanzadas y asistencia personalizada para afrontar determinados riesgos y amenazas, pero dada la naturaleza variable de dichos riesgos y amenazas no contiene garantía ni obligación de resultado.

Telefónica Empresas responderá única y exclusivamente del servicio que preste por sí misma. En cualquier caso, excluye toda responsabilidad con toda la extensión que permita el ordenamiento jurídico, por los daños y perjuicios de cualquier naturaleza, daño emergente y/o lucro cesante.

El software se proporciona "AS-IT IS" sin garantías de ningún tipo, excepto por cualquier garantía, término o condición que no pueda excluirse con arreglo a la ley aplicable y las mencionadas en este contrato y sujeto a los EULAS de fabricante que aplican.

En la medida máxima permitida por la ley aplicable, y por estas condiciones generales, Telefónica Empresas no otorga ninguna garantía, término o condición que el software estará libre de errores, interrupciones o fallos, o que es compatible con un hardware o software específico, excepto en la forma indicada expresamente

Privacidad y seguridad en la utilización de los servicios y contenidos.

Telefónica Empresa se compromete a adoptar e instalar las medidas y medios técnicos exigibles por la legislación sectorial vigente en función de las infraestructuras utilizadas para

garantizar el secreto de las comunicaciones en su tránsito a través de la red de Telefónica sin perjuicio de las interceptaciones legales que, en su caso, pudieran ordenarse. Telefónica Empresas queda exonerada de cualquier responsabilidad que pueda derivarse de la obtención por parte de terceros de Contenidos almacenados en el Servicio o del daño que terceros puedan provocar en los mismos.

Telefónica Empresas no garantiza la utilidad del Servicio para la realización de ninguna actividad en particular, ni su infalibilidad y en consecuencia no garantiza que la misma operará de manera permanente y libre de fallos, ni asumirá responsabilidad alguna por los daños sufridos por el Cliente por el no uso o imposibilidad de uso de la información o servicios prestados a través del Servicio. El Cliente asume toda la responsabilidad por la interpretación y el uso de la información contenida en esta aplicación.

Tampoco Telefónica Empresas será responsable del inadecuado funcionamiento del Servicio si ello obedece a labores de mantenimiento, a incidencias que afecten a operadores internacionales, a una defectuosa configuración de los equipos del Cliente o a su insuficiente capacidad para soportar los sistemas informáticos indispensables para poder hacer uso del Servicio. Telefónica Empresas, para mantener la calidad del servicio para todos sus Clientes, podrá establecer limitaciones de uso del servicio, incluyendo el número máximo de accesos a una funcionalidad o al Servicio o duración de dichos accesos. En particular:

1. Telefónica Empresas se reserva el derecho de limitar o detener el Servicio a cualquier usuario por el uso peligroso o ilegal del Servicio.

2. Telefónica Empresas se reserva el derecho de limitar o detener el Servicio a cualquier usuario ante la imposición de una carga excesiva en el sistema de Telefónica de manera que ponga en peligro el rendimiento del sistema para el resto de los usuarios.

6.2 PROPIEDAD INDUSTRIAL E INTELECTUAL

El Cliente acepta que todos los elementos integrados dentro del Servicio están protegidos por la legislación sobre derechos de propiedad intelectual e industrial y que los derechos sobre los mismos corresponden a Telefónica Empresas o, en su caso, a terceros.

Telefónica Empresas conservará la plena titularidad de los derechos de propiedad intelectual e industrial que le pertenecieran al tiempo de celebrar el contrato y le corresponderán, igualmente, los derechos de propiedad Intelectual e industrial relativos a cualquier software, tecnología y documentación, creados, desarrollados, modificados, mejorados o transformados como consecuencia de la prestación del Servicio. En consecuencia, el Cliente y los Usuarios se comprometen a respetar los términos y condiciones establecidos por las presentes Condiciones, siendo el Cliente el único responsable de su incumplimiento frente a Terceros.

Sin perjuicio de lo anterior, en el caso de que como consecuencia de la ejecución y cumplimiento del contrato el Cliente tuviese necesidad de utilizar metodología y herramientas software titularidad de Telefónica Empresas conforme a lo arriba

indicado, el Cliente no adquirirá más derechos sobre los mismos que el uso que se requiera durante la ejecución del proyecto o el tiempo previsto expresamente, se abstendrá de hacer copias y/o introducir variantes en los mismos y no permitirá a terceros el acceso y uso de dichos programas y metodologías, salvo en el caso de que sea autorizada de forma expresa y con carácter previo por Telefónica Empresas.

7. PROTECCION DE DATOS DE CARÁCTER PERSONAL.

Telefónica informa al Cliente de que tratará los datos personales que sean estrictamente necesarios para la prestación del Servicio contratado, el mantenimiento y gestión de la relación contractual, así como labores de información de los distintos servicios contratados y de las actividades relacionadas con los mismos.

Los datos de contacto de los interlocutores proporcionados por el Cliente para mantener la relación contractual con Telefónica (en adelante, "los interlocutores"), así como para otras finalidades que permita o autorice, serán tratados conforme a lo establecido en la Política de Privacidad de Telefónica, cuya información básica se recoge en la presente cláusula. El contenido íntegro de la misma se puede consultar en el siguiente enlace: www.movistar.es/privacidad, solicitando un ejemplar en el 1489 o en las Tiendas Movistar.

De acuerdo con la normativa europea de protección de datos de carácter personal y en virtud de lo establecido en dicha Política, las siguientes empresas del Grupo Telefónica son corresponsables del tratamiento de los datos personales del Cliente en función de los productos y servicios que tenga contratados: Telefónica de España, S.A.U., Telefónica **Móviles España, S.A.U. y Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U.**

Adicionalmente, Telefónica podrá tratar los datos del Cliente o de los interlocutores relativos a los servicios contratados, datos de tráfico y de facturación, así como los relativos a la adquisición de productos y servicios por el Cliente, con la finalidad de realizarles ofertas comerciales sobre productos y servicios Movistar.

Si el Cliente no desea que Telefónica utilice la información indicada con la citada finalidad, podrá comunicarlo enviando un email a privacidad.telefonicaempresas@telefonica.com; o un escrito dirigido a Telefónica, Ref. "Datos" al Apartado de Correos 46155, 28080, Madrid, y en todo caso, los interlocutores tendrán la facultad de oponerse a la recepción de comunicaciones comerciales a través de los mismos medios indicados anteriormente. Es responsabilidad del Cliente facilitar esta información a los interlocutores cuyos datos se estén tratando por Telefónica en este contexto, e indicarles que podrán consultar el detalle en la web www.movistar.es/privacidad.

Para cualquiera de las finalidades previstas en la Política de Privacidad, Telefónica podrá encargar su tratamiento a proveedores de confianza. La relación actualizada de las categorías de dichos proveedores, así como de aquellos que realizan transferencias internacionales de datos en el ejercicio de sus funciones se recoge en www.movistar.es/privacidad/info-adicional.

Tanto el Cliente como los interlocutores, podrán siempre consultar el detalle de la Política de Privacidad en www.movistar.es/privacidad o solicitando un ejemplar en el 1489 o en las Tiendas Movistar, así como ejercer sus derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad enviando un email a la dirección privacidad.telefonicaempresas@telefonica.com, o dirigiendo un escrito al Apartado de Correos 46155, 28080, Madrid.

Puesto que la prestación del servicio regulado en las presentes condiciones da lugar a operaciones o actuaciones que, según la normativa aplicable en materia de protección de datos, se consideran un encargo de tratamiento de datos de carácter personal, las Partes acuerdan que resultará de aplicación el Anexo III (Convenio de tratamiento de datos

personales) a las presentes Condiciones, que regulará el citado encargo del tratamiento de conformidad con el artículo 28 del RGPD**.**

8. RESPONSABILIDAD.

Telefónica responderá de los daños y perjuicios ocasionados directamente al cliente, por causa exclusivamente imputable a Telefónica en relación con el presente contrato y la prestación de los servicios objeto del mismo. El resarcimiento de daños y perjuicios:

- No cubrirá daños indirectos o lucro cesante, pérdida de datos, pérdida de beneficios o de negocio del cliente.

- Alcanzará hasta una suma máxima equivalente al precio a pagar por el cliente por el servicio o servicios afectados por el plazo de un (1) mes en relación con los servicios objeto de reclamación. Para ello se calculará la media mensual correspondiente a la anualidad anterior o, en caso de no haber transcurrido un año desde el inicio en la prestación del servicio, a los meses transcurridos.

- No procederá en caso de que el daño o perjuicio haya sido resarcido por Telefónica por medio de cualquier tipo de penalizaciones o compensaciones**.**

9. CAMBIOS PERMITIDOS DURANTE LA VIGENCIA DEL CONTRATO

La contratación de la modalidad paquete Lite no admite el cambio hacia las otras modalidades de paquete durante la vigencia del contrato. Sólo admite aumentar o reducir el número de unidades contratadas de dicho paquete

En el resto de los casos, el cliente puede cambiar el paquete del servicio contratado a una modalidad superior en cualquier momento, pero deberá tener en cuenta que:

- Un cambio de Modalidad Paquete Básico a Modalidad Paquete Avanzado o Premium, iniciará un compromiso de permanencia de 12 meses a partir de que se le notifica el alta efectiva de los nuevos productos que incluye.
- Un cambio de Modalidad Paquete Premium a Modalidad Paquete Avanzado, no interrumpe ni reinicia la permanencia.
- No está permitido un cambio de Modalidad Paquete Premium o Avanzado a Modalidad Paquete Básico durante el periodo de permanencia.
  En caso de realizarse este cambio, generará al Cliente la obligación de pago de la penalización correspondiente.

Para todas las modalidades de paquete:

- El cliente puede incrementar en cualquier momento el número de usuarios contratados en el paquete, pero deberá tener en cuenta las limitaciones que se indican en el Anexo VI Modalidad Paquete Avanzado o en el Anexo VII Modalidad Paquete Premium, según corresponda

- El cliente puede reducir el número de usuarios contratados en el paquete también está permitido con las siguientes limitaciones:
  - En la Modalidad Paquete Lite y paquete Básico está permitido en cualquier momento
  - En la Modalidad Paquete Avanzado y Paquete Premium, sólo se puede reducir el número de usuarios **una vez terminado el periodo de permanencia**.

La reducción en el número de usuarios en una Modalidad Avanzado o Premium durante el periodo de permanencia generará al Cliente la obligación de pago de la penalización correspondiente.

Los módulos adicionales pueden contratarse en cualquier momento mientras el cliente tenga vigente el servicio con un paquete en modalidad Básica, Avanzada o Premium (no está permitido con el paquete Lite)

En función del tipo de módulo están permitidas las siguientes acciones:

- **Puesta en Marcha** y **Visita**: Alta de nuevas unidades a consumir al provisionarse. No está permitida la baja al ser unidades con facturación única.
- **Firma Digital** y **Buzón Adicional de Correo Limpio**: Alta de nuevas unidades en el servicio, reducción del número de unidades o baja total del módulo en cualquier momento de la vigencia del contrato.
- **Protección de la Identidad**: Alta del módulo al servicio o baja total del módulo. No se contrata por unidades sino por empresa (CIF) y en una única sede.

10. NOTIFICACIONES

Las comunicaciones del Cliente a Telefónica Empresas deberán dirigirse al Servicio de Atención al Cliente utilizando los números de atención comercial.

Las notificaciones que EL Cliente haya de efectuar a Telefónica Empresas con motivo de lo previsto en el presente Contrato y en ejecución del mismo, se efectuarán, bien telefónicamente a los números de atención personal de Telefónica Empresas, bien por escrito a los apartados de correo o direcciones postales previstas, en cada caso, a lo largo de este contrato.

Las notificaciones y comunicaciones por parte de Telefónica Empresas al Cliente se realizarán de alguna de las siguientes formas:

(a) envío por correo postal al domicilio designado por EL Cliente a tal efecto en el momento de la contratación. En defecto de designación o comunicación de la modificación del domicilio inicialmente designado, se entenderá, a todos los efectos, que el domicilio del Cliente es el lugar en donde se realiza la prestación del servicio, y en caso de ser estos varios, cualquiera de ellos;

(b) envío por correo electrónico, siempre que ello sea posible, a cualquiera de las direcciones de correo electrónico que el Cliente facilite a Telefónica Empresas a dichos efectos;

(c) comunicación por medio de una llamada telefónica o SMS si procede, bien al número de teléfono a través del cual se presta el SERVICIO al Cliente, o bien al número de teléfono indicado por el Cliente en el Formulario de Solicitud de Alta en el SERVICIO, o modificado posteriormente por el Cliente conforme a esta Condición.

d) comunicación por medio del área privada “Tu Empresa Segura” del cliente, a la que podrá acceder a través de la web https://tuempresasegura.movistar.es/

En este sentido, El Cliente manifiesta que todos los datos facilitados por él son ciertos y correctos, y se compromete a comunicar a Telefónica Empresas las variaciones que, en su caso, se produzcan en su domicilio o en cualquier otra dirección o medio de contacto, en los datos de cobro, así como en cualquier otro tipo de información necesaria para la gestión y mantenimiento de la relación contractual entre Telefónica Empresas y EL Cliente.

11. MODIFICACIÓN DE LAS CONDICIONES DEL SERVICIO

El Cliente se compromete a comunicar a Telefónica Empresas cualquier cambio en los datos del contrato, especialmente en los correspondientes al domicilio de facturación y de la cuenta bancaria de domiciliación de los pagos.

Telefónica Empresas, con el único fin de restablecer el equilibrio de las prestaciones entre las Partes, podrá modificar las condiciones establecidas en el contrato y en particular el precio del mismo, por alguno de los siguientes motivos cuando los mismos obedezcan a situaciones acaecidas en un momento posterior a la fijación de las tarifas del Servicio por parte de Telefónica Empresas:

- Incremento de los costes del sector empresarial en el que esté presente Telefónica Empresas y que redunden en la cobertura, en la calidad de la red o en las características del Servicio prestado.

- Modificaciones normativas (incluyendo impuestos, tasas o resoluciones administrativas o judiciales) que afecten a las condiciones de prestación del Servicio.

- Incremento del índice de precios al consumo (IPC) o en su defecto del índice de precios Industriales (IPRI).

Telefónica Empresas informará al cliente de cualquier modificación con indicación del motivo preciso a la que obedece con una antelación mínima de UN (1) mes a la fecha en que la modificación vaya a ser efectiva, teniendo el cliente derecho a resolver el contrato sin penalización alguna, sin perjuicio de otros compromisos adquiridos por el propio cliente. Transcurrido el plazo de un mes sin que Telefónica Empresas haya recibido ninguna comunicación, se entenderá que el Cliente acepta las modificaciones.

12. CESIÓN DEL CONTRATO:

El servicio objeto de este contrato tiene carácter personal, si bien el cliente podrá cederlo a un tercero previo consentimiento de Telefónica DE ESPAÑA, S.A.U. Telefónica DE ESPAÑA, S.A.U podrá ceder este contrato informando previamente al cliente conforme a la normativa vigente, y sin perjuicio del derecho que el cliente pudiera tener a resolver el contrato.

13. LEY APLICABLE Y RESOLUCION DE CONFLICTOS

En caso de que el Cliente tenga alguna incidencia o duda en relación con el Servicio podrá ponerse en contacto con Telefónica Empresas para la resolución de la misma llamando 1489.

Será de aplicación a las presentes Condiciones la legislación española. En caso de controversia acerca de la interpretación o ejecución de las mismas el usuario podrá dirigirse, para la resolución de los conflictos derivados o relacionados con el servicio a los Juzgados y Tribunales que resulten competentes en cada momento, conforme a lo dispuesto en la legislación vigente.

Anexos Condiciones Particulares Tu Empresa Segura.

Anexo I Precios Vigentes

Anexo II Modelo de Atención

Anexo III Convenio de Tratamiento de Datos Personales

Anexo IV Modalidad Paquete Lite

Anexo V Modalidad Paquete Básico

Anexo VI Modalidad Paquete Avanzado

Anexo VII Modalidad Paquete Premium

Anexo VIII Módulos Adicionales

Anexo IX Glosario

ANEXO I: PRECIOS VIGENTES

1. Precios Vigentes de los Paquetes del servicio TU EMPRESA SEGURA

Se facturará al Cliente una cuota mensual por sede, a mes vencido, que dependerá del paquete contratado para dicha sede (modalidad, número de usuarios y opcionales y/o módulos adicionales)
Se muestran a continuación los precios (antes de impuestos) de cada concepto.

Precios Paquetes					
Tipo	**Concepto**	**Lite**	**Básico**	**Avanzado**	**Premium**
Obligatorio	Por Usuario	5 €/mes	4,99 €/mes	6,99 €/mes	9,99 €/mes
	Por Sede		0 €/mes	135 €/mes	180 €/mes

En cualquiera de las 3 modalidades de paquete Básico, Avanzado o Premium, se aplica un descuento en la cuota mensual correspondiente con el concepto Usuarios de la sede de acuerdo con la tabla siguiente:

Descuento por volumen en el Paquete Básico, Avanzado o Premium		
Concepto	**Rango**	**Descuento en la cuota Usuarios**
N.º usuarios	0-29	Sin descuento
N.º Usuarios	30-149	5%
N.º Usuarios	150-200	10%

Estos descuentos se aplican en la contratación individual de cada paquete y en ningún caso se aplican agregando usuarios de varios paquetes.

1.1 Opcionales del paquete Avanzado y Premium

Adicionalmente, se ofrecerán dos opciones asociadas a la Modalidad Avanzada: **HA (Alta Disponibilidad) y upgrade (Modelo superior de Firewall)** que deberán solicitarse siempre en el momento de la contratación, sin posibilidad de poder hacerlo en fase de postventa del servicio.

En caso de que se requiera la **capacidad de HA** (Alta Disponibilidad), este coste adicional al de la tabla anterior, se calculará en función del número de usuarios que se tenga contratado en una determinada sede.

Precios HA				
Usuarios/sede	**1-50**	**51-100**	**101-150**	**151-200**
Opcional	119 €/mes	149 €/mes	239 €/mes	577,57 €/mes

En caso de que se requiera la **capacidad de UPGRADE** (Modelo superior de Firewall), se añadirá, a continuación, el siguiente coste mensual.

Precios Upgrade				
Usuarios sede	**1-50**	**51-100**	**101-150**	**151-200**
Opcional	43 €/mes	109 €/mes	371,92 €/mes	No Aplica

Para un paquete vendido en HA (Alta Disponibilidad), al contar con dos equipos, el coste se calculará, multiplicando por dos el precio del upgrade.

1.2 Precios vigentes de los módulos de contratación adicional

Módulos Opcionales	Concepto	Precio por unidad
Puesta en marcha	Hasta 5 aplicaciones y puesta en marcha del Correo Limpio	40,5 €
Visita	1 visita a domicilio	250 €
Firma Digital	Paquete de 250 firmas al año	9,99 €/mes
Buzón Adicional de Correo Limpio	Por buzón adicional	2,15 €/mes
Protección de la Identidad	1 unidad (para toda la empresa (CIF))	15 €/mes

1.3 Desplazamiento del Técnico a instalaciones del Cliente

En caso de que se produzca un desplazamiento a casa del Cliente después de concertar una cita para llevarle el equipamiento UTM o para resolver alguna incidencia relacionada con sustitución de piezas por mantenimiento y no pudiera llevarse a cabo esta tarea por aspectos exclusivamente imputable al Cliente, Telefónica facturará esta visita.

Precio visita a casa de Cliente **250€**

ANEXO II: MODELO DE ATENCIÓN

1. MODELO DE ATENCIÓN DEL SERVICIO TU EMPRESA SEGURA PARA LAS MODALIDADES PAQUETE BÁSICO, AVANZADO Y PREMIUM

Una vez el Cliente ha contratado el servicio en modalidad gestionada (paquete Básico, Avanzado y Premium), Telefónica pone a disposición del cliente un portal de servicio con varios canales de comunicación con el SOC Pyme así como una dirección de correo electrónico al que poder dirigirse y los teléfonos habituales de contacto:

- Portal del servicio en https://tuempresasegura.movistar.es
- e.soportetuempresasegura.tcct@telefonica.com
- 1489/1002
- También está habilitado el acceso a través del portal ***Mi Gestión Digital*** de Telefónica Empresas: https://paut.telefonica.es/login
- A través del teléfono que le comunicarán en el correo de bienvenida una vez dado de alta en el servicio

Por defecto sólo se habilita un único contacto técnico **como usuario autorizado por sede** para la apertura de peticiones, incidencias y consultas al SOC Pyme. En caso de ser necesario que se habilite un segundo usuario, el cliente tendrá que solicitarlo abriendo un ticket.

