Condiciones Técnicas Servicio

Soporte y Seguridad Digital

PRIMERO: Objeto

En el presente documento se detallan los alcances y limitaciones aplicables a las funcionalidades comprendidas en el Servicio de Soporte y Seguridad Digital contratado por el cliente (el "Servicio"), regulado en el respectivo Anexo de prestación de servicios celebrado entre ENTEL y el CLIENTE (el "Anexo").

Las funcionalidades aplicables dependerán del servicio y respectivo plan contratado: Soporte Digital Pyme, Seguridad Digital Pyme o Seguridad Digital Plus.

SEGUNDO: Funcionalidades

Para los puntos desarrollados a continuación se entenderá como "incidencias" aquellos eventos o actividades no deseadas que afectan la confidencialidad, integridad o disponibilidad de los sistemas de información o datos de la organización. Estas incluyen accesos no autorizados, infecciones por malware, ataques de ingeniería social o la explotación de vulnerabilidades por amenazas internas o externas, entre otras.

3.1 Asistencia Experta a Domicilio

Alcance del Servicio:

Este servicio abarca la resolución de incidencias en sistemas operativos Windows y MAC en versiones soportadas, siempre que no hayan podido ser resueltas de manera remota. La prestación está sujeta a la disponibilidad del sistema operativo propiedad del CLIENTE y a la posesión de una copia legítima del mismo, entendida como la clave de producto válida y el medio de instalación original del fabricante.

Quedan excluidas las configuraciones o solicitudes de cualquier otro servicio que no se derive de un mal funcionamiento de los equipos del CLIENTE, de conformidad con lo regulado en el Contrato y en las presentes Condiciones Técnicas.

La mano de obra será proporcionada sin costo adicional. En caso de que sea necesario reemplazar piezas, se facilitarán las especificaciones técnicas para que el CLIENTE pueda adquirirlas a su costo, para posteriormente ser instaladas bajo la prestación del actual servicio sin pago alguno.

Garantía del Servicio:

La garantía del servicio de asistencia prestado por Entel tendrá una vigencia de 30 días hábiles a partir de la finalización del servicio. Si se produce una nueva incidencia después de este plazo, se considerará como una asistencia a domicilio adicional.

La garantía cubre únicamente los fallos de funcionamiento derivados de instalaciones o reparaciones en los sistemas informáticos del CLIENTE en los que él haya trabajado directamente. No se aplica a sistemas en los que Entel no haya realizado ninguna intervención, a menos que se demuestre que el trabajo realizado en un sistema ha afectado el funcionamiento de otro sistema directamente relacionado.

La garantía comienza a partir de la fecha de finalización de los servicios y no incluye reconfiguraciones o reinstalaciones derivadas de nuevas especificaciones solicitadas por el CLIENTE tras la finalización del trabajo.

No se incluye en el Servicio:

- Limpieza interna y externa de los equipos.
- Manipulación de equipos en garantía cuando se requiera intervención física. Por ejemplo, al realizar un reemplazo de piezas de hardware.
- Reparaciones de desperfectos físicos del hardware, quedando el costo de las piezas de hardware bajo responsabilidad del CLIENTE.
- Suministro de software necesario para la reinstalación del sistema; el CLIENTE debe disponer del mismo.
- Soporte para servidores y dispositivos de red (hub/switch).
- Soporte para la instalación de programas crackeados o no oficiales.
- Asistencia in situ para routers.
- Configuración avanzada o asistencia en conectividad y uso de equipos o dispositivos multimedia profesionales.

- Piezas, accesorios o software necesarios para la resolución de las incidencias.
- Asistencia en sistemas operativos Linux y UNIX.
- No se incluye la realización de configuraciones ni la solicitud de servicios que no deriven de un mal funcionamiento de los equipos del CLIENTE.

3.2 Soporte Tecnológico Integral

Alcance del Servicio:

Software:

El servicio cubre asistencia informática en sistemas operativos y aplicaciones de uso común en el entorno del CLIENTE, en todas sus versiones soportadas por los fabricantes. A continuación, se detallan las aplicaciones y sistemas soportados por el Servicio:

- **Sistemas operativos:** Microsoft Windows, Mac OSX, Android e iOS en versiones soportadas por sus fabricantes.
- **Programas de oficina:** Microsoft Office, Microsoft Office para MAC, iWorks, Open Office y LibreOffice.
- **Navegadores y correo electrónico:** Microsoft Edge, Mozilla Firefox, Chrome, Outlook, Hotmail, Gmail, Office 365, Workspace, Safari, Thunderbird y Mac OS Mail.
- **Programas multimedia:** Adobe Acrobat, Windows Media Player, Real Player, iTunes, iLife, VLC Media Player, QuickTime, y otros códecs principales.
- **Compresores:** WinZip, WinRAR, StuffIt Expander y Keka.
- **Antivirus y firewalls:** Bitdefender, TrendMicro, Microsoft Security Essentials, Panda, Symantec, McAfee, Kaspersky, AVG, Avast, y firewall de Mac OS. El servicio incluye la instalación, configuración y actualización gratuita de antivirus.
- **Programas de videoconferencia y mensajería instantánea:** Zoom, Google Meet, Cisco Webex, Microsoft Teams, Google Duo, Skype y Hangouts.

Entel se compromete a proporcionar soporte para cualquier aplicación o sistema que sustituya o sea una evolución de los anteriores.

Servicios incluidos:

- Ayuda en el manejo de las aplicaciones soportadas en el Centro de Soporte (las indicadas anteriormente).
- •Instalación y desinstalación de las aplicaciones soportadas.
- Actualización de versiones y Service Pack para el software soportado, siempre que el USUARIO disponga de la licencia pertinente o la actualización sea gratuita.
- Configuración de los sistemas operativos y aplicaciones soportadas.
- Asesoramiento sobre requisitos hardware y software para las aplicaciones soportadas.
- Asistencia en instalación y configuración de certificados electrónicos.
- Asistencia en instalación de escritorios virtuales
- Revisión de sistema de back-up para copias de seguridad y recuperación de datos y realización de copias de seguridad de archivos: Soporte al sistema de back-up que tenga el USUARIO. Limitado al puesto de trabajo, no para servidores.
- Encriptación de discos con información sensible para cumplimiento de la ley de Protección de Datos: El cifrado se realizará con la herramienta BitLocker siempre que el equipo del USUARIO cuente con la licencia del software. En el caso de que el USUARIO tenga otro software licenciado, se ayudará al USUARIO en el proceso de cifrado siempre que el software sea mono-puesto. En cualquier caso, las claves de cifrado nunca serán almacenadas en los sistemas de FRACTALIA, por lo que nuestro personal no podrá realizar ningún descifrado si el USUARIO olvidó la clave de encriptación.
- Asistencia a terminales punto de venta (TPV): El servicio cubre el soporte remoto a la computadora y a su conectividad con la impresora de tickets y el lector de código de barras. El USUARIO deberá tener contrato de mantenimiento vigente del software de TPV para casos de incidencias con el SW o su funcionalidad.
- Servicio de soporte al almacenamiento de documentación en la nube (aplicaciones gratuitas): Asesoramiento y configuración del backup en las

herramientas gratuitas existentes en el mercado (Dropbox, GDrive, ...), o bien en la que ya tenga contratada el USUARIO, con licencia en vigor.

- Servicio de gestión de contraseñas: Soporte en el uso del almacenamiento de credenciales de Windows y de los Navegadores.
- Conectividad dentro de la red interna del USUARIO.
- Asesoría en el procedimiento para cambiar la contraseña de acceso a la computadora.
- Asesoría en el procedimiento para consultar contraseñas guardadas en los navegadores.
- Asesoría en el procedimiento para eliminar contraseñas específicas y eliminar todas las contraseñas de los navegadores.

El servicio se presta sobre los sistemas operativos y aplicaciones soportadas, siempre sujeto a la disponibilidad en función del sistema operativo propiedad del CLIENTE y la posesión de una copia legítima de la misma, entendiéndose ésta como la clave y el medio de instalación válidos para el fabricante.

Si fuera necesario a juicio del técnico especialista una toma de control remoto del equipo para solucionar la incidencia, éste informará al CLIENTE y solicitará consentimiento. Previo a la toma de control remoto, el CLIENTE deberá realizar copias de seguridad de los datos, software u otros ficheros almacenados en los discos de su computadora u otros soportes.