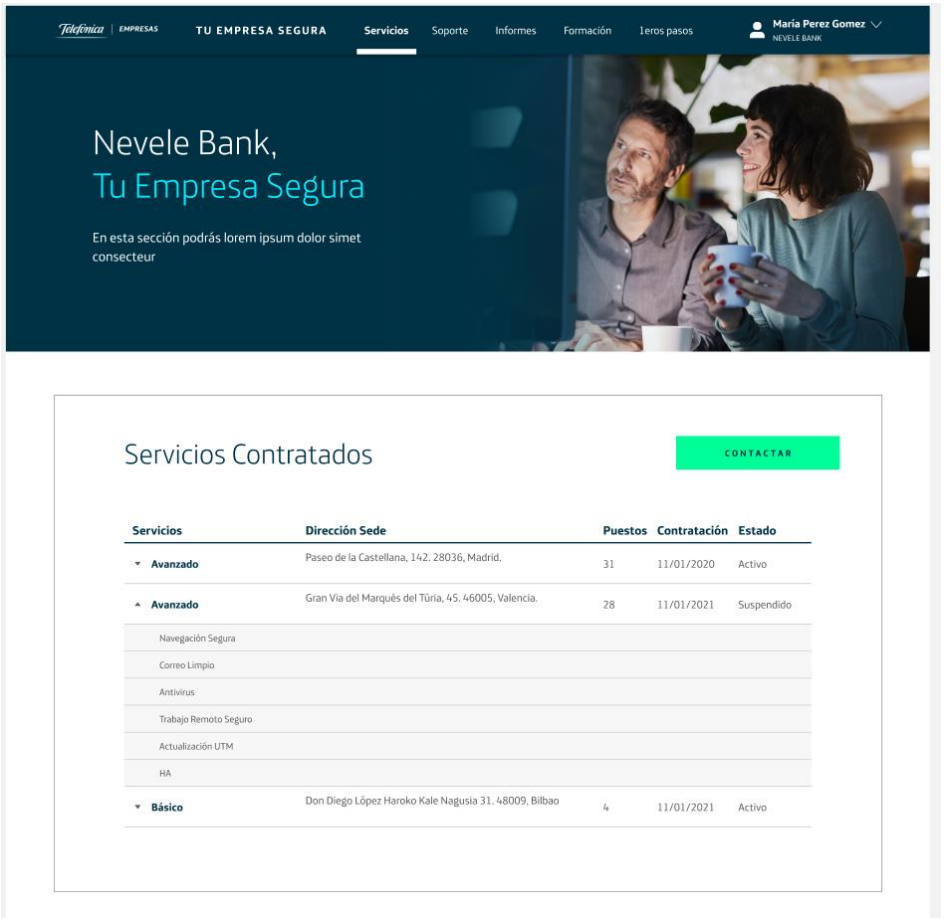
Nota: Para el caso de modalidad paquete Lite no será de aplicación nada de lo descrito en este apartado ya que el servicio es autogestionado por el propio cliente.

Sólo se atenderán incidencias relacionadas con temas administrativos (incidencias relacionadas con el suministro de la licencia, facturación, etc), por los siguientes canales:

- Vía telefónica al 1489/1002

1.1 Portal del Servicio

El Cliente recibirá un email de bienvenida en el que se le indicará que para dar los primeros pasos deberá acceder al portal de gestión de TU EMPRESA SEGURA. El email se enviará al correo indicado como contacto técnico. La primera vez que acceda al portal deberá crear una nueva contraseña. A partir de ese momento, ya podrá acceder con sus credenciales: el usuario será el mail de contacto y la contraseña la que el Cliente configure.



El área de clientes del portal TU EMPRESA SEGURA incluye las siguientes funcionalidades:

- Información sobre el servicio contratado (modalidad, número de usuarios y sedes).
- Guía de configuración paso a paso y manual del servicio.
- Canal de comunicación con el SOC Pyme para la apertura y seguimiento del estado de tickets (incidencias, peticiones y consultas)
- Chat para la comunicación con un agente para consultas y peticiones

1.2 Horario de Atención de incidencias y peticiones

Definiciones previas

Las diferentes acciones que puede ejecutar el Cliente como parte de los servicios de se establecen como Peticiones, Consultas e Incidencias (PCI). Englobaremos las consultas como peticiones al no tener el carácter consultivo. Adicionalmente existen actividades que por su propia naturaleza son iniciadas por el SOC Pyme. Se definen como sigue:

- Incidencia: Fallo, degradación o comportamiento no esperado del servicio comunicada por el Cliente o detectada por Telefónica.
- Peticiones: Solicitud de ejecución de actividad de entrega del servicio o consulta de parámetros propios del mismo que se extraen de las herramientas.
- Consulta: Solicitud de información sobre el estado o configuración de los servicios, bien de forma genérica o en concreto para algún dispositivo sobre el que se esté prestando el servicio.
- Actividad del servicio: Actividad de entrega del servicio iniciada por el SOC Pyme.

Horario de atención

Servicio	Horario Incidencias	Horario Solicitudes (Peticiones y Consultas)
Operación SOC Pyme	24x7	8x5

El horario de atención en 8x5 será de 8:00 a 17:00 de lunes a viernes, laborables de acuerdo con el calendario laboral de Madrid.

Tiempo objetivo de respuesta

Período de tiempo que trascurre desde que un usuario envió la petición o incidencia hasta que recibe una respuesta por parte de Telefónica una vez realizado el triaje inicial.

El SOC pyme trabaja con un tiempo objetivo de respuesta de:

- 60 minutos si la incidencia/petición se abre en el portal web o por correo electrónico
- 90 minutos si la incidencia/petición se hace por vía telefónica (1002/1489)

Tiempo objetivo de resolución de peticiones

Este indicador mide el tiempo de resolución de Peticiones en 8x5

Niveles de Severidad	Tiempo Objetivo	Horario
URGENTE	12 horas	Peticiones y consultas en 8x5
NORMAL	24 horas	Peticiones y consultas en 8x5

Tiempo objetivo de resolución de incidencias

La severidad de cada una de las PCI abiertas por el Cliente o por el propio SOC Pyme tendrán, como norma general, una severidad según el nivel de afectación al servicio prestado por el SOC Pyme, tal y como se muestra en la siguiente tabla:

NIVELES DE SEVERIDAD	DEFINICIÓN
CRÍTICO	Aquellas incidencias en las que la hay corte de servicio.
ALTO	Aquellas incidencias en las que la hay degradación de servicio.
MEDIO-BAJO	Incidencias con impacto en el servicio.

Este indicador mide el tiempo objetivo de resolución de incidencias en horario 24x7

Niveles de Severidad	Tiempo Objetivo	Horario
CRÍTICO	<8 horas*	Incidencias en 24x7
ALTO	<24 horas *	Incidencias en 24x7
MEDIO-BAJO	<72 horas*	Incidencias en 24x7

***Estos tiempos se verán incrementados en caso de que la incidencia conlleve algún tipo de desarrollo por parte del fabricante (para resolución, por ejemplo, de un bug de producto) o en el caso de que implique sustitución o reparación del Hardware UTM, en donde se añadirá el tiempo de los RMAs establecidos por el fabricante.**

Los valores objetivo de los niveles de Severidad Crítica y Alta hacen referencia al tiempo de resolución de la incidencia relacionada con la falta de disponibilidad o la degradación de la plataforma. Posteriormente, se realizará un diagnóstico del origen que ha provocado la incidencia, no computando el tiempo de duración de dicho diagnóstico en la medición del tiempo objetivo.

El tiempo objetivo considera únicamente el tiempo en que la tarea ha estado bajo la responsabilidad del personal de Telefónica. Por tanto, se excluyen los periodos de tiempo en los que haya estado a la espera de datos, instrucciones o actuaciones solicitadas al Cliente.

Los tiempos objetivo de respuesta y resolución del servicio se comunica a los Clientes a título informativo pero el incumplimiento de este no conlleva penalizaciones

Exclusiones

A la hora de calcular mensualmente los tiempos objetivo se tendrán en cuenta las siguientes exclusiones:

- No se tendrán en cuenta los problemas derivados de elementos que no están incluidos en el servicio.
- No se tendrán en cuenta en el cálculo los tiempos que coincidan con los periodos de inactividad planificados, que son ventanas programadas para la realización de actividades que tendrán como objetivo el mantenimiento de la disponibilidad acordada. Los tiempos de inactividad planificados estarán predefinidos y serán avisados con al menos 48 horas y se efectuarán en el horario que menor impacto tenga para el Cliente.

- No se tendrán en cuenta en el cómputo los correspondientes a las siguientes tareas consideradas como tiempos excusables:
    - Periodos de desconexión no programados y solicitados por el Cliente, generalmente asociados a emergencias.
    - Ataques a los servicios con entradas no autorizadas, desastres naturales, cambios debidos a acciones gubernamentales, políticas u otras acciones reglamentarias, órdenes judiciales, huelgas o disputas laborales, actos de desobediencia civil, actos de guerra, actos contra las partes (incluyendo los operadores y demás proveedores Telefónica Empresas), y otros elementos de fuerza mayor.
      Instalación de parches

1.3 Aspectos excluidos y restricciones

Solo se dará soporte a la persona identificada como Contacto Técnico del Cliente los especificado en el momento de contratación del paquete asociado a una sede. No se dará soporte a los usuarios finales del Cliente.

ANEXO III: CONVENIO DE TRATAMIENTO DE DATOS PERSONALES

Por un lado, el Cliente que haya contratado el servicio de **TU EMPRESA SEGURA** (en adelante, "**Responsable del Tratamiento**" o "**Cliente**");

Por otro lado, TELEFÓNICA DE ESPAÑA, S.A.U., con domicilio social en calle Gran Vía 28, 28013, Madrid (en adelante, el "**Encargado del Tratamiento**" o "**Prestador del Servicio**"),

denominadas conjuntamente las "**Partes**" e individualmente la "**Parte**".

Si, como consecuencia de la ejecución de las presentes Condiciones, el Prestador del Servicio realizara algún tipo de tratamiento de los datos de carácter personal por cuenta del Cliente, el Prestador del Servicio sería considerado "Encargado del Tratamiento", de conformidad con lo previsto en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "**RGPD**").

En ese caso, el Encargado del Tratamiento se compromete a respetar las disposiciones del presente acuerdo (en adelante, el "**Acuerdo**"):

a) Compromisos del Prestador de Servicios como Encargado del Tratamiento.

El Encargado del Tratamiento cumplirá en todo momento, con todas las obligaciones que resulten exigibles al tratamiento conforme a lo previsto en el Reglamento General de Protección de Datos, la Ley Orgánica de Protección de Datos, y cualquier otra normativa (nacional o supranacional) aplicable, así como y con las instrucciones razonables y documentadas del Responsable del Tratamiento que, en su caso, puedan ser consideradas parte de estas Condiciones, prestando en todo momento las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para este fin.

En particular, el Encargado del Tratamiento se obliga a:

i. Tratar los datos personales estrictamente necesarios para la ejecución de las presentes Condiciones, no pudiendo ser comunicados o entregados a terceras personas en ningún caso, salvo que cuente con la autorización previa, expresa y por escrito del Responsable del Tratamiento para aquellos supuestos legalmente admisibles o salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al Encargado del Tratamiento. En ningún caso el Encargado del Tratamiento utilizará dichos datos personales (incluyendo copias de seguridad) para fines propios;

ii. Llevar un registro documentado de todas las categorías de actividades de tratamiento efectuadas por cuenta del Responsable del Tratamiento en el marco de estas Condiciones, que contenga:

a. el nombre y los datos de contacto del Encargado o Encargados del Tratamiento, y de cada Responsable del Tratamiento por cuenta del cual actúe el Encargado del Tratamiento así como, en su caso, del representante del Responsable del Tratamiento o del Encargado de Tratamiento y en su caso del delegado de protección de datos;

b. Las categorías de tratamientos efectuados por cuenta del Responsable del Tratamiento;

c. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de ese tercer país u organización internacional y de ser necesario por la Normativa de Protección de Datos Aplicable, la documentación de garantías adecuadas;

d. Una descripción general de las medidas técnicas y organizativas de seguridad;

iii. Trasladar al Responsable del Tratamiento las medidas técnicas y organizativas de que disponen los servicios contratados por el primero, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. El Cliente será el único responsable de que estas medidas resulten apropiadas en cada caso para garantizar un nivel de seguridad adecuado al riesgo de conformidad con el artículo 32 del RGPD. Previa solicitud por escrito por parte del Responsable del Tratamiento, el Encargado del Tratamiento pondrá a disposición del Responsable del Tratamiento una lista actualizada de las medidas de seguridad adoptadas en los concretos servicios prestados al Responsable del Tratamiento. Sin perjuicio de lo anterior, el Encargado del Tratamiento aplicará las medidas de seguridad contenidas en el **Apéndice A**.

iv. Asistir al Responsable del Tratamiento, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados, esto es, los derechos de transparencia, información, acceso, rectificación y supresión (derecho al olvido), limitación del tratamiento, portabilidad, oposición o a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles), entre otros que se especifican en el Capítulo III del RGPD. En todo caso, esta obligación de asistencia se encuentra condicionada a las concretas prestaciones incluidas en las condiciones de cada servicio contratado, siempre que sean posteriores a la aplicación del RGPD.

v. Corresponde al Responsable del Tratamiento facilitar el derecho de información en el momento de la recogida de los datos, salvo que se especifique expresamente lo contrario en las condiciones del servicio contratado, siempre que sean posteriores a la aplicación del RGPD.

vi. Asistir al Responsable del Tratamiento en relación con la realización de las evaluaciones de impacto relativas a la protección de datos en los términos del artículo 35 del RGPD.

vii. Asistir al Responsable del Tratamiento en la realización de las consultas previas a la autoridad de control competente, cuando procede, en los términos del artículo 36 del

RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del Encargado del Tratamiento.

viii. Asistir al Responsable del Tratamiento en relación con las notificaciones y comunicaciones de una violación de la seguridad de los datos personales a las autoridades de control e interesados, en los términos recogidos en el presente Anexo.

ix. Suprimir todos los datos personales una vez finalice la prestación de los servicios objeto de las presentes Condiciones, salvo petición expresa en sentido contrario por parte del Responsable del Tratamiento, así como las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros que se aplique al Encargado del Tratamiento.
En todo caso, la medida que se adopte se encontrará condicionada a las concretas prestaciones incluidas en las condiciones de cada servicio contratado, siempre que sean posteriores a la aplicación del RGPD.

x. Garantizar la formación y sensibilización necesaria en materia de protección de datos personales de las personas autorizadas para tratar los Datos Personales que estén a cargo del Encargado del Tratamiento. En particular, garantizará que su personal tenga conocimiento de las medidas de seguridad utilizadas por el Encargado del Tratamiento y cómo aplicarlas y la forma de responder a incidentes relacionados con las violaciones de seguridad.

xi. Designar por escrito a un Representante en la Unión Europea cuando el Encargado del Tratamiento no esté establecido en la Unión.

xii. Designar, cuando proceda, a un delegado de protección de datos.

En el supuesto de que las obligaciones de asistencia contenidas en los apartados anteriores precisen la realización de auditorías externas o internas, o exijan una dedicación de recursos superior a la utilizada en el cumplimiento de las presentes Condiciones, el Encargado del Tratamiento se reserva el derecho a trasladar al Responsable del Tratamiento los sobrecostes razonables y motivados que dicho incremento de recursos le suponga.

b) Subcontratación.

El Responsable del Tratamiento autoriza la subcontratación por parte del Encargado del Tratamiento de aquellos subcontratistas que considere necesarios para la correcta prestación de los servicios objeto de las presentes Condiciones. Previa solicitud por parte del Responsable del Tratamiento, el Encargado del Tratamiento le facilitará una lista actualizada de todas las categorías de subcontratistas que participen en la prestación de los servicios contratados por el primero.

El subcontratista también tendrá la consideración de encargado del tratamiento en los mismos términos que el Encargado del Tratamiento en estas Condiciones. En este sentido, el Encargado del Tratamiento se obliga a suscribir con el tercero subcontratado un acuerdo de encargo de tratamiento de datos mediante el cual el subcontratista se obligue a cumplir con las obligaciones de estas Condiciones, en tanto que encargado del tratamiento.

En todo caso, se impondrán al subencargado las mismas obligaciones de protección de datos, de manera que el tratamiento sea conforme con las disposiciones del RGPD.

c) Transferencias Internacionales.

El Encargado del Tratamiento podrá almacenar los Datos Personales en servidores ubicados fuera del Espacio Económico Europeo o realizar acciones relacionadas con el tratamiento que impliquen una transferencia internacional de datos siempre y cuando haya obtenido las autorizaciones requeridas o medidas legalmente exigibles que legitiman dichas transferencias.

El Encargado del Tratamiento deberá asegurar un nivel adecuado de protección y garantizará un cumplimiento de la normativa europea y la legislación española vigente en cada momento. En este sentido, el Encargado del Tratamiento debe aportar garantías suficientes, y a condición de que los derechos de los interesados exigibles y acciones legales efectivas para los interesados estén disponibles.

d) Violación de la seguridad de los datos personales.

En caso de que el Encargado del Tratamiento tenga conocimiento de una violación de seguridad de los datos personales, entendida ésta según el RGDP como toda violación de la seguridad que ocasionare la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, que afecte a los datos personales responsabilidad del Responsable, originada en los sistemas de los que el Encargado del Tratamiento sea responsable de su gestión, mantenimiento o administración, el Encargado del Tratamiento deberá notificar al Responsable del Tratamiento sobre dicha violación de seguridad en los términos previstos en la normativa vigente.

Desde que tenga conocimiento de la violación de seguridad de los datos personales, el Encargado del Tratamiento adoptará las medidas necesarias para poner remedio a la misma, incluyendo, si procede, medidas para mitigar los posibles efectos negativos.

Sin perjuicio de lo anterior, el Encargado del Tratamiento ejecutará con la máxima celeridad las instrucciones que el Responsable pudiera encomendarle.

La notificación a que se refiere el primer apartado deberá: a) incluir el nombre del Encargado del Tratamiento, datos de contacto del punto de contacto único designado por el Encargado del Tratamiento para la violación de la seguridad de los dato personales; b) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; c) describir las posibles consecuencias de la violación de seguridad de los datos personales; d) describir las medidas adoptadas para poner remedio a la violación, incluyendo, si procede, las medidas para mitigar los posibles efectos negativos, así como, cualquier ticket de incidencia o número de seguimiento asignado a la violación de la seguridad de los datos personales.

En todo caso, el Encargado del Tratamiento implementará y mantendrá un proceso documentado de gestión de incidentes de seguridad que, al menos, incluya la siguiente información con respecto a una posible violación de la seguridad de los datos personales: identificación, fecha de detección, categorización, priorización, escalado, investigación y diagnóstico, resolución y recuperación, y cierre.

e) Confidencialidad.

El Encargado del Tratamiento se compromete a cumplir con la obligación de guardar la debida confidencialidad y secreto sobre los hechos, datos personales, informaciones, conocimientos, documentos, y otros elementos a los que tengan acceso con motivo de la prestación del servicio convenido sin que pueda conservarse copia o utilizarlos para cualquier finalidad distinta a las expresamente recogidas en estas Condiciones.

Asimismo, el Encargado del Tratamiento se compromete a que la información confidencial únicamente esté disponible para aquellas personas físicas o jurídicas que necesiten la información para el desarrollo de tareas para las que el uso de esta información sea estrictamente necesario. A este respecto, el Encargado del Tratamiento advertirá a dichas personas físicas o jurídicas de sus obligaciones respecto a la confidencialidad, velando por el cumplimiento de las mismas y garantizará que las personas autorizadas por el Encargado del Tratamiento dentro de su organización para tratar Datos Personales, se hayan comprometido a respetar la confidencialidad en términos equivalentes a los establecidos en estas Condiciones;

Estas obligaciones de confidencialidad subsistirán aún después de la finalización de estas Condiciones.

f) Auditoría.

El Encargado del Tratamiento se obliga a poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable y por entera cuenta y cargo del Responsable del Tratamiento. El Responsable del Tratamiento será el encargado de contratar a tal efecto a una entidad independiente (que no sea competencia del Encargado y que esté correctamente cualificado), que deberá guardar estricto secreto profesional.

El responsable del Tratamiento podrá hacer una solicitud de auditoría al año, y deberá solicitar la realización de la auditoría o inspección, con una antelación mínima de treinta (30) días antes del comienzo de la auditoría, y tan pronto como el Responsable del Tratamiento tenga conocimiento de dicha necesidad, con el fin de proceder a la preparación del espacio físico comprometido. En dicha Solicitud, el Responsable del Tratamiento deberá especificar:

- el alcance, que en todo caso será acotado a las obligaciones del artículo 28 RGPD,
- la ubicación,
- la duración de la auditoría,
- los nombres y DNIs de los auditores y
- un calendario con las reuniones previstas y los controles que se desean auditar en cada una.

En todo caso, las auditorías del Responsable estarán limitadas, en lo relativo a la duración en días de la auditoría, a un máximo de 3 días laborables. Las auditorías e inspecciones solo podrán tener lugar hasta la finalización del tratamiento de los datos personales por parte del Encargado de tratamiento. Además, las partes utilizarán certificaciones expedidas por el Encargado u otros informes de auditoría para evitar o minimizar auditorías repetitivas. El Responsable deberá proporcionar los resultados de cualquier auditoría al Encargado.

La auditoría no podrá tener lugar sin la firma previa de un Acuerdo de Confidencialidad con el Responsable del Tratamiento ("**NDA**"). Si decide contratar, por cuenta propia, a un tercero como firma auditora, será necesario que el Encargado del Tratamiento apruebe la firma elegida. En este caso, la firma auditora deberá firmar también el Acuerdo de Confidencialidad. Se deberá evidenciar que los auditores que efectivamente realicen la auditoría firmaron, en su contrato de trabajo, una cláusula de no divulgación de información o, en su defecto, evidenciar que procedieron a la firma de un Acuerdo de Confidencialidad antes de la realización de la auditoría.