Hardware:

Todos los servicios de asistencia remota abajo descritos son aplicables a estaciones de trabajo Intel o AMD con sistema operativo MS Windows y a estaciones de trabajo Apple con sistema operativo MAC OSX con procesadores Intel.

Los servicios de asistencia incluidos son:

- Incidencias en estaciones de trabajo (equipos de sobremesa, portátiles y dispositivos móviles).
- Configuración del hardware y sistema operativo.
- Conexión y configuración de periféricos tales como impresoras, escáneres, teclados, ratón, cámaras web o digitales, monitores, micrófonos, etc.

- Dado que para la realización de estas actividades en muchas ocasiones será necesario el software original del dispositivo, si el USUARIO no dispone del mismo, los técnicos buscarán y descargarán el software de controladores disponible en Internet en el PC del USUARIO siempre que sea posible.

No se incluye en el Servicio:

Quedan excluidas las asistencias para equipos o programas ajenos al ámbito de cobertura de los servicios contratados, usos y soporte profesional de aplicaciones y plataformas, así como servidores.

El servicio de Asistencia tecnológica integral no cubre la asistencia a:

- Las asistencias para equipos o programas ajenos al ámbito de cobertura del alcance descrito anteriormente.

- Averías referentes a la conectividad, que sean responsabilidad del operador de internet del USUARIO.

- El software necesario para solucionar alguna avería, ni la reparación de desperfectos físicos. Si fuera necesario reparar o suministrar algún tipo de software, se haría al USUARIO el correspondiente presupuesto.
- Instalación / configuración de software no contemplado en el alcance del servicio o de programas crackeados o ilegales.

- El soporte a programas o aplicaciones desarrolladas específicamente para una empresa.

- Soporte a programas o software de gestión específicos.

- Soporte sobre Access, Macros, tablas dinámicas, fórmulas complejas o sistemas estadísticos en Excel.

- Soporte a servidores.

- Capacitación sobre programas e informática en general; no se prestará formación avanzada o repetitiva sobre una misma cuestión.

3.3 OPTIMIZACIÓN DE DISPOSITIVOS Y CONECTIVIDAD

Alcance del Servicio:

Este servicio analizará, para dispositivos con sistemas operativos Windows, Mac y Android, los siguientes 4 puntos clave:

- Dispositivos
- Conectividad
- Router
- Test de velocidad

En cada uno de ellos se analizarán aquellas características críticas para la velocidad de conexión.

Se requerirá un dispositivo con un sistema operativo soportado por el fabricante.

3.4 RECUPERACIÓN DE COPIAS DE SEGURIDAD

Alcance del Servicio:

Se abrirá una sesión de chat con un técnico especializado que atenderá al CLIENTE, evaluará la situación y proporcionará una solución guiada para la recuperación de datos o problemática asociada. Si es necesario, el técnico podrá solicitar autorización para tomar el control del dispositivo y efectuar directamente las operaciones necesarias de manera remota.

Cuando alguno de los sistemas de almacenamiento de información resulte dañado por cualquier causa y no pueda acceder a los datos almacenados, ni se cuente con copia de seguridad, se realizará el análisis del dispositivo con el fin de concluir si es posible o no la recuperación de información.

No se incluye en el Servicio:

El servicio no incluye los posibles costes de reparación del dispositivo ni los correspondientes a servicios sofisticados de análisis físico del dispositivo para la recuperación.

3.5 SOPORTE MICROSOFT 365

Alcance del Servicio:

El servicio comprende las siguientes coberturas:

- Recuperación de contenido de buzones de correo borrados por error siempre que la copia de seguridad sea accesible y no esté dañada.
- Configuración del dominio en la creación de cuentas de correo.
- Creación de grupos de seguridad.
- Modificación de los permisos de acceso.
- Soporte en el uso de la plataforma Microsoft 365.
- Soporte para la resolución de incidencias del servicio y de su configuración.
- Soporte en lo relativo a actualizaciones de software del sistema Microsoft 365.
- Asesoramiento en el uso de las aplicaciones incluidas dentro del paquete Microsoft 365.
- Escalaciones a Microsoft de problemas de la plataforma.

3.6 SOPORTE GOOGLE WORKSPACE

Alcance del Servicio:

Este servicio comprende las siguientes acciones:

- Recuperación de contenido de buzones de correo borrados por error siempre que la copia de seguridad sea accesible y no esté dañada.
- Configuración del dominio en la creación de cuentas de correo.
- Creación de grupos de seguridad.
- Modificación de los permisos de acceso.
- Soporte en el uso de la plataforma Google Workspace.
- Soporte para la resolución de incidencias del servicio y de su configuración.
- Soporte en lo relativo a actualizaciones de software del sistema Google Workspace.
- Asesoramiento en el uso de las aplicaciones incluidas dentro del paquete Google Workspace.
- Asesoramiento al Cliente para escalaciones a Google de problemas de la plataforma.

3.7 E-LEARNING Y CONCIENCIACIÓN

Alcance del Servicio:

El objetivo de este servicio es concienciar sobre las amenazas y vulnerabilidades en materia de riesgos en Ciberseguridad, así como formar en la prevención, detección y reacción ante los principales riesgos en el actual entorno tecnológico.

A través de la plataforma de formación el CLIENTE podrá realizar la formación de concienciación en ciberseguridad que se encuentra compuesta por varios módulos sobre los cuales podrá ir avanzando de forma gradual. En ella quedarán registrados todos los CLIENTES, el tiempo que han permanecido aprendiendo, la evaluación de los cuestionarios realizados y se podrán obtener las evidencias a través de informes generados desde la propia plataforma.

Nuestra plataforma será el punto de encuentro de todos los CLIENTES, disponible 24 horas y accesible desde cualquier dispositivo. Tendrán acceso al curso de Ciberseguridad y además existirá la opción de poder alojar diferentes contenidos, así como acceso a cuestionarios de satisfacción y cualquier otro tipo de encuesta que se habilite dentro del plan de formación. Dentro de la plataforma de servicios se tendrá acceso a los manuales de formación para que el CLIENTE pueda consultarlos cuando necesite.

3.8 CUESTIONARIO DE CIBERSEGURIDAD

Alcance del Servicio:

La calificación resultante es una opinión basada en el criterio y metodología creada para este servicio. Esta es revisada y actualizada periódicamente, buscando un mejor entendimiento de las necesidades de los CLIENTES. Las calificaciones no son hechos, por tanto, no deberían ser juzgadas como “exactas” o “inexactas”.

Las calificaciones incluyen una cierta visión futura En muchos casos, estas predicciones pueden estar basadas en tendencias de mercado (globales o específicas) o en datos históricos.

Características:

- Conocimiento de la puntuación asociada a cada una de las áreas de tu empresa.
- Orientado a cualquier tipo de empresa, pyme o corporación.

- Análisis fácil y rápido de completar.

- Resultado y proceso didáctico para el CLIENTE.

- Genera recomendaciones y evidencias útiles para tu empresa, ayudando a conocer que áreas son más vulnerables a posibles ataques, además de conocer su riesgo real.

- Histórico de todas las evaluaciones para contrastar la evolución en cada una de las áreas.

3.9 SIMULADOR DE ATAQUES

Alcance del Servicio:

Con este servicio de concienciación se podrá comprobar el nivel de precaución de los trabajadores ante incidencias de ciberseguridad. En el caso de que accediera al ataque la plataforma le ofrecerá píldoras formativas para evitar el incidente en un futuro.

Concienciación CiberAttack Simulator es un servicio de entrenamiento interactivo continuo y automatizado de concienciación, para la prevención de riesgos en ciberseguridad, basado en ataques simulados con varios niveles de complejidad como, por ejemplo: Ransomware, Phishing, Malware, Exploits, Privacidad, Fraude, etc. Con este servicio mantenemos formado, informado y alerta todo el año al personal de la organización sobre los riesgos y ataques en ciberseguridad, simulándolos directamente en sus dispositivos, ya sea por email o por SMS. Una vez activado se procederá al envío de un promedio entre 3 a 5 correos mensuales de ataques simulados para mantener alerta a los empleados. El administrador podrá comprobar en la plataforma de servicios la evolución y madurez de sus empleados ante este tipo de ataques.