En ningún caso, se entregará información restringida o reservada del Encargado del Tratamiento. El Responsable del Tratamiento no podrá instalar software de auditoría o scripts en los sistemas de información del Encargado del Tratamiento para la toma de datos.

g) Datos de contacto de las Partes.

Cada una de las Partes queda informada de que los datos de contacto de sus representantes y empleados serán tratados por la otra parte con la finalidad de permitir el desarrollo, cumplimiento y control de la relación de prestación de servicios concertada, siendo la base del tratamiento el cumplimiento de la relación contractual, y conservándose los datos durante todo el tiempo en que esta subsista y aún después, hasta que prescriban las eventuales responsabilidades derivadas de ella. Asimismo, cada una de las partes deberá cumplir con su obligación de información a sus respectivos representantes y empleados.

Los datos de las Partes podrán ser comunicados a los bancos y entidades financieras, para la gestión de cobros y pagos, a la Agencia Tributaria y demás Administraciones Públicas, a los efectos de llevar a cabo las declaraciones tributarias correspondientes y cumplir con sus respectivas obligaciones legales de conformidad con la normativa vigente y a las Administraciones Públicos en los casos previstos en la Ley para los fines en ellos definidos.

Las partes podrán solicitar el acceso a los datos personales a los que se refiere esta cláusula, su rectificación, su supresión, su portabilidad y la limitación de su tratamiento, así como oponerse al mismo, en el domicilio de la otra parte.

h) Responsabilidad.

El Encargado del Tratamiento será responsable de cuantas sanciones y multas se deriven del incumplimiento de lo expuesto a lo largo de este Acuerdo.

i) Vigencia, derecho aplicable y jurisdicción.

Los apéndices son una parte vinculante de este Acuerdo.

Las disposiciones del presente Acuerdo preceden a las diferentes regulaciones en materia de protección de datos personales que pueda haber en las Condiciones.

El presente Acuerdo se regulará según la ley española y el fuero competente para eventuales controversias serán los Tribunales de la ciudad de Madrid.

Si una disposición de este Acuerdo es o sea declarada nula, o no se incluyera una disposición verdaderamente necesaria, la validez de las disposiciones restantes de este Acuerdo no se verá afectada. La disposición nula o laguna legal será reemplazada por un precepto legal válido que corresponda en la mayor medida posible a las potenciales intenciones o intenciones de las Partes de acuerdo con el propósito del presente Acuerdo si las Partes hubieran tenido conocimiento de la laguna legal.

Cliente **ENCARGADO DEL TRATAMIENTO**

ANEXO IV: MODALIDAD PAQUETE LITE

1. DESCRIPCIÓN DEL PAQUETE LITE

La modalidad Paquete Lite está formada por una serie de componentes orientados a la protección del puesto de trabajo del usuario. En concreto incluye:

- Una **solución de antivirus** para el puesto de trabajo del usuario.
- **Una formación a través de un portal sobre concienciación** en ciberseguridad.

1.1 Permanencia

Este paquete no tiene asociado ningún compromiso de permanencia.

1.2 Solución de Antivirus autogestionado

Con el paquete Lite se proporciona una aplicación software de ciberseguridad, de uno de los principales fabricantes del mercado, con la que se protege la integridad y seguridad del dispositivo frente a amenazas como, por ejemplo, virus, troyanos, ransomware, exploits, comunicaciones sospechosas, sitios web no seguros etc.

La funcionalidad del software incluye:

Antimalware y antispyware

- Protección automática en tiempo real y/o bajo demanda
- Detección y bloqueo de amenazas de tipologías conocidas y avanzadas: virus, gusanos, troyanos, exploits, rootkits y spyware.
- Protección multi-nivel contra ransomware mediante diversas capas de protección contra cifrado.
- Entorno de rescate: algunos virus sofisticados, como los rootkits, han de eliminarse antes de arrancar Windows. Cuando el antivirus detecta ese tipo de amenazas, reinicia el equipo en modo Rescate para limpiarlo y restaurarlo.

Correo seguro:

- Antiphishing y antifraude, ayuda a evitar el phishing o el fraude por Internet cuando el usuario navega, compra o utiliza su banca online.
- Antispam, filtra los mensajes irrelevantes de su bandeja de entrada. Está disponible para clientes de correo electrónico locales Microsoft Outlook y Thunderbird.

Navegación segura:

- Anti-tracker: ayuda a mantener la privacidad del usuario mientras navega por Internet y le permite gestionar los rastreadores que recopilan datos.
- Banca online segura: ofrece protección en las transacciones bancarias online
- Protección de redes sociales: protege de enlaces maliciosos y de amenazas online que puedan llegar a través de las redes sociales.
- Bloqueo de adware: categoriza y filtra las webs de anuncios para limitar la presencia de adware durante la navegación.

Monitorización de red:

- Prevención de amenazas de red: incorpora nuevas tecnologías de inteligencia sobre amenazas informáticas para analizar e identificar actividades sospechosas a nivel de red y bloquear sofisticados exploits, malware o URL relacionadas con botnets, así como ataques de fuerza bruta.

Evaluación de vulnerabilidades:

- Analiza posibles vulnerabilidades y brechas de seguridad en el sistema operativo, aplicaciones y red.

Actualizaciones y consola de gestión:

- El producto se actualiza automáticamente a la versión más reciente sin necesidad de procedimiento manual de desinstalación e instalación.
- La aplicación software que se suministra dispone de una consola desde la que el cliente podrá visualizar las métricas del servicio así como modificar la configuración del mismo.

Alcance

Se proporcionará al Cliente 1 licencia por cada unidad contratada del software de antivirus autogestionado descrito en este apartado. El software se entrega (AS-IT IS) conforme a lo descrito en los Términos y Condiciones (EULA) del propio fabricante.

Durante la activación del servicio se facilitarán al cliente las instrucciones para registrarse como usuario con su email y activar su suscripción.

El cliente, si así lo prefiere, podrá solicitar asistencia para la puesta en marcha, utilizando para ello la vía y procedimiento que se le comunique en el correo de bienvenida al servicio.

El software tendrá preconfiguradas una serie de políticas de seguridad globales de aplicación a todos los usuarios, que el cliente podrá modificar posteriormente de acuerdo con sus necesidades, al ser una solución que se ofrece en modo autogestionado por el propio cliente.

Exclusiones

Queda excluida cualquier acción no definida en el alcance de la provisión, incluidas expresamente:

- La Instalación o atención in-situ.
- El despliegue en equipos no compatibles, no soportados o no licenciados.
- El despliegue en equipos que no sean propiedad del Cliente o cuya administración no esté delegada al Cliente.
- La desinstalación de software incompatible como otros antivirus.
- La instalación en equipos infectados. Cualquier manipulación de equipos informáticos fuera del software proporcionado.

1.3 Curso de Concienciación

A través de un portal se proporciona el acceso a un curso en el que se aborda de una forma amena y práctica los conceptos básicos en materia de seguridad de la información para mantener una buena primera línea de defensa en las organizaciones.

Este curso es adecuado para cualquier tipo de empleados de empresas de los diferentes sectores que utilicen para su trabajo medios electrónicos (ordenador y correo).

Temario

- Introducción
- Conceptos básicos y responsabilidad de las personas
- La información y su tratamiento
- Uso aceptable de equipamiento
- Phishing
- Malware
- Gestión de Incidencias y referencias
- Buenas prácticas en seguridad de la información

Impacto

Al finalizar el curso, el alumno sabrá acerca de:

- Principios y conceptos básicos en ciberseguridad y su importancia en entornos de trabajo.
- Tipos de amenazas y su impacto en las organizaciones
- Políticas internas en materia de seguridad de la información.
- Legislación, reglamentación y tratamiento de la información y sus implicaciones.
- Uso básico en ciberseguridad del equipamiento corporativo.
- Gestión de incidentes y sus consecuencias.
-

Duración y certificación

El curso tiene una duración aproximada de 2 horas.
Al finalizar el itinerario, el alumno realizará un test que le permite obtener un diploma (propio de la plataforma).

1.4 Modelo de prestación del servicio

Conforme a lo ya indicado en anteriores apartados, la contratación de la modalidad paquete Lite ofrece el suministro de los distintos elementos que lo componen. Será responsabilidad del cliente la instalación y gestión del software en los equipos presentes o futuros para los que ha contratado el servicio y siendo dicha responsabilidad no transferible de ningún modo a Telefónica.

ANEXO V: MODALIDAD PAQUETE BASICO

1. DESCRIPCIÓN DEL PAQUETE BASICO

El Paquete Básico del Servicio TU EMPRESA SEGURA se centra en la seguridad de los dispositivos de los usuarios. Incluye una solución de antivirus y una de detección y filtrado de amenazas para el correo electrónico, además se ofrece el soporte, mantenimiento y administración del SOC Pyme de estas dos soluciones.
Se describen a continuación con mayor detalle cada una de las soluciones incluidas, el alcance de los servicios prestados por el SOC Pyme en el proceso de instalación y durante la fase de explotación del servicio y los requisitos y tareas que tiene que realizar el Cliente para poder empezar a disfrutar del servicio.

1.1 Permanencia

Este paquete no tiene asociada ningún compromiso de permanencia.

1.2 Solución de Antivirus gestionado

Se proporcionará una solución consiste en un software o conjunto de aplicaciones de un proveedor de reconocido prestigio en el ámbito de este tipo de soluciones con el fin de prevenir que malware como virus, troyanos, ransomware o exploits puedan dañar la información contenida en los dispositivos en los que se instala.
El servicio incluye, por cada usuario contratado, (1) licencia de este software, que podrá utilizarse en 5 dispositivos diferentes (Smartphone, Tablet o PC) del mismo usuario.

El modelo de servicio será gestionado, esto es que el equipo de seguridad del SOC Pyme será el encargado de realizar las tareas de administración y mantenimiento de la solución.

El producto proporcionado consta de los siguientes módulos de seguridad:

- **Prevención de amenazas:** evita que las amenazas detectadas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis específicos en busca de malware en los sistemas en los que está instalado este software.
- **Firewall:** supervisa la comunicación entre el equipo en el que se encuentra instalado este software y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas. El Firewall analiza todo el tráfico de entrada y salida, y lo compara con su lista de reglas de firewall, el cual es un conjunto de criterios con acciones asociadas. Si un paquete coincide con todos los criterios de una regla, el firewall actúa de acuerdo con dicha regla, bloqueando o permitiendo el tráfico a través del Firewall.
- **Control web:** supervisa las búsquedas web y la actividad de navegación en los dispositivos en los que el software está instalado, bloquea los sitios web y las descargas según las calificaciones de seguridad y el contenido.
- **Protección adaptable frente a amenazas (ATP):** analiza el contenido de los dispositivos en los que está instalado el software y decide cómo responder en

función de la reputación de los archivos, las reglas y los umbrales de reputación establecidas.

Alcance

Se proporcionará al Cliente el Software asociado al presente módulo, así como las guías y procedimientos necesarios para la instalación del mismo. El software se entrega (AS-IT IS) conforme a lo descrito en los Términos y Condiciones (EULA) del propio fabricante. El software se proveerá empaquetado y pre-configurado.

Se ofrece bajo el modelo de Auto provisión, siendo el Cliente el responsable de su descarga, instalación y despliegue. No obstante, el Cliente que así lo necesite podrá solicitar el despliegue asistido por el equipo del SOC Pyme o solicitar soporte durante la instalación.

El despliegue asistido abordará la acción de instalar el software en los equipos del Cliente, de forma remota, en horario laboral 8x5 y siempre que esta instalación sea técnicamente posible de acuerdo con la política de uso razonable descrita a continuación.

Política de uso razonable

Conforme a lo estipulado, el presente servicio se presta en modelo de auto provisión siendo la responsabilidad del Cliente la instalación del software en todos los equipos, presentes o futuros para los que ha contratado el servicio y siendo dicha responsabilidad no transferible de ningún modo a Telefónica.

No obstante, como valor adicional, el Cliente podrá solicitar un soporte al SOC Pyme para que le guíe en la instalación o incluso la instalación sea realizada de forma remota por este equipo, entendiéndose que dicha acción en ningún caso exime al Cliente de la responsabilidad contemplada arriba.

Este ofrecimiento de instalación asistida o remota está amparado por una política de uso razonable donde realizada la **primera intervención** remota/telefónica, el Cliente realizará de buena fe y bajo su responsabilidad las provisiones subsiguientes amparado por la documentación y guías proporcionadas por Telefónica.

En las situaciones adicionales, donde el Cliente por causas ajenas al software entregado, requiera nuevas instalaciones, Telefónica se reserva el derecho a valorar tanto la planificación como su propia realización.

Cualquier otra acción adicional solicitada por parte del Cliente, no expresamente definida en este contrato, Telefónica se reserva el derecho a no ejecutarla.

Condiciones de uso, requisitos y limitaciones

Para la instalación en caso de despliegue asistido por parte del SOC Pyme, el cliente deberá asegurar entre otras:

- Acceso Remoto al dispositivo.
- Permisos suficientes para la instalación de software.
- Sistema Operativo compatible y con el nivel de parcheado indicado por el fabricante.
- Autorización de acceso y despliegue.

Exclusiones

Queda excluida cualquier acción no definida en el alcance de la provisión, incluidas expresamente:

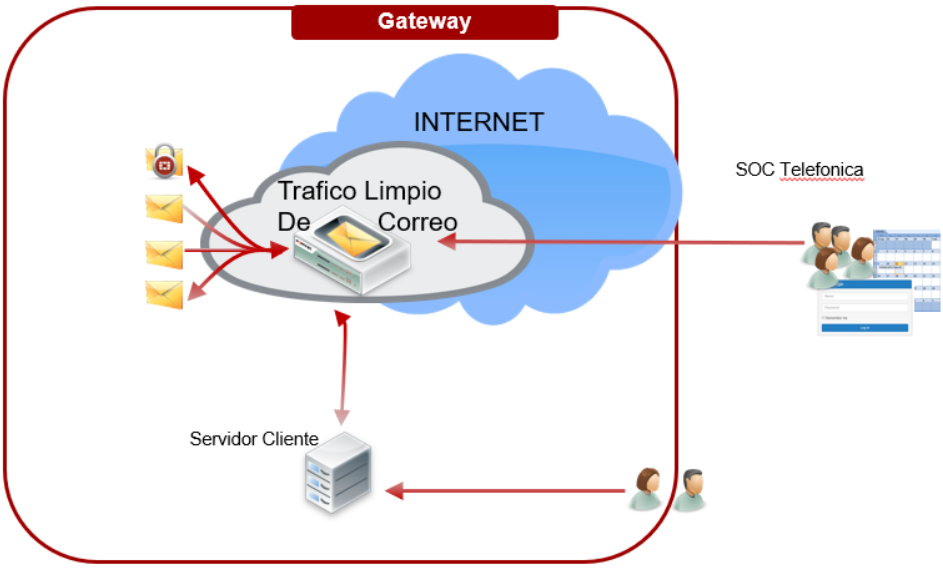
- La Instalación o atención in-situ.
- El despliegue en equipos no compatibles, no soportados o no licenciados.
- El despliegue en equipos que no sean propiedad del Cliente o cuya administración no esté delegada al Cliente.

- La desinstalación de software incompatible como otros antivirus.
- La instalación en equipos infectados. Cualquier manipulación de equipos informáticos fuera del software proporcionado.

1.3 Solución de Correo Limpio gestionado

Correo Limpio es un servicio cloud que ofrece una protección para el correo electrónico ante amenazas como el spam, malware o el phishing. Bloquea los correos sospechosos dirigidos del Cliente, y permite el cumplimiento de las políticas establecidas para el uso apropiado del correo que el Cliente defina. Detecta virus, correo basura o contenido inapropiado y en estos casos impide que lleguen por el correo, deteniéndolos antes de que entren en los sistemas de la empresa. También puede interceptar correos salientes potencialmente peligrosos antes de ser distribuidos por Internet fuera de los sistemas de la empresa.

Este servicio de filtrado del correo es independiente de las plataformas de correo de las empresas y de fácil implantación, lo que permita a las empresas complementar sus servicios de correo actuales con facilidades de antivirus, antispam, filtrado de contenidos, sin la necesidad de hacer inversiones en tecnología, ni en su mantenimiento, ni tener avanzados conocimientos en dicha tecnología, ya que el servicio incluye la administración de la herramienta por parte del equipo del SOC Pyme.



Se implementa como una puerta o pasarela gateway entrante y saliente para el correo electrónico del cliente filtrándolo en busca de spam y malware antes de reenviarlo a su destino. El correo electrónico entrante al dominio protegido, cubierto por el Servicio, se escaneará utilizando varios métodos de detección diferentes para determinar si se trata de correo electrónico no deseado, a través de filtros, como algunos los que se indican a continuación:

- Anti-Spam
- Anti-malware
- Métodos de filtrado por conexión con Listas blancas/negras, de reputación de IPs y otros tipos de listas.
- Validación de dominio remitente

Además la solución ofrece las siguiente funcionalidades adicionales:

- **Cuarentena**
  El servicio de Correo Limpio en nube analiza los correos con los mecanismos y tecnologías antes descritos y en función de los criterios que se tengan definidos en la herramienta, determina la acción a tomar. Si no detecta nada sospechoso o prohibido en el correo, lo envía al destinatario. En caso de detectar algún conflicto con las políticas definidas (por virus, spam) toma la acción establecida: borrar el mensaje, modificarlo añadiendo algún aviso o almacenarlo en lo que se ha llamado "cuarentena".
  La cuarentena permite albergar correos sospechosos o no válidos lejos de los servidores del Cliente por motivos de seguridad y para evitar saturar sus comunicaciones y sistemas con correo no deseado. La cuarentena permite (a las personas autorizadas para ello) revisar el mensaje de forma remota y así rescatar aquellos que puedan ser de interés para la empresa. Después de trascurrido el periodo de tiempo fijado durante la configuración del sistema, el sistema borrará aquellos mensajes que no han sido liberados (enviados al destinatario).
- Continuidad de correo

Este servicio incluye además, una funcionalidad para procurar la **continuidad del correo** electrónico en caso de que temporalmente el servidor de correo electrónico del cliente se encuentre indisponible o no sea accesible. En estos casos, la plataforma de limpieza del correo en nube, "pone en cola" y retiene los correos electrónicos hasta que se pueda restablecer la conexión y entregarlos al servidor de correo.

Alcance

Tras la contratación del servicio, el dominio del Cliente será provisionado por Telefónica en la plataforma y se le comunicará la disponibilidad para su uso para el número de usuarios contratados.

A partir de ese momento el Cliente tendrá que redirigir su correo a la plataforma en nube cambiando los registros MX en el Servidor de Nombres de Dominio (DNS) para que apunten a ésta. El servidor de correo del Cliente debe ser configurado para aceptar solo correo que provenga de la plataforma en nube.

Del mismo modo, el Cliente también tendrá que enviar todo su correo de salida a la plataforma, para poder garantizar el correcto funcionamiento del servicio de correo, y que no se produzca, por ejemplo, un uso malintencionado del servidor de correo del Cliente.

Se proporcionará al Cliente unas guías y procedimientos para que pueda hacer la redirección del su correo a la plataforma en nube y asistencia o soporte en caso de tener que modificar elementos internos (servidor de correo y firewall propio si lo tuviera).

Condiciones de uso, requisitos y limitaciones

- El Cliente ha de tener contratado un servicio de correo electrónico. No se incluyen los buzones de correo en el servicio, sino una solución para eliminar virus, y malware del mismo.
- Para la utilización de este servicio **el Cliente ha de tener un dominio propio**

- **El Cliente deberá contratar el servicio para todos los buzones de correo que tenga en el dominio que desea analizar con la plataforma.**
- La contratación de 1 usuario en un paquete otorga el disfrute del servicio de correo limpio para un único buzón en un único dominio. Dos buzones del mismo usuario en dominios distintos requerirían la contratación de buzones adicionales
- No se permite la utilización de la plataforma de Correo Limpio para el envío saliente de correos de dominios distintos al dominio protegido a través de la contratación del servicio.
- No está permitido el envío de correo masivo usando este servicio con el fin de evitar que el servicio de Correo Limpio pueda ser incluido en listas negras de spam.

Para mantener la integridad de la plataforma se establecen una serie de limitaciones técnicas al envío de correo saliente (con origen desde los servidores del Cliente final hacia la plataforma para ser distribuidos hacia internet).

El Cliente deberá configurar su servidor de correo con estos parámetros para un correcto funcionamiento del correo saliente a través del servicio.

Límite	Descripción	Valor
Número de conexiones simultaneas	Número de conexiones SMTP que una IP determinada puede abrir contra una máquina MTA del servicio. (por ejemplo, para enviar correo saliente). Sucesivas conexiones serán rechazadas.	5
Número de correos procesados inmediatamente por conexión	Número de correos por conexión que se procesan de inmediato. Los siguientes correos enviados en esa misma conexión se encolarán para su posterior procesado.	25

Limitaciones técnicas del servicio de correo

- En caso de falta de acceso al servidor de Correo desde la plataforma de Correo Limpio pon causas ajenas a Telefónica Empresas, ésta no será responsable de los daños causados por la imposibilidad de entrega de los correos a los Clientes ni de la posible eliminación de correos electrónicos que se produjera si la situación hace que se sobrepasen los siguientes límites para esta funcionalidad:
    a) una limitación de tiempo de hasta cinco (5) días de retención máximo a partir de la fecha de recepción; y
    b) una limitación de almacenamiento agregado de 200 GB de datos de correo electrónico.

Las presentes capacidades 200GB se refieren a la plataforma a escala global de todas las empresas que contraten el servicio y no solo dedicadas a un Cliente específico. Telefónica se reserva el derecho de modificar la capacidad de almacenamiento.

Los correos electrónicos que pudieran exceder estas limitaciones serán rechazados y pueden no ser recuperables. Los correos electrónicos almacenados en espera de entrega no serán accesibles.

La plataforma periódicamente hará intentos de envío hacia el servidor de correo del cliente.

- El Cliente será responsable de los daños causados como resultado de la acción tomada por el Cliente con respecto al correo electrónico no deseado ni de los daños causados por la eliminación de dichos correos electrónicos. Así también, si el Cliente elige liberar un correo electrónico infectado o señalado como potencialmente infectado por malware Telefónica Empresas no será responsable de los daños causados

De manera general el sistema de filtrado se aplica a los correos que entran al dominio del Cliente, pero no a los correos enviados entre cuentas del mismo dominio a menos que el Cliente así lo configure en su servidor de correo. El servicio requiere para su correcto funcionamiento de una interfaz por IP pública a la que entregar el correo entrante, y de la que recibir correo saliente. No funcionará, por tanto, con servidores de correo finales que cuenten únicamente con direccionamiento privado.

Exclusiones

Quedan expresamente excluidas:

- La configuración de los servidores DNS del Cliente.
- Será responsabilidad del cliente realizar los cambios de configuración de los registros MX de su dominio de correo para empezar a disfrutar del servicio, una vez se le haya comunicado desde Telefónica la disponibilidad del mismo
- Cambios de configuración en los servidores de correo del Cliente y/o en firewalls propiedad del Cliente (para el establecimiento de reglas que permitan el tráfico de correo desde y hacia la plataforma de Correo Limpio)

  Para estas configuraciones el Cliente podrá solicitar soporte al SOC Pyme que le guiará en las tareas a realizar.

1.4 Operación del SOC Pyme

Telefónica prestará desde el SOC Pyme el servicio de soporte, mantenimiento y administración delegada de todos los productos contratados por el Cliente en este paquete Avanzado.

El registro de peticiones, incidencias y consultas puede realizarse en cualquier momento y en cualquier día de la semana, a través de los canales de atención puestos a disposición del cliente y conforme a las características descritas en el Anexo II Atención al Cliente

Alcance

El servicio de TU EMPRESA SEGURA incluye la operación en remoto por parte del SOC Pyme del software del seguridad proporcionado y desplegado en los equipos del Cliente o en las plataformas en nube con el siguiente alcance:

- **Participación en incidentes de seguridad.** El SOC Pyme participará en el descubrimiento de los orígenes y mitigación dentro del alcance de la visión que le proporciona los equipos/software administrados de los incidentes de seguridad, no siendo en ningún caso el responsable de coordinar la gestión ni la respuesta ante dichos incidentes.

- **Participación en la resolución de Incidencias.** El SOC Pyme colaborará en la revisión de la configuración y eventos de los equipos que administra para ayudar al Cliente a solventar caídas en servicios críticos de sus procesos de negocio, sean de origen en la planta administrada por Telefónica o por el Cliente. En el caso de que el origen del problema sea por un *Sistema Monitorizado,* el SOC Pyme activará todos los mecanismos de resolución dentro de las limitaciones de los productos y sistemas desplegados con la finalidad de solventar o mitigar el problema.

- **Resolución de solicitudes**. Contempla la realización de las tareas de operación solicitadas por el Cliente y tipificadas dentro del servicio.
  Se entiende como tareas tipificadas, las siguientes, clasificadas en dos tipos:
  1) Incidencias: fallos o mal funcionamiento dentro de los servicios

2) Peticiones: solicitudes que realiza el Cliente sobre la configuración del servicio. Algunos ejemplos:
    a. Ayuda en la puesta en marcha
    b. Configuraciones respecto a listas negras y listas blancas del correo electrónico
    c. Configuraciones respecto a listas negras y listas blancas de dominios y urls

- **Identificación proactiva de riesgos**. Se informará de forma proactiva al Cliente si en el ejercicio de las funciones los administradores detectaran riesgos evidentes para la seguridad.

  Las herramientas de las soluciones desplegadas generarán alertas o indicadores de seguridad que serán revisados por el SOC Pyme bajo los criterios de seguridad y determinando si son susceptible de una actuación bien manual bien automatizada. Estará circunscrito a las únicamente al número de dispositivos/herramientas/ capacidades contratadas y siempre que éstas estén adecuadamente desplegadas conforme los criterios identificados anteriormente.

- **Corrección de vulnerabilidades identificadas en el software suministrado**. El servicio participará en la realización de los cambios necesarios para subsanar vulnerabilidades encontradas en el software suministrado.

- **Registro y control de las peticiones del servicio**. El Cliente podrá hacer una petición por cualquiera de las vías puestas a su disposición para esto y se recogerán en el portal web del servicio Tu Empresa Segura (Ver Anexo II. Atención al Cliente)
- **Comunicaciones/informes:** Recopilación de información y puesta a disposición del Cliente de informes en el portal.

- **Actualizaciones y parches**: Puesta al día de los servicios mediante actualizaciones y parches que se vayan generando los fabricantes/proveedores de los servicios.

Condiciones de uso, requisitos y limitaciones

- La comunicación con el equipo SOC Pyme deberá realizarse de la forma descrita en el apartado de atención postventa y se ofrecerá de acuerdo con el horario descrito en dicho apartado.
- Sólo se permitirá la existencia de 1 usuario autorizado (el Contacto Técnico) por sede para solicitar tareas (peticiones/consultas o incidencias) al SOC Pyme.
- Los equipos gestionados deberán tener conectividad con la plataforma de gestión, para poder ser gestionados y reportar cualquier incidente que pudiera suceder. En caso de que no tengan conectividad está información no podrá ser tratada ni las políticas aplicadas, la plataforma intentará en la medida de lo técnicamente posible la configuración y recopilación de eventos cuando el dispositivo posea nuevamente conectividad.
- El equipo del SOC Pyme podrá actualizar las políticas /reglas /bases de datos / configuraciones de seguridad con el fin de incrementar o mejorar la seguridad, estabilidad o rendimiento en el Cliente siempre que esta actuación no produzca interrupción al mismo
- En caso de actuación proactiva será siempre realizada con los criterios máximos de prudencia, con el fin de no interferir en la actividad del Cliente, de manera general, en caso de existir dudas específicas sobre la aplicabilidad de una política el equipo podrá contactar al Cliente para pedirle autorización. Siendo en este caso responsabilidad exclusiva del Cliente la actuación indicada.

- Cualquier acción proactiva de configuración o adecuación de las políticas o elementos de las plataformas podrá ser aplicadas por el equipo de soporte aún en ausencia de eventos de seguridad, y especialmente en caso de que exista una amenaza que pudiese ser masiva.
- En caso de un incidente dentro del alcance de Sistemas Monitorizados el SOC Pyme podrá solicitar pruebas, ejecutables, y evidencias que ayuden a la investigación y la determinación del mismo. El SOC Pyme se reserva el derecho de compartir dichas muestras con sus empresas partner y asociados siempre con el objetivo de incrementar el nivel de protección de los clientes. El Cliente será libre de proporcionar dicha información siempre que lo considere y entiende que, negándose a proporcionarla, la protección/investigación podrá verse gravemente mermada o ser del todo inefectiva
- El Cliente entiende y acepta que el equipo de seguridad es incapaz de actuar o mitigar cualquier ataque sobre un sistema que no esté siendo monitorizado

Exclusiones

QUEDA EXPRESAMENTE EXCLUIDO DEL SERVICIO DE **TU EMPRESA SEGURA** CUALQUIER ACTIVIDAD o SOPORTE SOBRE EQUIPOS/HERRAMIENTAS QUE NO SE ENCUENTREN INCLUIDOS EN EL MARCO DE ESTE SERVICIO Y QUE NO SE ENCUENTRE RECOGIDO EN LAS PRESENTES CONDICIONES PARTICULARES Y ANEXOS.

ANEXO VI: MODALIDAD PAQUETE AVANZADO

1. DESCRIPCIÓN DEL PAQUETE AVANZADO

El paquete Premium es el paquete intermedio que se ofrece en el Servicio. Contiene soluciones de seguridad para el puesto de trabajo y la sede del Cliente, todas ellas, con el soporte, mantenimiento y administración del SOC Pyme.
Se describen a continuación con mayor detalle cada una de las soluciones incluidas, el alcance de los servicios prestados por el SOC Pyme en el proceso de instalación y durante la fase de explotación del servicio y los requisitos y tareas que tiene que realizar el Cliente para poder empezar a disfrutar del servicio.

1.1 Permanencia

Al contratar este paquete del SERVICIO, y como consecuencia del apoyo recibido en concepto de condiciones económicas, instalación y equipamiento, el cliente se compromete a mantener vigente este producto por un periodo de 12 meses. La baja en el SERVICIO antes de finalizar el vencimiento del periodo comprometido implicará la aplicación de una penalización proporcional al tiempo no cumplido de dicho compromiso de permanencia.

1.2 Solución de Antivirus gestionado

Se proporcionará una solución consiste en un software o conjunto de aplicaciones de un proveedor de reconocido prestigio en el ámbito de este tipo de soluciones con el fin de prevenir que malware como virus, troyanos, ransomware o exploits puedan dañar la información contenida en los dispositivos en los que se instala.

El servicio incluye, por cada usuario contratado, (1) licencia de este software, que podrá utilizarse en 5 dispositivos diferentes (Smartphone, Tablet o PC) del mismo usuario.

El modelo de servicio será gestionado, esto es que el equipo de seguridad del SOC Pyme será el encargado de realizar las tareas de administración y mantenimiento de la solución.

El producto proporcionado consta de los siguientes módulos de seguridad:

- **Prevención de amenazas:** evita que las amenazas detectadas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis específicos en busca de malware en los sistemas en los que está instalado este software.
- **Firewall:** supervisa la comunicación entre el equipo en el que se encuentra instalado este software y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas. El Firewall analiza todo el tráfico de entrada y salida, y lo compara con su lista de reglas de firewall, el cual es un conjunto de criterios con acciones asociadas. Si un paquete coincide con todos los criterios de una regla, el firewall actúa de acuerdo con dicha regla, bloqueando o permitiendo el tráfico a través del Firewall.
- **Control web:** supervisa las búsquedas web y la actividad de navegación en los dispositivos en los que el software está instalado, bloquea los sitios web y las descargas según las calificaciones de seguridad y el contenido.
- **Protección adaptable frente a amenazas (ATP):** analiza el contenido de los dispositivos en los que está instalado el software y decide cómo responder en función de la reputación de los archivos, las reglas y los umbrales de reputación establecidas.

Alcance

Se proporcionará al Cliente el Software asociado al presente módulo, así como las guías y procedimientos necesarios para la instalación del mismo. El software se entrega (AS-IT IS) conforme a lo descrito en los Términos y Condiciones (EULA) del propio fabricante. El software se proveerá empaquetado y pre-configurado.

Se ofrece bajo el modelo de Auto provisión, siendo el Cliente el responsable de su descarga, instalación y despliegue. No obstante, el Cliente que así lo necesite podrá solicitar el despliegue asistido por el equipo del SOC Pyme o solicitar soporte durante la instalación.

El despliegue asistido abordará la acción de instalar el software en los equipos del Cliente, de forma remota, en horario laboral 8x5 y siempre que esta instalación sea técnicamente posible de acuerdo con la política de uso razonable descrita a continuación.

Política de uso razonable

Conforme a lo estipulado, el presente servicio se presta en modelo de auto provisión siendo la responsabilidad del Cliente la instalación del software en todos los equipos, presentes o futuros, para los que ha contratado el servicio y siendo dicha responsabilidad no transferible de ningún modo a Telefónica.

No obstante, como valor adicional, el Cliente podrá solicitar un soporte al SOC Pyme para que le guíe en la instalación o incluso la instalación sea realizada de forma remota por este equipo, entendiéndose que dicha acción en ningún caso exime al Cliente de la responsabilidad contemplada arriba.

Este ofrecimiento de instalación asistida o remota está amparado por una política de uso razonable donde realizada la **primera intervención** remota/telefónica, el Cliente realizará de buena fe y bajo su responsabilidad las provisiones subsiguientes amparado por la documentación y guías proporcionadas por Telefónica.

En las situaciones adicionales, donde el Cliente por causas ajenas al software entregado, requiera nuevas instalaciones, Telefónica se reserva el derecho a valorar tanto la planificación como su propia realización.

Cualquier otra acción adicional solicitada por parte del Cliente, no expresamente definida en este contrato, Telefónica se reserva el derecho a no ejecutarla.

Condiciones de uso, requisitos y limitaciones

Para la instalación en caso de despliegue asistido por parte del SOC Pyme, el cliente deberá asegurar entre otras:

- Acceso Remoto al dispositivo.
- Permisos suficientes para la instalación de software.
- Sistema Operativo compatible y con el nivel de parcheado indicado por el fabricante.
- Autorización de acceso y despliegue.

Exclusiones

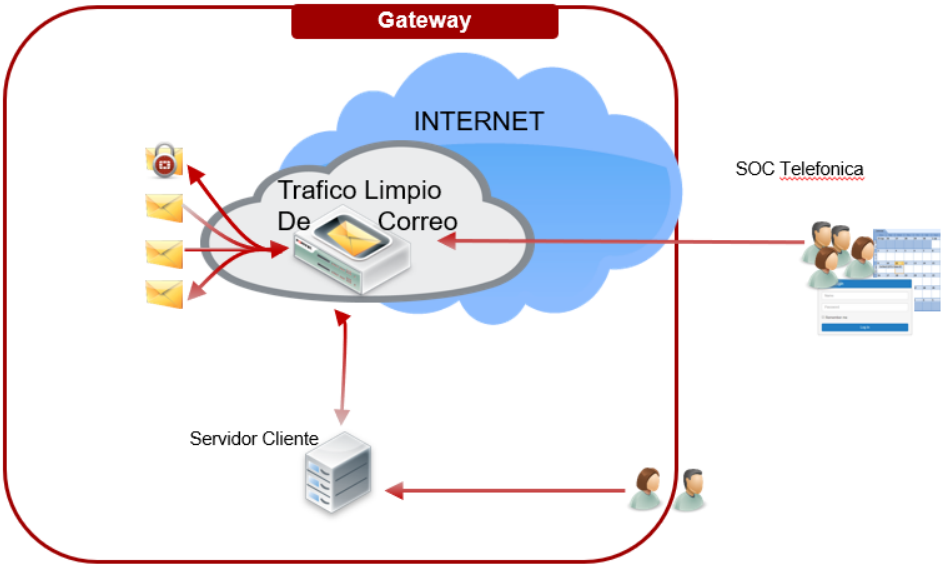
Queda excluida cualquier acción no definida en el alcance de la provisión, incluidas expresamente:

- La Instalación o atención in-situ.
- El despliegue en equipos no compatibles, no soportados o no licenciados.
- El despliegue en equipos que no sean propiedad del Cliente o cuya administración no esté delegada al Cliente.
- La desinstalación de software incompatible como otros antivirus.
- La instalación en equipos infectados. Cualquier manipulación de equipos informáticos fuera del software proporcionado.

1.3 Solución de Correo Limpio gestionado

Correo Limpio es un servicio cloud que ofrece una protección para el correo electrónico ante amenazas como el spam, malware y phishing. Bloquea los correos sospechosos dirigidos del Cliente, y permite el cumplimiento de las políticas establecidas para el uso apropiado del correo que el Cliente defina. Detecta virus, correo basura o contenido inapropiado y en estos casos impide que lleguen por el correo, deteniéndolos antes de que entren en los sistemas de la empresa. También puede interceptar correos salientes potencialmente peligrosos antes de ser distribuidos por Internet fuera de los sistemas de la empresa.

Este servicio de filtrado del correo es independiente de las plataformas de correo de las empresas y de fácil implantación, lo que permita a las empresas complementar sus servicios de correo actuales con facilidades de antivirus, antispam, filtrado de contenidos, sin la necesidad de hacer inversiones en tecnología, ni en su mantenimiento, ni tener avanzados conocimientos en dicha tecnología, ya que el servicio incluye la administración de la herramienta por parte del equipo del SOC Pyme.



Se implementa como una puerta o pasarela gateway entrante y saliente para el correo electrónico del cliente filtrándolo en busca de spam y malware antes de reenviarlo a su destino. El correo electrónico entrante al dominio protegido, cubierto por el Servicio, se escaneará utilizando varios métodos de detección diferentes para determinar si se trata de correo electrónico no deseado, a través de filtros, como algunos los que se indican a continuación:

- Anti-Spam
- Anti-malware
- Métodos de filtrado por conexión con Listas blancas/negras, de reputación de IPs, y otras listas.
- Validación de dominio remitente

Además la solución ofrece las siguiente funcionalidades adicionales:

- **Cuarentena**

  El servicio de Correo Limpio en nube analiza los correos con los mecanismos y tecnologías antes descritos y en función de los criterios que se tengan definidos en la herramienta, determina la acción a tomar. Si no detecta nada sospechoso o prohibido en el correo, lo envía al destinatario. En caso de detectar algún conflicto con las políticas definidas (por virus, spam) toma la acción establecida: borrar el mensaje, modificarlo añadiendo algún aviso o almacenarlo en lo que se ha llamado "cuarentena".

  La cuarentena permite albergar correos sospechosos o no válidos lejos de los servidores del Cliente por motivos de seguridad y para evitar saturar sus comunicaciones y sistemas con correo no deseado. La cuarentena permite (a las personas autorizadas para ello) revisar el mensaje de forma remota y así rescatar aquellos que puedan ser de interés para la empresa. Después de trascurrido el periodo de tiempo fijado durante la configuración del sistema, el sistema borrará aquellos mensajes que no han sido liberados (enviados al destinatario).

- **Continuidad de correo**

  Este servicio incluye además, una funcionalidad para procurar la continuidad del correo electrónico en caso de que temporalmente el servidor de correo electrónico del cliente se encuentre indisponible o no sea accesible. En estos casos, la plataforma de limpieza del correo en nube, "pone en cola" y retiene los correos electrónicos hasta que se pueda restablecer la conexión y entregarlos al servidor de correo.

Alcance

Tras la contratación del servicio, el dominio del Cliente será provisionado por Telefónica en la plataforma y se le comunicará la disponibilidad para su uso para el número de usuarios contratados.

A partir de ese momento el Cliente tendrá que redirigir su correo a la plataforma en nube cambiando los registros MX en el Servidor de Nombres de Dominio (DNS) para que apunten a ésta. El servidor de correo del Cliente debe ser configurado para aceptar solo correo que provenga de la plataforma en nube.

Del mismo modo, el Cliente también tendrá que enviar todo su correo de salida a la plataforma, para poder garantizar el correcto funcionamiento del servicio de correo, y que no se produzca, por ejemplo, un uso malintencionado del servidor de correo del Cliente.

Se proporcionará al Cliente unas guías y procedimientos para que pueda hacer la redirección del su correo a la plataforma en nube y asistencia o soporte en caso de tener que modificar elementos internos (servidor de correo y firewall propio si lo tuviera).

Condiciones de uso, requisitos y limitaciones

- El Cliente ha de tener contratado un servicio de correo electrónico. No se incluyen los buzones de correo en el servicio, sino una solución para eliminar virus y malware del mismo.

- Para la utilización de este servicio **el Cliente ha de tener un dominio propio**
- **El Cliente deberá contratar el servicio para todos los buzones de correo que tenga en el dominio que desea analizar con la plataforma.**
- La contratación de 1 usuario en un paquete otorga el disfrute del servicio de correo limpio para un único buzón en un único dominio. Dos buzones del mismo usuario en dominios distintos requerirían la contratación de buzones adicionales
- No se permite la utilización de la plataforma de Correo Limpio para el envío saliente de correos de dominios distintos al dominio protegido a través de la contratación del servicio.
- No está permitido el envío de correo masivo usando este servicio con el fin de evitar que el servicio de Correo Limpio pueda ser incluido en listas negras de spam.

Para mantener la integridad de la plataforma se establecen una serie de limitaciones técnicas al envío de correo saliente (con origen desde los servidores del Cliente final hacia la plataforma para ser distribuidos hacia internet).

El Cliente deberá configurar su servidor de correo con estos parámetros para un correcto funcionamiento del correo saliente a través del servicio.

Límite	Descripción	Valor
Número de conexiones simultaneas	Número de conexiones SMTP que una IP determinada puede abrir contra una máquina MTA del servicio. (por ejemplo, para enviar correo saliente). Sucesivas conexiones serán rechazadas.	5
Número de correos procesados inmediatamente por conexión	Número de correos por conexión que se procesan de inmediato. Los siguientes correos enviados en esa misma conexión se encolarán para su posterior procesado.	25

Limitaciones técnicas del servicio de correo

- En caso de falta de acceso al servidor de Correo desde la plataforma de Correo Limpio pon causas ajenas a Telefónica Empresas, ésta no será responsable de los daños causados por la imposibilidad de entrega de los correos a los Clientes ni de la posible eliminación de correos electrónicos que se produjera si la situación hace que se sobrepasen los siguientes límites para esta funcionalidad:
    a) una limitación de tiempo de hasta cinco (5) días de retención máximo a partir de la fecha de recepción; y
    b) una limitación de almacenamiento agregado de 200 GB de datos de correo electrónico.