3.10 ACCESO REMOTO SEGURO

Alcance del Servicio:

Este servicio incluye:

- **SSL**: Protocolo de capa de sockets seguros, para crear una conexión segura y cifrada con AES256
- **Cifrado de extremo a extremo**: Comunicaciones cifradas en todo su recorrido, con el objetivo de la prevención en ataques.
- **Control de acceso:** Acceso únicamente a aquellos dispositivos que han sido previamente autorizados para el uso del servicio.
- **Dispositivos móviles**: Este servicio también puede ser utilizado en dispositivos móviles. (Android y IOS).
- **Configuración inicial**: Se incluye configuración inicial para su correcto uso.
- **Uso**: Uso recomendado para 10 dispositivos en remoto.

3.11 INFORME PRESENCIA EN INTERNET

Alcance del Servicio:

Este servicio le ayudará a conocer la presencia en internet de su organización, dependiendo del alcance contratado el CLIENTE tendrá derecho a un número de informes anuales para conocer la presencia en internet en cada momento. El informe se elaborará para la empresa CLIENTE, mediante previa autorización de su representante legal o a sus colaboradores. El CLIENTE deberá indicar expresamente cuantos datos necesite para poder identificarle entre todos los resultados encontrados en las búsquedas realizadas durante la prestación del servicio, con el objetivo de determinar fehacientemente que la información o datos encontrados en la red se corresponden con el CLIENTE.

Por lo que respecta al servicio mencionado, Entel se compromete a garantizarlo, siempre y cuando no requiera de actuaciones extraordinarias ante órganos administrativos o judiciales, o sea considerado de dudosa viabilidad por motivos fundados ajenos a su voluntad o legales.

Para solicitar el informe el CLIENTE deberá acceder mediante la plataforma de servicios conectada y rellenará un formulario donde deberá aportar la siguiente documentación:

- Razón social y RUT del CLIENTE sobre el que se quiere realizar el informe.
- El CLIENTE podrá añadir comentarios u observaciones adicionales que se deban tener en cuenta en la búsqueda que se realice.

El CLIENTE podrá solicitar a ENTEL una copia del formulario rellenado en ocasión de auditoría o requerimiento administrativo, debiendo Entel entregarlo en no más de dos días hábiles.

El documento PDF que contiene el informe de Presencia en Internet estará disponible en la cuenta del CLIENTE en un máximo de 5 (cinco) a 7 (siete) días hábiles contados a partir de la fecha de la solicitud del servicio. Todos los documentos PDF solicitados a lo largo de la prestación del servicio se encontrarán siempre disponibles para su consulta y descarga en la cuenta del USUARIO.

No se incluye en el Servicio:

El servicio NO incluye:

- La defensa por las acciones legales que se ejerciten contra el CLIENTE por el uso incorrecto de la cobertura.
- Las consecuencias que puedan derivarse de la aportación de datos falsos por el CLIENTE.
- Las acciones legales que pueda emprender el CLIENTE ni los costes derivados de su ejercicio.
- Cualquier prestación o servicio distintos a los descritos en esta cobertura.
- Cualquier acción realizada por profesionales no designados por Entel.
- Gastos y costes adicionales como consecuencia de la realización de trabajos de duración extraordinaria o de tipología jurídica, los cuales podrán facturarse independientemente.

3.12 CIBERSCORING

Alcance del Servicio:

Para el servicio de Ciberscoring existen dos alcances diferenciados:

Ciberscoring Freemium

Con nuestra tecnología de auditoría podemos analizar los riesgos de la infraestructura informática de una empresa y ayudar a saber qué puntos son más vulnerables a posibles ataques, este servicio en su modalidad freemium servirá para descubrir los activos de la compañía y tener un primer scoring con el que poder valorar la situación actual de la empresa.

Capacidades:

- Descubrimiento de activos. Inventariado automático de activos expuestos a internet relacionado con la organización.
- Descubrimiento y análisis de activos en IPv4 e IPv6 (dual-stack).
- Integración con los entornos cloud para monitorizar la seguridad de las instancias publicadas hacia internet.
- Cálculo de un score de seguridad basado en criterios técnicos que permite obtener un diagnóstico del nivel de seguridad del perímetro.
- Indicación de los incidentes descubiertos según nivel de criticidad.

Este servicio estará limitado a un máximo de doce (12) activos de la Empresa.