Las presentes capacidades 200GB se refieren a la plataforma a escala global de todas las empresas que contraten el servicio y no solo dedicadas a un Cliente específico. Telefónica se reserva el derecho de modificar la capacidad de almacenamiento.

Los correos electrónicos que pudieran exceder estas limitaciones serán rechazados y pueden no ser recuperables. Los correos electrónicos almacenados en espera de entrega no serán accesibles.

La plataforma periódicamente hará intentos de envío hacia el servidor de correo del cliente.

- El Cliente será responsable de los daños causados como resultado de la acción tomada por el Cliente con respecto al correo electrónico no deseado ni de los daños causados por la eliminación de dichos correos electrónicos. Así también, si el Cliente elige liberar

un correo electrónico infectado o señalado como potencialmente infectado por malware Telefónica Empresas no será responsable de los daños causados
De manera general el sistema de filtrado se aplica a los correos que entran al dominio del Cliente, pero no a los correos enviados entre cuentas del mismo dominio a menos que el Cliente así lo configure en su servidor de correo. El servicio requiere para su correcto funcionamiento de una interfaz por IP pública a la que entregar el correo entrante, y de la que recibir correo saliente. No funcionará, por tanto, con servidores de correo finales que cuenten únicamente con direccionamiento privado.

Exclusiones

Quedan expresamente excluidas:

- La configuración de los servidores DNS del Cliente.
- Será responsabilidad del cliente realizar los cambios de configuración de los registros MX de su dominio de correo para empezar a disfrutar del servicio, una vez se le haya comunicado desde Telefónica la disponibilidad del mismo
- Cambios de configuración en los servidores de correo del Cliente y/o en firewalls propiedad del Cliente (para el establecimiento de reglas que permitan el tráfico de correo desde y hacia la plataforma de Correo Limpio)

  Para estas configuraciones el Cliente podrá solicitar soporte al SOC Pyme que le guiará en las tareas a realizar.

1.4 UTM Gestionado

Esta funcionalidad proporciona mediante el despliegue y configuración de un dispositivo Firewall de Nueva Generación, UTM, basado en una tecnología de un reconocido proveedor en el ámbito de la Gestión de Amenazas Unificadas en la sede del cliente, con la gestión en remoto del mismo por parte del equipo del SOC Pyme.

Esta plataforma servirá para crear una frontera o perímetro entre Internet y la red interna del Cliente, monitorizando los flujos de información entre ambas redes, pudiendo aplicar:

- Filtrado Antivirus.
- Protección frente ataques.
- Detección y control de aplicaciones.
- Control de navegación de usuarios internos.
- Protección antimalware.
- Visibilidad y obtención de informes
- Acceso Remoto Seguro (túneles): VPN (Site2Site o Portal VPN SSL).
- Balanceo de líneas: gestionando el que el tráfico para que entre por una de las 2 líneas Movistar

Mediante este dispositivo se protege la red de una empresa de las principales amenazas de seguridad permitiendo monitorizar, filtrar y aplicar políticas de seguridad a todo su tráfico (saliente y entrante) de internet. Además, se ofrece una mejora a Cliente al permitir la

priorización de las aplicaciones de negocio sobre tráfico no productivo que pudieran estar utilizando sus empleados.

Gracias a este UTM el Cliente dispondrá de la funcionalidad de VPN para que el personal de su empresa pueda trabajar remotamente y con sus propios equipos desde cualquier lugar, navegando y accediendo de forma segura a las aplicaciones y archivos de su empresa.

Todo ello gestionado por expertos en seguridad desde el SOC Pyme, desde donde se ofrecerá al Cliente una atención personalizada.

Opciones contratables asociadas al UTM gestionado

En el momento de la contratación inicial de un paquete Avanzado es posible seleccionar una o las dos siguientes opciones:

- **Modelo superior de equipamiento**

  El equipamiento UTM se dimensiona en el momento de la contratación, en función del número de usuarios que se incluyen en el paquete, de la siguiente forma:

Rango de usuarios en la sede	Modelo correspondiente por defecto	Upgrade permitido
De 4 a 50 usuarios /sede	UTM1	UTM2
De 51 a 100 usuarios /sede	UTM2	UTM3
De 101 a 150 usuarios/sede	UTM3	UTM4
De 151 a 200 usuarios/sede	UTM4	No aplica

  Es posible contratar la opción de Upgrade, para que el modelo incluido en el servicio sea el inmediatamente superior.

- **Alta disponibilidad (HA)**

  Con la contratación de esta opción, se desplegarán 2 equipos del mismo modelo en la sede del Cliente para poder configurar la alta disponibilidad de este servicio.

En caso de seleccionar las dos opciones, se desplegarán 2 equipos UTM del modelo superior. No es posible tener dos modelos distintos.

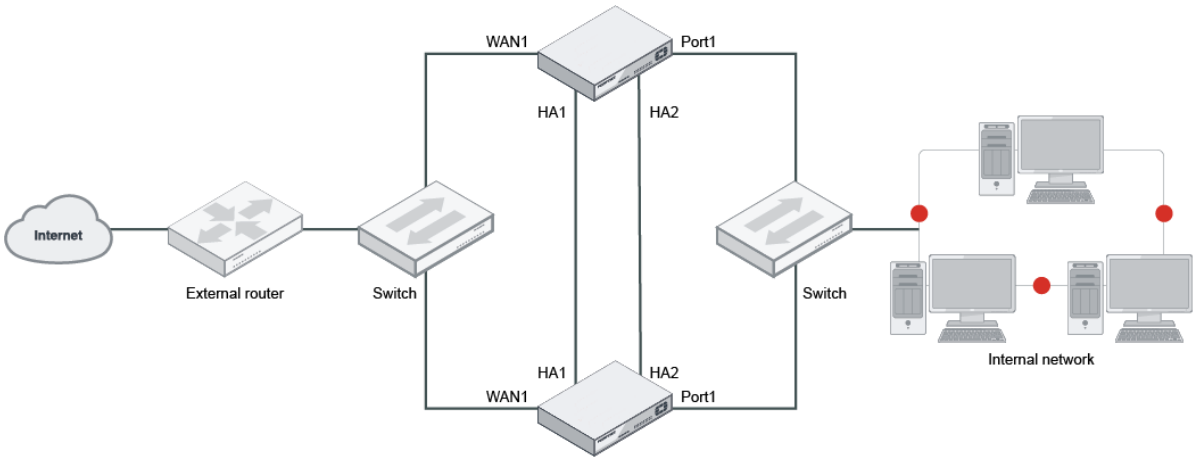
Modalidades de despliegue UTM

- **Simple**

  El dispositivo se desplegará en la sede del Cliente funcionando como elemento de seguridad entre el acceso a internet y la red interna. Al estar montado un solo dispositivo se le considera un punto único de fallo.

- **Alta disponibilidad (HA)**

  El Cliente puede elegir el despliegue en modo activo/pasivo de tal forma que en hipotético caso de que fallase uno de los dispositivos el otro continuaría prestando el servicio de protección a la sede.



Para poder desplegar el servicio en modo **alta disponibilidad es necesario la contratación de esta opción HA en el momento de contratación del Paquete Avanzado para que se desplieguen 2 dispositivos**

Modalidades de despliegue en presencia de dos accesos a internet

- **Activo/Pasivo**

El UTM utilizará de manera primaria la línea definida de acceso a internet, y en caso de fallo enrutará el tráfico por el otro acceso a internet.

- **Balanceado**

El UTM utilizará de manera agregada cada una de las líneas de acceso a internet.

Alcance de la provisión

Se suministrarán al Cliente/Empresa el equipamiento mencionado más arriba. Este servicio aborda todas las tareas necesarias para la adquisición y entrega al Cliente del equipamiento contratado, así como los servicios profesionales necesarios para la instalación inicial de los mismos, cubriendo la configuración básica de los equipos (interfaces de red, direccionamiento, rutas) y la configuración necesaria para dejar operativos las funcionalidades del equipo.

Las tareas a realizar son:

- Envío e instalación del equipamiento a un destino del Cliente ubicado en España.
- Preconfiguración y conectividad por parte de Telefónica.
- Puesta en marcha en remoto de la plataforma. Esta puesta en marcha está basada en el modelo definido por el SOC Pyme y especificada en la **política de uso razonable** de este apartado.
- Aplicación de la configuración básica.
- Parametrización y ajuste de la plataforma según requisitos identificados con Cliente:
    - Servicio navegación.
    - Publicación de servicios.
    - Antivirus.
    - IPS (Intrusion Prevention System)
    - Filtrado web
    - Control de aplicaciones
    - AntiDOS
    - VPN Site to Site.

- VPN SSL (definición de portales, usuarios, redes que se instalan…).
- Pruebas.
- Paso a explotación.

Política de uso razonable para la provisión de UTM

La puesta en marcha está basada en la disponibilidad de una bolsa de provisión a consumir por parte del Cliente final, en concreto, veinticinco (25) puntos, teniendo en cuenta el esfuerzo identificado en la tabla siguiente. La configuración por defecto consumiría 16 puntos

FUNCIONALIDAD		COSTE	OBSERVACIONES
1 x VPN Site-to -Site		**3**	
1x Portal VPN SSL		**2**	Con autenticación de usuarios en Local
Integración LDAP/AD		**4**	El técnico asignado solicitará los datos concretos
Balanceo/backup de 2 líneas Movistar		**4**	
Activación DoS			
	Por Defecto	**1**	Sólo modo monitor
	Personalizado	**2**	Estudio de umbrales excluido
Control de aplicaciones			
	Por Defecto	**1**	Categorías fijas.
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
Filtrado web			
	Por Defecto	**1**	Categorías fijas.
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
IPS			
	Por Defecto	**1**	Perfil fijo. Protección workstations.
	Personalizado	**2**	Perfiles personalizados, servidores
Antivirus			
	Por Defecto	**1**	Modo flujo aplicado en salida.
	Personalizado	**2**	Modo Proxy
Creación Reglas Firewall			Las reglas por defecto para cada facilidad no se incluyen aquí
	Regla < 10 objetos	**1**	
	Regla > 10 objetos	**2**	
Solicitud funcionalidades complejas no contempladas		**4**	El técnico asignado solicitará los datos concretos

Condiciones de uso, requisitos y limitaciones

Para poder disfrutar del servicio el Cliente ha de disponer de línea de comunicaciones contratada con y con **direccionamiento IP público estático**.

Las comunicaciones soportadas son:

- **Movistar Fusión Digital:**
  - Router de Cliente gestionado por Telefónica.
  - El servicio es incompatible con los siguientes escenarios de conectividad de Fusión Digital: con switches de 100 MBs. (en caso de darse esta situación el Cliente **deberá actualizar sus switches**)

- **FTTH Residencial/ADSL/VDSL:**
  Router gestionado por el propio Cliente. El Cliente debe cambiar la configuración de router a "monopuesto" para permitir acceso remoto del SOC Pyme al UTM.

Dado que en la contratación de los paquetes Avanzado y Premium **se dimensiona el modelo de dispositivo a desplegar** en la sede del Cliente en función del **número de usuarios contratados** en el paquete, podrían verse mermadas las prestaciones del servicio al Cliente en caso de que el número de usuarios que trabajen en dicha sede (utilicen la conectividad) sea superior al indicado.

Cualquier problema derivado de un incorrecto dimensionamiento por esta causa será responsabilidad exclusiva del Cliente.

Exclusiones

Quedan expresamente excluidos de la cobertura del suministro e Instalación del equipamiento UTM:

- Cualquier tipo de instalación eléctrica en el bastidor (rack) o ubicación donde se vaya a instalar el equipamiento contratado.
- Cableado de red fuera del bastidor (rack) donde físicamente se instale el equipamiento.
- Cables de red o alimentación adicionales a los que vengan incluidos en el propio equipamiento y que han sido suministrados por el fabricante.
- Los trabajos de migración de políticas desde otros dispositivos.
- Cualquier daño debido a fallos de la instalación eléctrica a la que se hallen conectados los equipos o s defectos originados por carecer el local donde se halle ubicado el material de las condiciones de entorno exigidas por el fabricante en las especificaciones técnicas de los equipos.
- El Cliente entiende y es consciente de que el lugar donde solicite a Telefónica la instalación ha de tener adecuadas las instalaciones tanto en conectividad, espacio y fuerza eléctrica. Además de tener preparadas las configuraciones o accesos a elementos de conectividad que así sea necesario.

  En caso de que durante la visita no pueda realizarse la instalación por causas ajenas a Telefónica, ésta podrá facturar al Cliente el desplazamiento del técnico.

- Las configuraciones asociadas directamente al router del Cliente, deberán ser realizadas por parte de éste siempre que sea posible (en conectividad de residencial) o con el soporte de Telefónica en caso de que dicha configuración en el equipo no sea accesible para el Cliente (servicios de Conectividad de Telefónica Empresas-1002)
- Cualquier tarea que no esté explícitamente descrita en la presente oferta.

Al realizar la instalación y configuración del Firewall UTM, por defecto, se desactiva el WiFi del router. Si el Cliente desea asegurar también el acceso Wi-Fi, debe adquirir AP/s (Punto/s de acceso) Wi-fi y conectarlo/s a su LAN para garantizar la supervisión de ésta mediante el firewall. Queda excluido del alcance de esta oferta, el suministro y configuración de APs Wi-fi.

1.5 Curso de Concienciación

Este curso es adecuado para cualquier tipo de empleados de empresas de los diferentes sectores que utilicen para su trabajo medios electrónicos (ordenador, correo). Se aborda de una forma amena y práctica los conceptos básicos en materia de seguridad de la información para mantener una buena primera línea de defensa en las organizaciones.

Impacto

Al finalizar el curso, los alumnos sabrán:

- Principios y conceptos básicos en ciberseguridad y su importancia en entornos de trabajo.
- Tipos de amenazas y su impacto en las organizaciones
- Políticas internas en materia de seguridad de la información.
- Legislación, reglamentación y tratamiento de la información y sus implicaciones.
- Uso básico en ciberseguridad del equipamiento corporativo.
- Gestión de incidentes y sus consecuencias.

Temario

- Introducción
- Conceptos básicos y responsabilidad de las personas
- La información y su tratamiento
- Uso aceptable de equipamiento
- Phishing
- Malware
- Gestión de Incidencias y referencias
- Buenas prácticas en seguridad de la información

Este temario podrá sufrir modificaciones, en función de la evolución de la ciberseguridad de las pymes, sus conocimientos o los cambios que puedan producirse en el servicio.

Duración y certificación

El curso tiene una duración aproximada de 2 horas.

Al finalizar el itinerario, el alumno realizará un test que le permite obtener un diploma (propio de la plataforma).

Esta duración tiene relación directa con el temario actual. En caso de que se modifique el temario, la duración del curso es susceptible de ser modificada.

1.6 Operación del SOC Pyme

Telefónica prestará desde el SOC Pyme el servicio de soporte, mantenimiento y administración delegada de todos los productos contratados por el Cliente en este Paquete Avanzado.

El registro de peticiones, incidencias y consultas puede realizarse en cualquier momento y en cualquier día de la semana, a través de los canales de atención puestos a disposición del cliente y conforme a las características descritas en el Anexo II Atención al Cliente

Alcance

El servicio de TU EMPRESA SEGURA incluye la operación en remoto por parte del SOC Pyme del software del seguridad proporcionado y desplegado en los equipos del Cliente o en las plataformas en nube con el siguiente alcance:

- **Participación en incidentes de seguridad.** El SOC Pyme participará en el descubrimiento de los orígenes y mitigación dentro del alcance de la visión que le proporciona los equipos/software administrados de los incidentes de seguridad, no siendo en ningún caso el responsable de coordinar la gestión ni la respuesta ante dichos incidentes.

- **Participación en la resolución de Incidencias.** El SOC Pyme colaborará en la revisión de la configuración y eventos de los equipos que administra para ayudar al Cliente a solventar caídas en servicios críticos de sus procesos de negocio, sean de origen en la planta administrada por Telefónica o por el Cliente. En el caso de que el origen del problema sea por un *Sistema Monitorizado,* el SOC Pyme activará todos los mecanismos de resolución dentro de las limitaciones de los productos y sistemas desplegados con la finalidad de solventar o mitigar el problema.
- **Resolución de solicitudes**. Contempla la realización de las tareas de operación solicitadas por el Cliente y tipificadas dentro del servicio.
  Se entiende como tareas tipificadas, las siguientes, clasificadas en dos tipos:
  3) Incidencias: fallos o mal funcionamiento dentro de los servicios
  4) Peticiones: solicitudes que realiza el Cliente sobre la configuración del servicio. Algunos ejemplos:
     d. Ayuda en la puesta en marcha
     e. Configuraciones respecto a listas negras y listas blancas del correo electrónico
     f. Configuraciones respecto a listas negras y listas blancas de dominios y urls
     g. Apertura de puertos
     h. Gestión de usuarios de la VPN

- **Identificación proactiva de riesgos**. Se informará de forma proactiva al Cliente si en el ejercicio de las funciones los administradores detectaran riesgos evidentes para la seguridad.

  Las herramientas de las soluciones desplegadas generarán alertas o indicadores de seguridad que serán revisados por el SOC Pyme bajo los criterios de seguridad y determinando si son susceptible de una actuación bien manual bien automatizada. Estará circunscrito a las únicamente al número de dispositivos/herramientas/ capacidades contratadas y siempre que éstas estén adecuadamente desplegadas conforme los criterios identificados anteriormente.

- **Corrección de vulnerabilidades identificadas en el software suministrado**. El servicio participará en la realización de los cambios necesarios para subsanar vulnerabilidades encontradas en el software suministrado.

- **Registro y control de las peticiones del servicio**. El Cliente podrá hacer una petición por cualquiera de las vías puestas a su disposición para esto y se recogerán en el portal web del servicio Tu Empresa Segura (Ver Anexo de Atención Postventa en el contrato de condiciones generales del servicio Tu Empresa Segura)
- **Mantenimiento y soporte de los equipos UTM**
  En lo referente a las tareas de mantenimiento relacionadas con el dispositivo o dispositivos UTM, Telefónica Empresas prestará el servicio de mantenimiento remoto encaminado a solucionar las situaciones en las que el dispositivo UTM muestre una indisponibilidad. En el caso de que se determine una avería en alguno de los componentes del dispositivo, Telefónica Empresas gestionará la sustitución de la pieza o el equipo completo (RMA) según la situación y el contrato suscrito con el fabricante.

  Una vez se ha diagnosticado la avería según los requisitos que el fabricante establece en sus condiciones de activación de RMAs (en base a los tiempos establecidos en el contrato del equipamiento con el fabricante), se realizará la gestión para la entrega del equipo al cliente, restaurando la última configuración operativa del dispositivo.
- **Comunicaciones/informes:** Recopilación de información y puesta a disposición del Cliente de informes en el portal.
- **Actualizaciones y parches**: Puesta al día de los servicios mediante actualizaciones y parches que se vayan generando los fabricantes/proveedores de los servicios.

Condiciones de uso, requisitos y limitaciones

- La comunicación con el equipo SOC Pyme deberá realizarse de la forma descrita y en el horario indicado en el Anexo II ATENCIÓN AL Cliente.
- Sólo se permitirá la existencia de 1 usuario autorizado (el Contacto Técnico) por sede para solicitar tareas (peticiones/consultas o incidencias) al SOC Pyme.
- Los equipos gestionados deberán tener conectividad con la plataforma de gestión, para poder ser gestionados y reportar cualquier incidente que pudiera suceder. En caso de que no tengan conectividad está información no podrá ser tratada ni las políticas aplicadas, la plataforma intentará en la medida de lo técnicamente posible la configuración y recopilación de eventos cuando el dispositivo posea nuevamente conectividad.
- Al ser un Servicio administrado por el SOC Pyme, el Cliente no contará con permisos de administrador sobre ninguna de las consolas de gestión de las herramientas incluidas (Antivirus gestionado, Correo Limpio gestionado, ni UTM gestionado).
- El equipo del SOC Pyme podrá actualizar las políticas /reglas /bases de datos / configuraciones de seguridad con el fin de incrementar o mejorar la seguridad, estabilidad o rendimiento en el Cliente siempre que esta actuación no produzca interrupción al mismo
- En caso de actuación proactiva será siempre realizada con los criterios máximos de prudencia, con el fin de no interferir en la actividad del Cliente, de manera general, en caso de existir dudas específicas sobre la aplicabilidad de una política el equipo podrá contactar al Cliente para pedirle autorización. Siendo en este caso responsabilidad exclusiva del Cliente la actuación indicada.
- Cualquier acción proactiva de configuración o adecuación de las políticas o elementos de las plataformas podrá ser aplicadas por el equipo de soporte aún en ausencia de eventos de seguridad, y especialmente en caso de que exista una amenaza que pudiese ser masiva.
- En caso de un incidente dentro del alcance de Sistemas Monitorizados el SOC Pyme podrá solicitar pruebas, ejecutables, y evidencias que ayuden a la investigación y la determinación del mismo. El SOC Pyme se reserva el derecho de compartir dichas muestras con sus empresas partner y asociados siempre con el objetivo de incrementar el

nivel de protección de los clientes. El Cliente será libre de proporcionar dicha información siempre que lo considere y entiende que, negándose a proporcionarla, la protección/investigación podrá verse gravemente mermada o ser del todo inefectiva

- El Cliente entiende y acepta que el equipo de seguridad es incapaz de actuar o mitigar cualquier ataque sobre un sistema que no esté siendo monitorizado

Política de uso razonable para la operación del equipamiento UTM

El servicio de administración delegada del SOC Pyme se basa en la disponibilidad de una bolsa de gestión a consumir por parte del Cliente, en concreto, cinco (5) puntos mensuales, teniendo en cuenta el siguiente esfuerzo por tipo de solicitud:

FUNCIONALIDAD		COSTE	OBSERVACIONES
1 x VPN Site-to -Site		**3**	
1x Portal VPN SSL		**2**	Con autenticación de usuarios en Local
Integración LDAP/AD		**4**	El técnico asignado solicitará los datos concretos
Balanceo/backup de 2 líneas Movistar		**4**	
Activación DoS			
	Por Defecto	**1**	Sólo modo monitor
	Personalizado	**2**	Estudio de umbrales excluido
Control de aplicaciones			
	Por Defecto	**1**	Categorías fijas
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
Filtrado web			
	Por Defecto	**1**	Categorías fijas
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
IPS			
	Por Defecto	**1**	Perfil fijo. Protección workstations.
	Personalizado	**2**	Perfiles personalizados, servidores
Antivirus			
	Por Defecto	**1**	Modo flujo aplicado en salida.
	Personalizado	**2**	Modo Proxy
Creación Reglas Firewall			Las reglas por defecto para cada facilidad no se incluyen aquí
	Regla < 10 objetos	**1**	
	Regla > 10 objetos	**2**	
Solicitud funcionalidades complejas no contempladas		**4**	El técnico asignado solicitará los datos concretos

El Cliente entiende y acepta que no podrá excederse del número de puntos indicados y que no puede excederse más de 1 mes del número de puntos disponibles.

A continuación, se indican unas métricas que Telefónica considera un uso razonable de los esfuerzos de servicios profesionales que sustentan la operativa del servicio.

Métricas por actividad, cantidad y periodicidad

Actividad	Cantidad	Periodicidad
Resolución incidencias de negocio	Todas con afectación de servicio	Continua
Resolución incidencias de seguridad	Todas	Continua
Resolución solicitudes	5 puntos mensuales	Contrato
Registro y Control peticiones de servicio	Todas	Continua

Exclusiones

QUEDA EXPRESAMENTE EXCLUIDO DEL SERVICIO DE **TU EMPRESA SEGURA** CUALQUIER ACTIVIDAD o SOPORTE SOBRE EQUIPOS/HERRAMIENTAS QUE NO SE ENCUENTREN INCLUIDOS EN EL MARCO DE ESTE SERVICIO Y QUE NO SE ENCUENTRE RECOGIDO EN LAS PRESENTES CONDICIONES PARTICULARES Y ANEXOS.

ANEXO VII: MODALIDAD PAQUETE PREMIUM

1. DESCRIPCIÓN DEL PAQUETE PREMIUM

El paquete Premium es el paquete que incluye un mayor número de soluciones de seguridad del servicio Tu Empresa Segura, todas ellas, con el soporte, mantenimiento y administración del SOC Pyme.
Se describen a continuación con mayor detalle cada una de las soluciones incluidas, el alcance de los servicios prestados por el SOC Pyme en el proceso de instalación y durante la fase de explotación del servicio y los requisitos y tareas que tiene que realizar el Cliente para poder empezar a disfrutar del servicio.

1.1 Permanencia

Al contratar este paquete del SERVICIO, y como consecuencia del apoyo recibido en concepto de condiciones económicas, instalación y equipamiento, el cliente se compromete a mantener vigente este producto por un periodo de 12 meses. La baja en el SERVICIO antes de finalizar el vencimiento del periodo comprometido implicará la aplicación de una penalización proporcional al tiempo no cumplido de dicho compromiso de permanencia.

1.2 Solución de Antivirus gestionado

Se proporcionará una solución consiste en un software o conjunto de aplicaciones de un proveedor de reconocido prestigio en el ámbito de este tipo de soluciones con el fin de prevenir que malware como virus, troyanos, ransomware o exploits puedan dañar la información contenida en los dispositivos en los que se instala.

El servicio incluye, por cada usuario contratado, (1) licencia de este software, que podrá utilizarse en 5 dispositivos diferentes (Smartphone, Tablet o PC) del mismo usuario.

El modelo de servicio será gestionado, esto es que el equipo de seguridad del SOC Pyme será el encargado de realizar las tareas de administración y mantenimiento de la solución.

El producto proporcionado consta de los siguientes módulos de seguridad:

- **Prevención de amenazas:** evita que las amenazas detectadas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis específicos en busca de malware en los sistemas en los que está instalado este software.
- **Firewall:** supervisa la comunicación entre el equipo en el que se encuentra instalado este software y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas. El Firewall analiza todo el tráfico de entrada y salida, y lo compara con

su lista de reglas de firewall, el cual es un conjunto de criterios con acciones asociadas. Si un paquete coincide con todos los criterios de una regla, el firewall actúa de acuerdo con dicha regla, bloqueando o permitiendo el tráfico a través del Firewall.

- **Control web:** supervisa las búsquedas web y la actividad de navegación en los dispositivos en los que el software está instalado, bloquea los sitios web y las descargas según las calificaciones de seguridad y el contenido.
- **Protección adaptable frente a amenazas (ATP):** analiza el contenido de los dispositivos en los que está instalado el software y decide cómo responder en función de la reputación de los archivos, las reglas y los umbrales de reputación establecidas.

Alcance

Se proporcionará al Cliente el Software asociado al presente módulo, así como las guías y procedimientos necesarios para la instalación del mismo. El software se entrega (AS-IT IS) conforme a lo descrito en los Términos y Condiciones (EULA)del propio fabricante. El software se proveerá empaquetado y pre-configurado.

Se ofrece bajo el modelo de Auto provisión, siendo el Cliente el responsable de su descarga, instalación y despliegue. No obstante, el Cliente que así lo necesite podrá solicitar el despliegue asistido por el equipo del SOC Pyme o solicitar soporte durante la instalación.

El despliegue asistido abordará la acción de instalar el software en los equipos del Cliente, de forma remota, en horario laboral 8x5 y siempre que esta instalación sea técnicamente posible de acuerdo con la política de uso razonable descrita a continuación.

Política de uso razonable

Conforme a lo estipulado, el presente servicio se presta en modelo de auto provisión siendo la responsabilidad del Cliente la instalación del software en todos los equipos, presentes o futuros, para los que ha contratado el servicio y siendo dicha responsabilidad no transferible de ningún modo a Telefónica.

No obstante, como valor adicional, el Cliente podrá solicitar un soporte al SOC Pyme para que le guíe en la instalación o incluso la instalación sea realizada de forma remota por este equipo, entendiéndose que dicha acción en ningún caso exime al Cliente de la responsabilidad contemplada arriba.

Este ofrecimiento de instalación asistida o remota está amparado por una política de uso razonable donde realizada la **primera intervención** remota/telefónica, el Cliente realizará de buena fe y bajo su responsabilidad las provisiones subsiguientes amparado por la documentación y guías proporcionadas por Telefónica.

En las situaciones adicionales, donde el Cliente por causas ajenas al software entregado, requiera nuevas instalaciones, Telefónica se reserva el derecho a valorar tanto la planificación como su propia realización.

Cualquier otra acción adicional solicitada por parte del Cliente, no expresamente definida en este contrato, Telefónica se reserva el derecho a no ejecutarla.

Condiciones de uso, requisitos y limitaciones

Para la instalación en caso de despliegue asistido por parte del SOC Pyme, el cliente deberá asegurar entre otras:

- Acceso Remoto al dispositivo.
- Permisos suficientes para la instalación de software.
- Sistema Operativo compatible y con el nivel de parcheado indicado por el fabricante.
- Autorización de acceso y despliegue.

Exclusiones

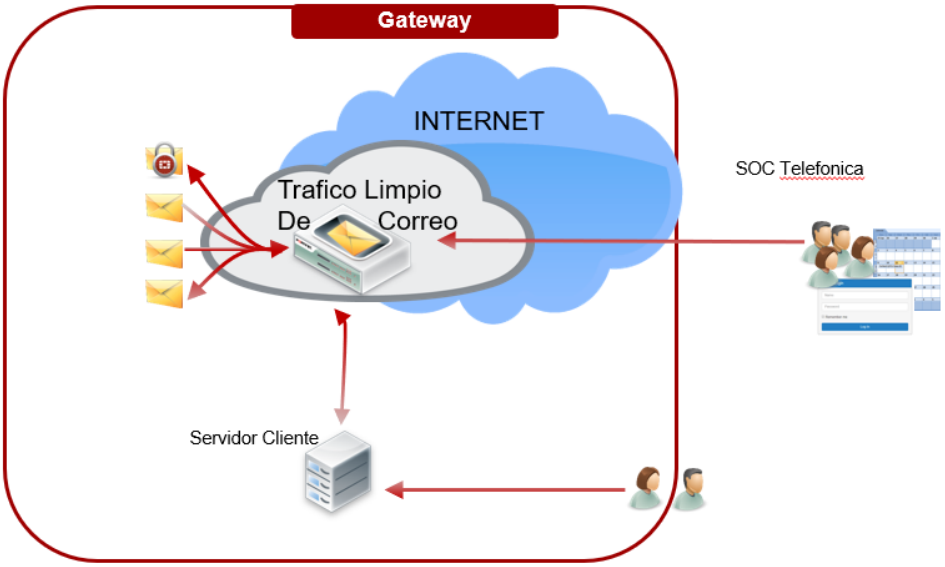
Queda excluida cualquier acción no definida en el alcance de la provisión, incluidas expresamente:

- La Instalación o atención in-situ.
- El despliegue en equipos no compatibles, no soportados o no licenciados.
- El despliegue en equipos que no sean propiedad del Cliente o cuya administración no esté delegada al Cliente.
- La desinstalación de software incompatible como otros antivirus.
- La instalación en equipos infectados. Cualquier manipulación de equipos informáticos fuera del software proporcionado.

1.3 Solución de Correo Limpio gestionado

Correo Limpio es un servicio cloud que ofrece una protección para el correo electrónico ante amenazas como el spam, malware y phishing. Bloquea los correos sospechosos dirigidos del Cliente, y permite el cumplimiento de las políticas establecidas para el uso apropiado del correo que el Cliente defina. Detecta virus, correo basura o contenido inapropiado y en estos casos impide que lleguen por el correo, deteniéndolos antes de que entren en los sistemas de la empresa. También puede interceptar correos salientes potencialmente peligrosos antes de ser distribuidos por Internet fuera de los sistemas de la empresa.

Este servicio de filtrado del correo es independiente de las plataformas de correo de las empresas y de fácil implantación, lo que permita a las empresas complementar sus servicios de correo actuales con facilidades de antivirus, antispam, filtrado de contenidos, sin la necesidad de hacer inversiones en tecnología, ni en su mantenimiento, ni tener avanzados conocimientos en dicha tecnología, ya que el servicio incluye la administración de la herramienta por parte del equipo del SOC Pyme.



Se implementa como una puerta o pasarela gateway entrante y saliente para el correo electrónico del cliente filtrándolo en busca de spam y malware antes de reenviarlo a su destino. El correo electrónico entrante al dominio protegido, cubierto por el Servicio, se

escaneará utilizando varios métodos de detección diferentes para determinar si se trata de correo electrónico no deseado, a través de filtros, como algunos los que se indican a continuación:

- Anti-Spam
- Anti-malware
- Métodos de filtrado por conexión con Listas blancas/negras, de reputación de IPs y otras listas.
- Validación de dominio remitente

Además la solución ofrece las siguiente funcionalidades adicionales:

- **Cuarentena**

  El servicio de Correo Limpio en nube analiza los correos con los mecanismos y tecnologías antes descritos y en función de los criterios que se tengan definidos en la herramienta, determina la acción a tomar. Si no detecta nada sospechoso o prohibido en el correo, lo envía al destinatario. En caso de detectar algún conflicto con las políticas definidas (por virus y spam) toma la acción establecida: borrar el mensaje, modificarlo añadiendo algún aviso o almacenarlo en lo que se ha llamado "cuarentena".

  La cuarentena permite albergar correos sospechosos o no válidos lejos de los servidores del Cliente por motivos de seguridad y para evitar saturar sus comunicaciones y sistemas con correo no deseado. La cuarentena permite (a las personas autorizadas para ello) revisar el mensaje de forma remota y así rescatar aquellos que puedan ser de interés para la empresa. Después de trascurrido el periodo de tiempo fijado durante la configuración del sistema, el sistema borrará aquellos mensajes que no han sido liberados (enviados al destinatario).

- **Continuidad de correo**

  Este servicio incluye además, una funcionalidad para procurar la continuidad del correo electrónico en caso de que temporalmente el servidor de correo electrónico del cliente se encuentre indisponible o no sea accesible. En estos casos, la plataforma de limpieza del correo en nube, "pone en cola" y retiene los correos electrónicos hasta que se pueda restablecer la conexión y entregarlos al servidor de correo.

Alcance

Tras la contratación del servicio, el dominio del Cliente será provisionado por Telefónica en la plataforma y se le comunicará la disponibilidad para su uso para el número de usuarios contratados.

A partir de ese momento el Cliente tendrá que redirigir su correo a la plataforma en nube cambiando los registros MX en el Servidor de Nombres de Dominio (DNS) para que apunten a ésta. El servidor de correo del Cliente debe ser configurado para aceptar solo correo que provenga de la plataforma en nube.

Del mismo modo, el Cliente también tendrá que enviar todo su correo de salida a la plataforma, para poder garantizar el correcto funcionamiento del servicio de correo, y que no se produzca, por ejemplo, un uso malintencionado del servidor de correo del Cliente.

Se proporcionará al Cliente unas guías y procedimientos para que pueda hacer la redirección del su correo a la plataforma en nube y asistencia o soporte en caso de tener que modificar elementos internos (servidor de correo y firewall propio si lo tuviera).

Condiciones de uso, requisitos y limitaciones

- El Cliente ha de tener contratado un servicio de correo electrónico. No se incluyen los buzones de correo en el servicio, sino una solución para eliminar virus y malware del mismo.
- Para la utilización de este servicio **el Cliente ha de tener un dominio propio**
- **El Cliente deberá contratar el servicio para todos los buzones de correo que tenga en el dominio que desea analizar con la plataforma.**
- La contratación de 1 usuario en un paquete otorga el disfrute del servicio de correo limpio para un único buzón en un único dominio. Dos buzones del mismo usuario en dominios distintos requerirían la contratación de buzones adicionales
- No se permite la utilización de la plataforma de Correo Limpio para el envío saliente de correos de dominios distintos al dominio protegido a través de la contratación del servicio.
- No está permitido el envío de correo masivo usando este servicio con el fin de evitar que el servicio de Correo Limpio pueda ser incluido en listas negras de spam.

Para mantener la integridad de la plataforma se establecen una serie de limitaciones técnicas al envío de correo saliente (con origen desde los servidores del Cliente final hacia la plataforma para ser distribuidos hacia internet).

El Cliente deberá configurar su servidor de correo con estos parámetros para un correcto funcionamiento del correo saliente a través del servicio.

Límite	Descripción	Valor
Número de conexiones simultaneas	Número de conexiones SMTP que una IP determinada puede abrir contra una máquina MTA del servicio. (por ejemplo, para enviar correo saliente). Sucesivas conexiones serán rechazadas.	5
Número de correos procesados inmediatamente por conexión	Número de correos por conexión que se procesan de inmediato. Los siguientes correos enviados en esa misma conexión se encolarán para su posterior procesado.	25

Limitaciones técnicas del servicio de correo

- En caso de falta de acceso al servidor de Correo desde la plataforma de Correo Limpio pon causas ajenas a Telefónica Empresas, ésta no será responsable de los daños causados por la imposibilidad de entrega de los correos a los Clientes ni de la posible eliminación de correos electrónicos que se produjera si la situación hace que se sobrepasen los siguientes límites para esta funcionalidad:
    c) una limitación de tiempo de hasta cinco (5) días de retención máximo a partir de la fecha de recepción; y
    d) una limitación de almacenamiento agregado de 200 GB de datos de correo electrónico.

Las presentes capacidades 200GB se refieren a la plataforma a escala global de todas las empresas que contraten el servicio y no solo dedicadas a un Cliente específico. Telefónica se reserva el derecho de modificar la capacidad de almacenamiento.

Los correos electrónicos que pudieran exceder estas limitaciones serán rechazados y pueden no ser recuperables. Los correos electrónicos almacenados en espera de entrega no serán accesibles.

La plataforma periódicamente hará intentos de envío hacia el servidor de correo del cliente.

- El Cliente será responsable de los daños causados como resultado de la acción tomada por el Cliente con respecto al correo electrónico no deseado ni de los daños causados por la eliminación de dichos correos electrónicos. Así también, si el Cliente elige liberar un correo electrónico infectado o señalado como potencialmente infectado por malware Telefónica Empresas no será responsable de los daños causados
  De manera general el sistema de filtrado se aplica a los correos que entran al dominio del Cliente, pero no a los correos enviados entre cuentas del mismo dominio a menos que el Cliente así lo configure en su servidor de correo. El servicio requiere para su correcto funcionamiento de una interfaz por IP pública a la que entregar el correo entrante, y de la que recibir correo saliente. No funcionará, por tanto, con servidores de correo finales que cuenten únicamente con direccionamiento privado.

Exclusiones

Quedan expresamente excluidas:

- La configuración de los servidores DNS del Cliente.
- Será responsabilidad del cliente realizar los cambios de configuración de los registros MX de su dominio de correo para empezar a disfrutar del servicio, una vez se le haya comunicado desde Telefónica la disponibilidad del mismo
- Cambios de configuración en los servidores de correo del Cliente y/o en firewalls propiedad del Cliente (para el establecimiento de reglas que permitan el tráfico de correo desde y hacia la plataforma de Correo Limpio)

  Para estas configuraciones el Cliente podrá solicitar soporte al SOC Pyme que le guiará en las tareas a realizar.

1.4 UTM Gestionado

Esta funcionalidad proporciona mediante el despliegue y configuración de un dispositivo Firewall de Nueva Generación, UTM, basado en una tecnología de un reconocido proveedor en el ámbito de la Gestión de Amenazas Unificadas en la sede del cliente, con la gestión en remoto del mismo por parte del equipo del SOC Pyme.

Esta plataforma servirá para crear una frontera o perímetro entre Internet y la red interna del Cliente, monitorizando los flujos de información entre ambas redes, pudiendo aplicar:

- Filtrado Antivirus.
- Protección frente ataques.
- Detección y control de aplicaciones.
- Control de navegación de usuarios internos.
- Protección antimalware.
- Visibilidad y obtención de informes
- Acceso Remoto Seguro (túneles): VPN (Site2Site o Portal VPN SSL).
- Balanceo de líneas: gestionando el que el tráfico para que entre por una de las 2 líneas Movistar

Mediante este dispositivo se protege la red de una empresa de las principales amenazas de seguridad permitiendo monitorizar, filtrar y aplicar políticas de seguridad a todo su tráfico (saliente y entrante) de internet. Además, se ofrece una mejora a Cliente al permitir la priorización de las aplicaciones de negocio sobre tráfico no productivo que pudieran estar utilizando sus empleados.

Gracias a este UTM el Cliente dispondrá de la funcionalidad de VPN para que el personal de su empresa pueda trabajar remotamente y con sus propios equipos desde cualquier lugar, navegando y accediendo de forma segura a las aplicaciones y archivos de su empresa.

Todo ello gestionado por expertos en seguridad desde el SOC Pyme, desde donde se ofrecerá al Cliente una atención personalizada.

Opciones contratables asociadas al UTM gestionado

En el momento de la contratación inicial de un paquete Avanzado es posible seleccionar una o las dos siguientes opciones:

- **Modelo superior de equipamiento**

  El equipamiento UTM se dimensiona en el momento de la contratación, en función del número de usuarios que se incluyen en el paquete, de la siguiente forma:

Rango de usuarios en la sede	Modelo correspondiente por defecto	Upgrade permitido
De 4 a 50 usuarios /sede	UTM1	UTM2
De 51 a 100 usuarios /sede	UTM2	UTM3
De 101 a 150 usuarios/sede	UTM3	UTM4
De 151 a 200 usuarios/sede	UTM4	No aplica

  Es posible contratar la opción de Upgrade, para que el modelo incluido en el servicio sea el inmediatamente superior.

- **Alta disponibilidad (HA)**

  Con la contratación de esta opción, se desplegarán 2 equipos del mismo modelo en la sede del Cliente para poder configurar la alta disponibilidad de este servicio.

En caso de seleccionar las dos opciones, se desplegarán 2 equipos UTM del modelo superior. No es posible tener dos modelos distintos.