Beneficios:

- Análisis del perímetro de las organizaciones y reducción del riesgo.
- Detección de fallos de seguridad de alto riesgo en el menor tiempo posible.
- Informe de incidencias global, para que la empresa tenga una visión de su estado general. Para un informe detallado y continuo deberá adquirir el servicio de Ciberscoring.

Ciberscoring Premium

Con nuestra tecnología de auditoría podemos analizar los riesgos de la infraestructura informática de una empresa y ayudar a saber qué puntos son más vulnerables a posibles ataques, este servicio en su modalidad premium permitirá un análisis

periódico de los activos de la compañía, así como la evolución del scoring en cada uno de los análisis. Además, con cada análisis se podrá acceder a un informe pormenorizado de los descubrimientos y una página adicional que nos permita contemplar la evolución del scoring de la compañía.

Capacidades:

- Descubrimiento de activos. Inventariado automático de activos expuestos a internet relacionado con la organización.
- Descubrimiento y análisis de activos en IPv4 e IPv6 (dual-stack).
- Integración con los entornos cloud para monitorizar la seguridad de las instancias publicadas hacia internet.
- Análisis de seguridad de los activos de forma periódica y desatendida.
- Análisis en capa de red y capa aplicación simplificando los procesos de configuración y control de herramientas de seguridad.
- Cálculo de un score de seguridad basado en criterios técnicos que permite obtener un diagnóstico del nivel de seguridad del perímetro.

Beneficios:

- Control de los sistemas sensibles a sufrir ataques desde internet.
- Análisis de la totalidad del perímetro de las organizaciones y reducción del riesgo.
- Detección de fallos de seguridad de alto riesgo en el menor tiempo posible.
- Reducción al máximo del tiempo de operación. Automatización de detección y remediación.
- Ahorro en coste de licencias en herramientas de seguridad.

A través de nuestra plataforma de ciberseguridad se puede solicitar el análisis de ciberscoring. Tan solo es necesario rellenar un formulario indicando el nombre de la compañía, los dominios a analizar, así como los dominios de email. Una vez que el análisis esté completado, la plataforma mostrará el rating obtenido por parte de la empresa, así como un breve análisis inicial de lo descubierto. El siguiente análisis se

efectuará de forma automática dependiendo de la periodicidad contratada. Cada análisis será notificado además vía mail.

3.13 ANTIVIRUS

Alcance del Servicio:

Una vez completada la instalación, será el propio antivirus quien automáticamente y de forma ininterrumpida analice los dispositivos del CLIENTE en busca de amenazas. El CLIENTE encontrará un resumen de los resultados de estos análisis en nuestra plataforma y podrá consultarlos siempre que quiera.

Con la solución Bitdefender Total Security se proporciona a los dispositivos una seguridad avanzada ante cualquier tipo de amenaza, gracias a sus módulos de seguridad:

- Protección: Protección multicapa que mantiene sus dispositivos a salvo de todas las amenazas nuevas y existentes.
- Rendimiento: Reacciona instantáneamente ante el malware sin sacrificar el rendimiento de tu dispositivo.
- Privacidad: Cuida de su información personal y de su privacidad en Internet

Una protección completa contra el malware y contra las amenazas digitales en los principales sistemas operativos, Windows, MacOS, iOS y Android. Con módulos adicionales que hacen que la protección frente amenazas sea completa.

	Windows	MacOS	Android	iOS
Multicapa para las amenzas nuevas y existentes				
Protección completa de datos en tiempo real	x	x	x	x
Prevención de amenazas de red	x	x		
Defensa contra amenazas avanzadas	x	x		
Protección contra ransomware multicapa	x	x		
Evaluación de vulnerabilidad	x			
Prevención de ataques web	x	x	x	x
Antiphishing	x	x	x	x
Anti fraude	x	x	x	x
Antispam	x	x	x	x
Entorno de rescate	x			
Autopilot	x	x	x	
Bitdefender Photon™	x			
Red de Protección Mundial	x	x	x	x
Modos de juego, película y trabajo	x			
OneClick Optimizer	x	x	x	
Ficheros Seguros		x		
Anti AdWare	x	x		
Protección completa sobre su información personal y Privacidad en Internet				
Bitdefender VPN	x	x	x	x
Anti-tracker	x	x		
Monitor de micrófono	x			
Protección de cámara web	x			
Banca en línea segura	x	x		
Control parental	x	x	x	x
Cortafuegos de privacidad	x			
Anti-robo	x		x	
Asesor de seguridad wifi	x			
Protección de redes sociales	x			
App Lock			x	
WearON			x	
Wallet	x			
Destructora de ficheros	x			
Privacidad de cuenta			x	x