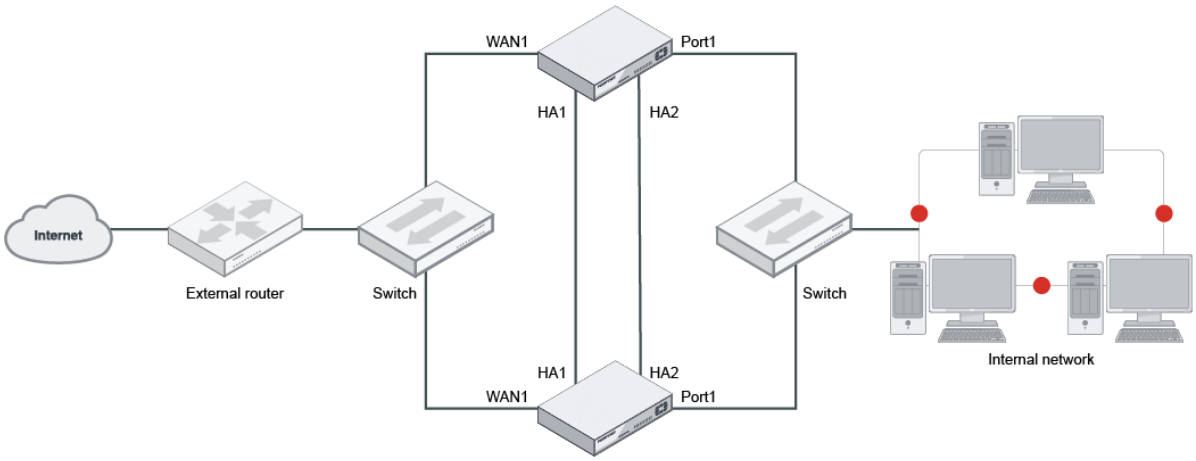
Modalidades de despliegue UTM

- **Simple**

El dispositivo se desplegará en la sede del Cliente funcionando como elemento de seguridad entre el acceso a internet y la red interna. Al estar montado un solo dispositivo se le considera un punto único de fallo.

- **Alta disponibilidad (HA)**

El Cliente puede elegir el despliegue en modo activo/pasivo de tal forma que en hipotético caso de que fallase uno de los dispositivos el otro continuaría prestando el servicio de protección a la sede.



Para poder desplegar el servicio en modo **HA es necesario la contratación de esta opción que incluye 2 dispositivos.**

Modalidades de despliegue en presencia de dos accesos a internet

- **Activo/Pasivo**

El UTM utilizará de manera primaria la línea definida de acceso a internet, y en caso de fallo enrutará el tráfico por el otro acceso a internet.

- **Balanceado**

El UTM utilizará de manera agregada cada una de las líneas de acceso a internet.

Alcance de la provisión

Se suministrarán al Cliente/Empresa los elementos mencionados más arriba. Este servicio aborda todas las tareas necesarias para la adquisición y entrega al Cliente del equipamiento contratado, así como los servicios profesionales necesarios para la instalación inicial de los mismos, cubriendo la configuración básica de los equipos (interfaces de red, direccionamiento, rutas) y la configuración necesaria para dejar operativos las funcionalidades del equipo.

Las tareas a realizar son:

- Envío e instalación del equipamiento a un destino del Cliente ubicado en España.
- Preconfiguración y conectividad por parte de Telefónica.
- Puesta en marcha en remoto de la plataforma. Esta puesta en marcha está basada en el modelo definido por el SOC Pyme y especificada en la **política de uso razonable** de este apartado.
- Aplicación de la configuración básica.
- Parametrización y ajuste de la plataforma según requisitos identificados con Cliente:
    - Servicio navegación.
    - Publicación de servicios.
    - Antivirus.
    - IPS (Intrusion Prevention System)
    - Filtrado web
    - Control de aplicaciones
    - AntiDOS
    - VPN Site to Site.

- VPN SSL (definición de portales, usuarios, redes que se instalan…).
- Pruebas.
- Paso a explotación.

Política de uso razonable para la provisión de UTM

La puesta en marcha está basada en la disponibilidad de una bolsa de provisión a consumir por parte del Cliente final, en concreto, veinticinco (25) puntos, teniendo en cuenta el esfuerzo identificado en la tabla siguiente. La configuración por defecto consumiría 16 puntos

FUNCIONALIDAD		COSTE	OBSERVACIONES
1 x VPN Site-to -Site		**3**	
1x Portal VPN SSL		**2**	Con autenticación de usuarios en Local
Integración LDAP/AD		**4**	El técnico asignado solicitará los datos concretos
Balanceo/backup de 2 líneas Movistar		**4**	
Activación DoS			
	Por Defecto	**1**	Sólo modo monitor
	Personalizado	**2**	Estudio de umbrales excluido
Control de aplicaciones			
	Por Defecto	**1**	Categorías fijas.
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
Filtrado web			
	Por Defecto	**1**	Categorías fijas.
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
IPS			
	Por Defecto	**1**	Perfil fijo. Protección workstations.
	Personalizado	**2**	Perfiles personalizados, servidores
Antivirus			
	Por Defecto	**1**	Modo flujo aplicado en salida.
	Personalizado	**2**	Modo Proxy
Creación Reglas Firewall			Las reglas por defecto para cada facilidad no se incluyen aquí
	Regla < 10 objetos	**1**	
	Regla > 10 objetos	**2**	
Solicitud funcionalidades complejas no contempladas		**4**	El técnico asignado solicitará los datos concretos

Condiciones de uso, requisitos y limitaciones

Para poder disfrutar del servicio el Cliente ha de disponer de línea de comunicaciones contratada con Movistar y con **direccionamiento IP público estático**.

Las comunicaciones soportadas son:

- **Fusión Digital:**
  - Router de Cliente gestionado por Telefónica.

- El servicio es incompatible con los siguientes escenarios de conectividad de Fusión Digital: con switches de 100 MBs. (en caso de darse esta situación el Cliente **deberá actualizar sus switches**)

- **FTTH Residencial/ADSL/VDSL:**
  Router gestionado por el propio Cliente. El Cliente debe cambiar la configuración de router a "monopuesto" para permitir acceso remoto del SOC Pyme al UTM.

Dado que en la contratación de los paquetes Avanzado y Premium **se dimensiona el modelo de dispositivo a desplegar** en la sede del Cliente en función del **número de usuarios contratados** en el paquete, podrían verse mermadas las prestaciones del servicio al Cliente en caso de que el número de usuarios que trabajen en dicha sede (utilicen la conectividad) sea superior al indicado.

Cualquier problema derivado de un incorrecto dimensionamiento por esta causa será responsabilidad exclusiva del Cliente.

Exclusiones

Quedan expresamente excluidos de la cobertura del suministro e Instalación del equipamiento UTM:

- Cualquier tipo de instalación eléctrica en el bastidor (rack) o ubicación donde se vaya a instalar el equipamiento contratado.
- Cableado de red fuera del bastidor (rack) donde físicamente se instale el equipamiento.
- Cables de red o alimentación adicionales a los que vengan incluidos en el propio equipamiento y que han sido suministrados por el fabricante.
- Los trabajos de migración de políticas desde otros dispositivos.
- Cualquier daño debido a fallos de la instalación eléctrica a la que se hallen conectados los equipos o s defectos originados por carecer el local donde se halle ubicado el material de las condiciones de entorno exigidas por el fabricante en las especificaciones técnicas de los equipos.
- El Cliente entiende y es consciente de que el lugar donde solicite a Telefónica la instalación ha de tener adecuadas las instalaciones tanto en conectividad, espacio y fuerza eléctrica. Además de tener preparadas las configuraciones o accesos a elementos de conectividad que así sea necesario.
  En caso de que durante la visita no pueda realizarse la instalación por causas ajenas a Telefónica, ésta podrá facturar al Cliente el desplazamiento del técnico.
- Las configuraciones asociadas directamente al router del Cliente, deberán ser realizadas por parte de éste siempre que sea posible (en conectividad de residencial) o con el soporte de Telefónica en caso de que dicha configuración en el equipo no sea accesible para el Cliente (servicios de Conectividad de Telefónica Empresas-1002)
- Cualquier tarea que no esté explícitamente descrita en la presente oferta.

Al realizar la instalación y configuración del Firewall UTM, por defecto, se desactiva el WiFi del router. Si el Cliente desea asegurar también el acceso Wi-Fi, debe adquirir AP/s (Punto/s de acceso) Wi-fi y conectarlo/s a su LAN para garantizar la supervisión de ésta mediante el firewall. Queda excluido del alcance de esta oferta, el suministro y configuración de APs Wi-fi.

1.5 Curso de Concienciación

Este curso es adecuado para cualquier tipo de empleados de empresas de los diferentes sectores que utilicen para su trabajo medios electrónicos (ordenador y correo). Se aborda de una forma amena y práctica los conceptos básicos en materia de seguridad de la información para mantener una buena primera línea de defensa en las organizaciones.

Impacto

Al finalizar el curso, los alumnos sabrán:

- Principios y conceptos básicos en ciberseguridad y su importancia en entornos de trabajo.
- Tipos de amenazas y su impacto en las organizaciones
- Políticas internas en materia de seguridad de la información.
- Legislación, reglamentación y tratamiento de la información y sus implicaciones.
- Uso básico en ciberseguridad del equipamiento corporativo.
- Gestión de incidentes y sus consecuencias.

Temario

- Introducción
- Conceptos básicos y responsabilidad de las personas
- La información y su tratamiento
- Uso aceptable de equipamiento
- Phishing
- Malware
- Gestión de Incidencias y referencias
- Buenas prácticas en seguridad de la información

Este temario podrá sufrir modificaciones, en función de la evolución de la ciberseguridad de las pymes, sus conocimientos o los cambios que puedan producirse en el servicio.

Duración y certificación

El curso tiene una duración aproximada de 2 horas.

Al finalizar el itinerario, el alumno realizará un test que le permite obtener un diploma (propio de la plataforma).

Esta duración tiene relación directa con el temario actual. En caso de que se modifique el temario, la duración del curso es susceptible de ser modificada.

1.6 Solución CASB gestionado

Un agente de seguridad de acceso a la nube, o CASB, es un software alojado en la nube o un software o hardware local que actúa como intermediario entre los usuarios y los proveedores de servicios en la nube. La capacidad de un CASB para resolver las deficiencias de seguridad se extiende a los entornos de software como servicio (también llamado SaaS), plataforma como servicio (también llamado PaaS) e infraestructura como servicio (también llamada IaaS). Además de proporcionar visibilidad, un CASB también permite a las organizaciones ampliar el alcance de sus políticas de seguridad desde su infraestructura local existente a la nube y crear nuevas políticas para el contexto específico de la nube.

Los CASB se han convertido en una parte vital de la seguridad empresarial, permitiendo a las empresas utilizar la nube de forma segura mientras protegen los datos corporativos sensibles.

El CASB sirve como centro de aplicación de políticas, consolidando múltiples tipos de aplicación de políticas de seguridad y aplicándolas a todo lo que su empresa utiliza en la nube, independientemente del tipo de dispositivo que intente acceder a ella.

Con el aumento de la movilidad de la plantilla, el incremento de uso de los dispositivos propios de los empleados en actividades laborales y la presencia del uso no autorizado de la nube por parte de los empleados, la capacidad de supervisar y gobernar el uso de aplicaciones en la nube como Microsoft Office 365 se ha convertido en algo esencial para el objetivo de la seguridad empresarial. En lugar de prohibir totalmente los servicios en la nube y afectar potencialmente a la productividad de los empleados, un CASB permite a las empresas adoptar un enfoque granular para la protección de datos y la aplicación de políticas, lo que hace posible utilizar de forma segura servicios en la nube que ahorran tiempo, mejoran la productividad y son rentables.

El servicio CASB ayuda a prevenir la fuga de datos confidenciales a través de las soluciones de compartición incluidas en el licenciamiento E3 de Microsoft.

Alcance

Telefónica proporcionará al Cliente la configuración necesaria para dejar el servicio CASB totalmente operativo en las aplicaciones SAAS del Cliente incluidas dentro del presente servicio:

- Mail 365
- Microsoft Teams
- Microsoft Sharepoint
- Microsoft OneDrive

Una vez Telefónica disponga de dichas credenciales de administrador global (Global Admin) del Cliente, el SOC Pyme comenzará a operar el servicio de CASB del Cliente sobre las aplicaciones arriba indicadas, siendo la operativa transparente para el Cliente.

Al ser un servicio administrado por el SOC Pyme, ningún usuario del Cliente tendrá acceso a ningún tipo de consola de gestión del servicio CASB.

Condiciones de uso, requisitos y limitaciones

Será totalmente necesario que la empresa disponga de:

- Licencias contratadas y desplegadas de Microsoft 365 E3 para que Telefónica pueda operar el servicio de CASB sobre el mismo.
- Una cuenta o credencial de administrador (con privilegios de Global Admin) del aplicativo que se quiera monitorizar de Microsoft (Las aplicaciones Mail 365, Teams, Sharepoint y/o OneDrive) y lo proporcione a Telefónica para que ésta pueda dar de alta el servicio de CASB en la nube de los aplicativos incluidos bajo este servicio.

Exclusiones

- Queda expresamente excluido de este contrato: El propio suministro de las aplicaciones mencionadas de Microsoft (365 E3, Mail 365, Sharepoint, OneDrive o Teams)
- Queda excluida cualquier configuración de las aplicaciones de Microsoft (365 E3 o E5, Mail 365, Sharepoint, OneDrive o Teams)

1.7 Operación del SOC Pyme

Telefónica prestará desde el SOC Pyme el servicio de soporte, mantenimiento y administración delegada de todos los productos contratados por el Cliente en este paquete Avanzado.

El registro de peticiones, incidencias y consultas puede realizarse en cualquier momento y en cualquier día de la semana, a través de los canales de atención puestos a disposición del cliente y conforme a las características descritas en el Anexo II Atención al Cliente.

Alcance

El servicio de TU EMPRESA SEGURA incluye la operación en remoto por parte del SOC pyme del software del seguridad proporcionado y desplegado en los equipos del Cliente o en las plataformas en nube con el siguiente alcance:

- **Participación en incidentes de seguridad.** El SOC Pyme participará en el descubrimiento de los orígenes y mitigación dentro del alcance de la visión que le proporciona los equipos/software administrados de los incidentes de seguridad, no siendo en ningún caso el responsable de coordinar la gestión ni la respuesta ante dichos incidentes.

- **Participación en la resolución de Incidencias.** El SOC Pyme colaborará en la revisión de la configuración y eventos de los equipos que administra para ayudar al Cliente a solventar caídas en servicios críticos de sus procesos de negocio, sean de origen en la planta administrada por Telefónica o por el Cliente. En el caso de que el origen del problema sea por un *Sistema Monitorizado,* el SOC Pyme activará todos los mecanismos de resolución dentro de las limitaciones de los productos y sistemas desplegados con la finalidad de solventar o mitigar el problema.
- **Resolución de solicitudes**. Contempla la realización de las tareas de operación solicitadas por el Cliente y tipificadas dentro del servicio.
  Se entiende como tareas tipificadas, las siguientes, clasificadas en dos tipos:
  5) Incidencias: fallos o mal funcionamiento dentro de los servicios
  6) Peticiones: solicitudes que realiza el Cliente sobre la configuración del servicio. Algunos ejemplos:
     i. Ayuda en la puesta en marcha
     j. Configuraciones respecto a listas negras y listas blancas del correo electrónico
     k. Configuraciones respecto a listas negras y listas blancas de dominios y urls
     l. Apertura de puertos
     m. Gestión de usuarios de la VPN

- **Identificación proactiva de riesgos**. Se informará de forma proactiva al Cliente si en el ejercicio de las funciones los administradores detectaran riesgos evidentes para la seguridad.

  Las herramientas de las soluciones desplegadas generarán alertas o indicadores de seguridad que serán revisados por el SOC Pyme bajo los criterios de seguridad y determinando si son susceptible de una actuación bien manual bien automatizada. Estará circunscrito a las únicamente al número de dispositivos/herramientas/ capacidades contratadas y siempre que éstas estén adecuadamente desplegadas conforme los criterios identificados anteriormente.

- **Corrección de vulnerabilidades identificadas en el software suministrado**. El servicio participará en la realización de los cambios necesarios para subsanar vulnerabilidades encontradas en el software suministrado.
- **Registro y control de las peticiones del servicio**. El Cliente podrá hacer una petición por cualquiera de las vías puestas a su disposición para esto y se recogerán en el portal web del servicio Tu Empresa Segura (Ver Anexo II de Atención al Cliente)

- **Mantenimiento y soporte de los equipos UTM**
  En lo referente a las tareas de mantenimiento relacionadas con el dispositivo o dispositivos UTM, Telefónica Empresas prestará el servicio de mantenimiento remoto encaminado a solucionar las situaciones en las que el dispositivo UTM muestre una indisponibilidad. En el caso de que se determine una avería en alguno de los componentes del dispositivo, Telefónica Empresas gestionará la sustitución de la pieza o el equipo completo (RMA) según la situación y el contrato suscrito con el fabricante.
  Una vez se ha diagnosticado la avería según los requisitos que el fabricante establece en sus condiciones de activación de RMAs (en base a los tiempos establecidos en el contrato del equipamiento con el fabricante), se realizará la gestión para la entrega del equipo al cliente, restaurando la última configuración operativa del dispositivo.
- **Comunicaciones/informes:** Recopilación de información y puesta a disposición del Cliente de informes en el portal.
- **Actualizaciones y parches**: Puesta al día de los servicios mediante actualizaciones y parches que se vayan generando los fabricantes/proveedores de los servicios.

Condiciones de uso, requisitos y limitaciones

- La comunicación con el equipo SOC Pyme deberá realizarse de la forma descrita y en el horario y SLOs descrito en el Anexo II Atención al Cliente.
- Sólo se permitirá la existencia de 1 usuario autorizado (el Contacto Técnico) por sede para solicitar tareas (peticiones/consultas o incidencias) al SOC Pyme.
- Los equipos gestionados deberán tener conectividad con la plataforma de gestión, para poder ser gestionados y reportar cualquier incidente que pudiera suceder. En caso de que no tengan conectividad está información no podrá ser tratada ni las políticas aplicadas, la plataforma intentará en la medida de lo técnicamente posible la configuración y recopilación de eventos cuando el dispositivo posea nuevamente conectividad.
- Al ser un Servicio administrado por el SOC Pyme, el Cliente no contará con permisos de administrador sobre ninguna de las consolas de gestión de las herramientas incluidas (Antivirus gestionado, Correo Limpio gestionado, ni UTM gestionado).
- El equipo del SOC Pyme podrá actualizar las políticas /reglas /bases de datos / configuraciones de seguridad con el fin de incrementar o mejorar la seguridad, estabilidad o rendimiento en el Cliente siempre que esta actuación no produzca interrupción al mismo
- En caso de actuación proactiva será siempre realizada con los criterios máximos de prudencia, con el fin de no interferir en la actividad del Cliente, de manera general, en caso de existir dudas específicas sobre la aplicabilidad de una política el equipo podrá contactar al Cliente para pedirle autorización. Siendo en este caso responsabilidad exclusiva del Cliente la actuación indicada.
- Cualquier acción proactiva de configuración o adecuación de las políticas o elementos de las plataformas podrá ser aplicadas por el equipo de soporte aún en ausencia de eventos de seguridad, y especialmente en caso de que exista una amenaza que pudiese ser masiva.
- En caso de un incidente dentro del alcance de Sistemas Monitorizados el SOC Pyme podrá solicitar pruebas, ejecutables, y evidencias que ayuden a la investigación y la determinación del mismo. El SOC Pyme se reserva el derecho de compartir dichas muestras con sus empresas partner y asociados siempre con el objetivo de incrementar el nivel de protección de los clientes. El Cliente será libre de proporcionar dicha información siempre que lo considere y entiende que, negándose a proporcionarla, la protección/investigación podrá verse gravemente mermada o ser del todo inefectiva
- El Cliente entiende y acepta que el equipo de seguridad es incapaz de actuar o mitigar cualquier ataque sobre un sistema que no esté siendo monitorizado

Política de uso razonable para la operación del equipamiento UTM

El servicio de administración delegada del SOC Pyme se basa en la disponibilidad de una bolsa de gestión a consumir por parte del Cliente, en concreto, cinco (5) puntos mensuales, teniendo en cuenta el siguiente esfuerzo por tipo de solicitud:

FUNCIONALIDAD		COSTE	OBSERVACIONES
1 x VPN Site-to -Site		**3**	
1x Portal VPN SSL		**2**	Con autenticación de usuarios en Local
Integración LDAP/AD		**4**	El técnico asignado solicitará los datos concretos
Balanceo/backup de 2 líneas Movistar		**4**	
Activación DoS			
	Por Defecto	**1**	Sólo modo monitor
	Personalizado	**2**	Estudio de umbrales excluido
Control de aplicaciones			
	Por Defecto	**1**	Categorías fijas
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
Filtrado web			
	Por Defecto	**1**	Categorías fijas
	Personalizado	**2**	Categorías personalizadas, lista negra, overrides
IPS			
	Por Defecto	**1**	Perfil fijo. Protección workstations.
	Personalizado	**2**	Perfiles personalizados, servidores
Antivirus			
	Por Defecto	**1**	Modo flujo aplicado en salida.
	Personalizado	**2**	Modo Proxy
Creación Reglas Firewall			Las reglas por defecto para cada facilidad no se incluyen aquí
	Regla < 10 objetos	**1**	
	Regla > 10 objetos	**2**	
Solicitud funcionalidades complejas no contempladas		**4**	El técnico asignado solicitará los datos concretos

El Cliente entiende y acepta que no podrá excederse del número de puntos indicados y que no puede excederse más de 1 mes del número de puntos disponibles.

A continuación, se indican unas métricas que Telefónica considera un uso razonable de los esfuerzos de servicios profesionales que sustentan la operativa del servicio.

Métricas por actividad, cantidad y periodicidad:

Actividad	Cantidad	Periodicidad
Resolución incidencias de negocio	Todas con afectación de servicio	Continua
Resolución incidencias de seguridad	Todas	Continua
Resolución solicitudes	5 puntos mensuales	Contrato
Registro y Control peticiones de servicio	Todas	Continua

Exclusiones

QUEDA EXPRESAMENTE EXCLUIDO DEL SERVICIO DE **TU EMPRESA SEGURA** CUALQUIER ACTIVIDAD o SOPORTE SOBRE EQUIPOS/HERRAMIENTAS QUE NO SE ENCUENTREN INCLUIDOS EN EL MARCO DE ESTE SERVICIO Y QUE NO SE ENCUENTRE RECOGIDO EN LAS PRESENTES CONDICIONES PARTICULARES Y ANEXOS.

ANEXO VIII: MÓDULOS ADICIONALES

1. FIRMA DIGITAL

Firma Digital es una avanzada plataforma en nube que permite la firma de documentos electrónicos en PDF mediante:

- **Firma Manuscrita biométrica**: Consiste en plasmar la rúbrica como se haría tradicionalmente en cualquier documento, solo que esta es recogida mediante medios electrónicos, recogiéndose además del grafo información como presión, cadencia y longitud de trazos.
- **Firma con OTP** enviada por mail. Uso de una contraseña de un solo uso (One Time Password, OTP) que se envía por mail para la firma de documentos

Las acciones que pueden realizar son aquellas que se pueden asociar a las personas que participan en un flujo de firma durante el momento de su creación.

- **Firmar**: Las personas que estén definidas como firmantes serán las que están obligadas a firmar el documento o rechazarlo, quedará registro explícito de su firma, así como los registros probatorios asociados al tipo de firma empleado.
- **Revisar:** Esta acción está asociada a las personas que han de revisar el documento y validarlo con un Aceptar o no aceptar, este proceso no deja evidencia directa visible en el documento (no se inserta un grafo) pero queda registrado a nivel de la plataforma del servicio.
- *Informar*: Son aquellas personas que han de estar informadas de ese flujo de firma llegándoles la notificación cuando se indique en el flujo.

Adicionalmente todos los implicados una vez finalizado el proceso de firma serán informados de su finalización y recibirán las copias de documentación completa.
El flujo de firma incluye los siguientes puntos:

- Tipo de firma que se desee utilizar (biométrica o por OTP enviado por mail)
- Personas que están involucradas en el proceso de firma.
- Acción que realizaran las personas involucradas: firmar, revisar o informar.
- Orden en el que han de producirse la firmas (Secuencial o paralelo).
- Documentación para firmar.
- Anexos que no se firmaran, pero forman parte del proceso.

Telefónica empresas proporcionará al Cliente final la configuración necesaria en la plataforma en nube para con el/los paquete/s de firmas contratado/s en el servicio, así como las guías y procedimientos necesarios para la activación de este.
Los datos de acceso al servicio se proporcionarán únicamente al usuario que ha sido identificado en el contrato principal como Contacto Técnico.

Alcance

Telefónica proporcionará al Cliente:

- Acceso a la plataforma de firma en nube para el usuario designado como Contacto Técnico en el momento de la contratación del paquete de Servicio, así como las guías y procedimientos necesarios para la activación de este.
- Con cada unidad de este módulo contratado se pondrá a disposición del Cliente una bolsa de 250 firmas al año.

Cada Cliente final podrá tener acceso a una cuenta propia y personal para gestionar la firma.

Será en todo caso responsabilidad del Cliente final (el Contacto el invitar, añadir o gestionar los usuarios que tengan que hacer uso de la solución de firma.

Condiciones de uso, requisitos y limitaciones

Los navegadores soportados son: (puede funcionar en versiones inferiores, pero no se asegura soporte)

- Microsoft Edge: versión 17 en adelante
- Microsoft Internet Explorer: versión 11 en adelante
- Google Chrome: versión 70 en adelante
- Mozilla Firefox: versión 55 en adelante (ídem con Chrome)
- Opera: versión 59 en adelante.
- Safari

Dispositivos Móviles:

- Android (App SealSign SaaS): Requiere Android 5.1 o superior
- IOS (App SealSign SaaS): Requiere IOS 8.0 o superior

Tipos de documentos que se pueden firmar: PDF. Otros formatos deben convertirse previamente a este formato antes de poder firmarse.

La contratación de este módulo se debe realizar conforme a la previsión del Cliente del número de firmas que necesita hacer en un año y por tanto el número de unidades de este módulo que necesita contratar. Finalizados los 12 meses desde la contratación inicial, el número de firmas se reiniciará de nuevo de acuerdo con el número de unidades que el Cliente tenga contratadas en dicho momento (250 firmas*número de unidades contratadas).

El Cliente no puede cursar baja en este módulo adicional y volverlo a contratar en un intervalo inferior a 12 meses desde la contratación inicial.

Si se detecta un uso abusivo de esta herramienta, Telefónica podría dar de baja al Cliente en el SERVICIO.

Exclusiones

- El Cliente final entiende y acepta que el servicio no es un repositorio documental, y por lo tanto no cuenta con una garantía de ningún tipo en cuanto al almacenamiento, y acepta expresamente que expirado el contrato o cancelado el contrato dejarán de estar disponibles los documentos.

- Telefónica bajo ninguna circunstancia será responsable de cualquier gestión de usuarios del cliente final, y el cliente final deberá usar las herramientas a su alcance dentro del interface para cualquier gestión incluida la gestión de cuentas.

- El cliente final será en todo caso responsable de la gestión de; los documentos, los firmantes, los esquemas de firma, el almacenamiento y conservación de la información, no siendo responsable Telefónica en ninguna de estas situaciones.

- El cliente final acepta y entiende que en ningún caso y en ninguna circunstancia Telefónica es responsable de verificar la validez de las firmas, validar la identidad de los firmantes ni de asegurar la corrección de los documentos, y queda completamente indemne de cualquier perjuicio que pudiese causar a la firma de un contrato incluido el lucro cesante.

2. BUZONES ADICIONALES DE CORREO LIMPIO

Si el cliente final lo desea, se podrán contratar licencias de uso adicionales de Correo Limpio de manera individual que se asociarán al paquete de servicio que tenga contratado.

Todas las condiciones de uso, requisitos, limitaciones y exclusiones son los ya indicados para el módulo de Correo Limpio del Anexo correspondiente al paquete contratado (Anexo IV Modalidad Paquete Básico, IV Modalidad Paquete Avanzado o Anexo IV Modalidad Paquete Premium)

3. PUESTA EN MARCHA

El servicio de Tu Empresa Segura proporciona acceso, a través del portal del servicio, a unos manuales con instrucciones detalladas para la instalación inicial de todos los componentes. Asimismo facilita, de ser necesario, ayuda y soporte en remoto para dicha instalación y configuración inicial. El acceso a este soporte se realiza a través de los cauces habituales: vía ticket, chat o por correo electrónico.

De manera opcional, el cliente puede contratar también que la instalación y puesta en marcha inicial del paquete contratado (Básico, Avanzado o Premium) se haga de manera parcial o total por parte del SOC pyme de Telefónica.

La contratación de 1 unidad del módulo adicional de “Puesta en Marcha” incluye:

- Para los clientes del paquete **Básico**:
  - Configuración del Correo Limpio
  - Instalación remota de **hasta 5 aplicaciones** de Antivirus/anti-ransomware y Navegación Segura
  - Recorrido por el portal en donde se explica y describen los beneficios del producto, la visualización de los informes y como contactar con el SOC Pyme para reportar incidencias o consultas.

- Para los clientes del paquete **Avanzado y Premium**:
  - Configuración de Correo Limpio
  - Instalación remota de hasta 5 aplicaciones de las incluidas en estos paquetes:
    - Aplicación Antivirus/anti-ransomware y Navegación Segura
    - **Aplicación VPN**.

    El cliente puede elegir de las 5 instalaciones contratadas cuántas quiere de cada aplicación (Antivirus/antiransomware y Navegación o VPN) y en qué dispositivos.

- Recorrido por el portal en donde se explica y describen los beneficios del producto, la visualización de los informes y como contactar con el SOC Pyme para reportar incidencias o consultas.

Una vez contratado el módulo adicional, Telefónica contactará (por teléfono) con el responsable técnico proporcionado por el cliente durante la contratación del servicio para acordar y coordinar las tareas.

El cliente también podrá iniciar la solicitud de inicio de las tareas de puesta en marcha desde el portal del servicio, mediante un ticket con esta petición.

El plazo máximo para solicitar la realización de esta puesta en marcha o para agendar la fecha con Telefónica es de 3 meses desde la contratación del módulo adicional.

Si durante la llamada inicial de Puesta en Marcha no se instalasen las 5 aplicaciones, el cliente podrá llamar para solicitar la instalación de las aplicaciones restantes durante los próximos 3 meses.

El cliente puede contratar tantas unidades de este módulo adicional como necesite.

Nota: Para la realización de estas tareas, es necesario el uso un software de acceso remoto que permita al SOC pyme acceder momentáneamente a los dispositivos del cliente en los que se vaya a realizar la instalación de la aplicación.
El SOC pyme puede utilizar el software del que disponga el cliente en su empresa para este propósito o, en caso de no tenerlo, Telefónica lo proporcionará de forma temporal hasta finalizar esta tarea.

4. VISITA

En las modalidades Avanzada y Premium del servicio, está incluido el suministro y la instalación inicial del equipo firewall UTM, en el domicilio que el cliente ha indicado en el momento de la contratación por parte de un técnico que se desplaza el día acordado.

Una vez conectado e instalado, el equipo del SOC pyme toma control del equipo en remoto y realiza de esta forma todas las configuraciones y tareas de soporte que se incluyen en el servicio.

No está contemplado en el alcance del servicio ningún desplazamiento adicional de un técnico a casa del cliente a excepción de los que tuvieran que hacerse por un fallo en el mismo debido a causas incluidas en la garantía del fabricante.

En caso de que el SOC pyme no pueda acceder al equipo en remoto por desconexión del equipo, se le dará en remoto soporte de cómo volver a conectarlo y que así el SOC pymes pueda de nuevo tomar el control.

Opcionalmente, si el cliente requiera la presencia de un técnico en sus dependencias para reconectar el equipo firewall y/o revisar la configuración in-situ, podrá contratarse esta actuación con el siguiente alcance:

- Desplazamiento de un técnico a la sede del cliente con una duración máxima de 2 horas de actuación en 8x5xNBD* para:
  - La instalación básica del equipamiento:
    - Fijar el equipo sobre un rack existente o desmontarlo si fuese necesario un cambio. (Instalación del mismo a menos de 3 metros de altura en entorno oficina)
    - Conectar la alimentación sobre una base de enchufes existente en el mismo rack.

- Realizar el parcheo entre equipos o equipo-panel. Todos los elementos han de estar presentes en el mismo rack.
- Instalar, desinstalar, dar acceso remoto, instalar o modificar cableado.

Nota: *NBD: Next Business Day (siguiente día laborable).

- Conectarse en local al equipo a través del puerto consola.
- Proporcionar acceso remoto al ingeniero de soporte de Telefónica para que pueda realizar la configuración / troubleshooting del equipo.

Quedan excluidos en la contratación de este módulo:

- El suministro de latiguillos de ningún tipo.
- El suministro de cable de alimentación.
- El suministro, en general, de ningún elemento.
- El suministro de cableado de ningún tipo.

5. PROTECCIÓN DE LA IDENTIDAD

Este módulo adicional ofrece un servicio de detección de filtraciones de datos que forman parte de la identidad de la empresa en la Dark Web (web Oscura) y que pueden posteriormente ser utilizados por ciberdelincuentes para realizar ataques a la misma.
En concreto se monitorizará la aparición de alguno de siguientes datos de la compañía:

- **Nombre de la empresa** que realiza la contratación del servicio y de la línea de conectividad asociada.
- **CIF/NIF** bajo el que se realiza la contratación del servicio y de la línea Fusión o BAF asociada.
- **Dirección postal de las sedes** de la empresa que tengan contratado el servicio Tu Empresa Segura (no sólo la sede que tenga asociado en el contrato el Addon) y las línea de conectividad asociadas.
- Por defecto, se incorporarán **los Teléfonos** proporcionados como contactos para la prestación del servicio Tu Empresa Segura (contacto técnico y contacto comercial).
- **Dominio/s de Correo electrónico** proporcionado para la prestación del servicio Tu Empresa Segura (para la funcionalidad de Correo Limpio). No es posible monitorizar un dominio no provisionado anteriormente en el servicio de Tu Empresa segura en la funcionalidad de protección del correo.
- Por defecto, se monitorizará la **IP de la empresa** correspondiente con la sede en la que se realiza la contratación del addon de protección de la identidad, así como las IPs de otras sedes en las que el cliente también haya contratado un paquete del servicio Tu Empresa Segura.

Esta detección se realiza en tiempo real, a partir de los datos de identificación proporcionados por la empresa, o bien durante la contratación del servicio Tu Empresa Segura o bien en modificaciones posteriores solicitadas al SOC por los canales de soporte.
Tras la contratación de este módulo adicional, se enviará un correo de bienvenida al contacto técnico identificado por el cliente como interlocutor único para el servicio Tu Empresa Segura.

Con la configuración inicial, el servicio comenzará una búsqueda inmediata de las posibles brechas y en caso de detectar alguna se comunicará vía correo electrónico al contacto técnico y se le informará de la misma, así como la recomendación de los pasos a seguir para resolverlo.

A partir de ese momento, el sistema monitorizará de manera continua los datos de identificación incluidos en la configuración del módulo para notificar posibles fugas al correo electrónico del contacto técnico del cliente.

ANEXO IX GLOSARIO

- **Addon:** Módulo contratable de manera adicional sobre el paquete base que representa el componente obligatorio del SERVICIO.
- **APs:** Access Point o punto de acceso, es un dispositivo para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas.
- **Balanceo de tráfico:** Dentro del servicio UTM Gestionado, se permite el balanceo entre dos líneas, siempre que estas sean Movistar y que, al menos una de las conectividades, disponga de IP pública estática.
- **Blacklist:** Lista negra. Es una lista o registro de correos electrónicos, dominios, URLs, que el cliente no quiere permitir, es decir, quiere bloquear, tanto a nivel de acceso como de navegación.
- **CASB:** es un software alojado en la nube o un software o hardware local que actúa como intermediario entre los usuarios y los proveedores de servicios en la nube.
- **Cuarentena:** dentro del servicio de Correo Limpio, la cuarentena es un depósito seguro para aquellos archivos detectados que puedan ser dañinos. Los elementos en cuarentena no se pueden propagar ni pueden dañar el equipo.
- **Dark Web:** Se denomina Web Oscura al contenido que se encuentra en Internet oculto para los motores de búsqueda habituales (contenido no indexado) y que sólo es accesible mediante un navegador especial. Se utiliza para mantener la actividad de Internet privada y en el anonimato y en muchos casos para actividades ilegales como, por ejemplo, la compraventa de datos de empresas y particulares con fines delictivos.
- **DNS:** Sistema de nombres de dominio, es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
- **Firewall:** también llamado cortafuegos, es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **Flujo (Modo Flujo):** Dentro del servicio UTM Gestionado, el modo Flow hace referencia al modo de inspección por defecto y el más rápido, manteniendo intacta la sesión TCP (Transmission Control Protocol) de cliente a servidor.
- **Gateway:** puerta de enlace o pasarela, es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, acceder a otra red. En otras palabras, sirve de enlace entre dos redes con protocolos y arquitecturas diferentes.
- **Global Admin:** Administrador global que tiene acceso a la mayoría de las características o funcionalidades del servicio.
- **HA:** Alta disponibilidad. Dentro del servicio UTM Gestionado, el Cliente puede elegir el despliegue en modo activo/pasivo de tal forma que en hipotético caso de que fallase uno de los dispositivos el otro continuaría prestando el servicio de redundancia a la sede.
- **IaaS:** Infraestructura como servicio
- **IP:** Dirección IP es el número que identifica a cada dispositivo dentro de una red.
- **IPS:** Prevención de intrusiones y ataques más perjudiciales, en el perímetro de la red, actuando en caso necesario.
- **Mail O365:** es un servidor de correo compartido de la empresa Microsoft, dentro del paquete Microsoft Office.

- **Máquina MTA:** Agente de transferencia de correo, que transfiere los mensajes de correo electrónico entre máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final.
- **Malware:** cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada (al contrario que el «software defectuoso») y sin el conocimiento del usuario (al contrario que el software potencialmente no deseado).
- **MX:** Un registro MX es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en internet. Los registros MX apuntan a los servidores a los cuales envían un correo electrónico, y a cuál de ellos debería ser enviado en primer lugar, por prioridad.
- **O365:** es un conjunto de programas informáticos de la empresa Microsoft.
- **Onedrive (Microsoft Onedrive):** es un servicio de alojamiento de archivos de Microsoft.
- **Overrides:** Dentro del servicio UTM Gestionado, hace referencia a las nuevas categorías personalizadas añadidas por parte del Cliente.
- **PaaS:** Plataforma en la que un proveedor de servicios ofrece acceso a un entorno basado en cloud en el cual los usuarios pueden crear y distribuir aplicaciones.
- **Parche:** se refiere a los distintos cambios que se han aplicado a un programa para corregir errores, actualizarlo, eliminar secciones antiguas de software o simplemente añadirle funcionalidad, por parte de los proveedores o fabricantes asociados a este servicio.
- **Partners:** Proveedores asociados al servicio.
- **Phishing:** es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).
- **Proxy (Modo Proxy):** dentro del servicio UTM Gestionado, hace referencia a un modo de inspección, en el cual se rompe la conexión TCP ((Transmission Control Protocol) en dos partes, permitiendo realizar full buffering (habilitando ciertas
- **Rack:** Bastidor. Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- **Reporting:** Informes definidos con información y detalle del servicio y, concretamente, de los servicios incluidos en la Modalidad contratada.
- **RMA** (Return Merchandise Authorization): Una autorización de devolución de mercancía, conocido por las siglas inglesas RMA o RGA se usa en distribuidores o corporaciones como parte del proceso de devolución de un producto para recibir un reembolso, reemplazo o reparación durante el período de garantía del producto.
- **SaaS:** Software como un Servicio, abreviado ScuS (del inglés: Software as a Service, SaaS), es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente.
- **Servicio Cloud:** Es una categoría de servicios Cloud que proporciona una plataforma y un entorno que permiten a los desarrolladores crear aplicaciones y servicios que funcionen a través de internet. El software se aloja en la nube y las empresas acceder a él a través de su navegador web.
- **Sharepoint:** Microsoft Sharepoint es una plataforma de colaboración empresarial, formada por productos y elementos de software que incluye, entre una selección cada vez mayor de componentes, funciones de colaboración, basado en el navegador web, módulos de administración de procesos, módulos de búsqueda y una plataforma de administración de documentos (gestión documental).

- **SMTP:** (Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo) es un protocolo de comunicación que permite el envío de correos electrónicos en internet.
- **SO:** Sistema operativo
- **SOC (Security Operations Center).** El Centro de Operaciones de Seguridad de Telefónica es un área dedicada al mantenimiento, soporte y administración del equipamiento de seguridad de los Clientes de Telefónica. Está formado por un grupo de expertos en las distintas tecnologías de Seguridad de los principales fabricantes del mercado.
- **SOC Pyme**: Es un grupo de expertos del SOC dedicados específicamente al segmento pyme y a las necesidades de seguridad de las empresas de este segmento.
- **Spam:** también llamado correo basura, correo no deseado o correo no solicitado, hace referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- **Switch:** o conmutador es el dispositivo digital lógico de interconexión de equipos dentro de una misma red. Constituyen las redes de área local o LAN.
- **Teams (Microsoft Teams):** es una plataforma unificada de comunicación y colaboración que combina chat persistente en el lugar de trabajo, reuniones de video, almacenamiento de archivos e integración de aplicaciones.
- **Túneles:** Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro creando un túnel de información dentro de una red de computadoras.
- **URL:** es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo.
- **UTM:** Servicio basado en el despliegue, configuración y gestión remota de un Firewall de nueva generación FortiGate y que ofrece funcionalidades avanzadas, como el Filtrado web, antimalware o control de aplicaciones.
- **Virus, troyano, ransomware, exploit:** diferentes tipos de virus que se aprovechan de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.
- **VPN Site to Site:** Una red privada virtual (VPN) de sitio a sitio es una conexión entre dos o más redes, como una red corporativa y una red de sucursales. Muchas organizaciones utilizan VPN de sitio a sitio para aprovechar una conexión a Internet para el tráfico privado como alternativa al uso de circuitos MPLS privados.
- **VPN SSL:** Una red VPN SSL (Virtual Private Network – Secure Sockets Layer) es una forma de red privada virtual (VPN) que se puede usar con un navegador web estándar. ... Se utiliza para proporcionar a usuarios remotos con acceso a aplicaciones Web, aplicaciones cliente/servidor y conexiones de red internas.
- **Whitelist:** Dentro del servicio UTM Gestionado, hace referencia a una lista o registro de correos electrónicos, dominios, URLs., que el cliente quiere permitir, tanto a nivel de acceso como de navegación.
- **Workstations:** Dentro del servicio UTM Gestionado, hace referencia a la funcionalidad de IPS (Intrusion Prevention System) que se encarga de la defensa de los equipos finales de los usuarios.