Requisitos del Servicio:

- Windows:
  - Sistema operativo: Windows 7 con Service Pack 1, Windows 8.1, Windows 10 y Windows 11
  - Memoria (RAM): 2 GB
  - Espacio libre en disco: 2,5 GB de espacio libre

- MacOS:
  - Sistema operativo: macOS X Yosemite (10.10) o posterior.
  - Espacio libre en disco disponible: 1 GB de espacio libre
  - Navegadores compatibles: Safari, Firefox, Google Chrome
  - Puede instalar Bitdefender VPN solo en dispositivos con macOS Sierra (10.12 o posterior)

- iOS:
  - Sistema operativo: iOS 12 o posterior

- Android:
  - Sistema operativo: Android 5.0 o posterior
  - Dispositivos habilitados para Google Play Services.

3.14 ANTIVIRUS PROFESIONAL

Alcance del Servicio:

El antivirus profesional es un sistema de protección antimalware contra virus, gusanos, troyanos, spyware, adware, keyloggers, rootkits y otros tipos de software malicioso. Dicha protección se efectúa por capas, y los análisis que se realizan son:

- **Análisis de firmas**: Constituye la primera capa de protección y es una tecnología que compara todo el contenido analizado con una base de datos de firmas para reconocer peligros potenciales. Este método de análisis es efectivo contra amenazas confirmadas que han sido descubiertas y documentadas.

- **Análisis heurístico**: Es una tecnología que actúa contra las amenazas de nueva generación. Este análisis constituye una segunda capa de protección. Los algoritmos heurísticos detectan el malware en función de las características de su comportamiento, ejecutan los archivos sospechosos en un entorno de protección virtual para asegurarse de que no supongan una amenaza, y en caso de posible amenaza el programa se encarga de eliminarlos.

- **Control de amenazas avanzadas**: Es un sistema encargado de luchar contra las amenazas que logran eludir las capas anteriores. Esta capa de seguridad monitorea continuamente los procesos en ejecución y detecta las conductas sospechosas para mitigarlas.

Este servicio mostrará dentro de la plataforma información sobre el estado de la protección.

Con la activación del servicio se recomienda realizar un análisis completo del dispositivo. Si el análisis ha sido satisfactorio y no se han encontrado amenazas, el dispositivo aparecerá como protegido. Si por el contrario se encuentra alguna anomalía, el CLIENTE podrá ver las amenazas y archivos que han sido bloqueados. Se recomienda al CLIENTE que revise los archivos que han sido puestos en cuarentena porque son aquellos que el antivirus ha catalogado como potencialmente peligrosos.

También se dispondrá de una vista general, desde allí el CLIENTE podrá ver cuándo se realizó el último análisis, gestionar los dispositivos protegidos o añadir algunos nuevos.

Si además de la información resumida que se muestra en los gráficos quiere profundizar un poco más, el CLIENTE encontrará una tercera sección con un historial

de todas las amenazas encontradas junto a información detallada sobre las mismas.

Antivirus Profesional EDR+ATP (Endpoint detection and response + Advance threat Protection).

El servicio de Antivirus Profesional se presta con la solución Bitdefender Gravity que incluye el módulo EDR+ATP.

La detección y respuesta en los endpoints (EDR) de Bitdefender Gravity es un componente de correlación de eventos, capaz de identificar amenazas avanzadas o ataques en curso con una monitorización proactiva para las alarmas de alta criticidad.

Como parte de nuestra plataforma de protección de endpoints completa e integrada, la EDR aporta inteligencia en los dispositivos para toda la red. Esta solución viene a apoyar el esfuerzo de los equipos de respuesta ante incidentes en su afán de investigar y responder a las amenazas avanzadas.

A través de Bitdefender Endpoint Security Tools, se pueden activar en los endpoints administrados un módulo de protección llamado Sensor EDR, con el fin de recopilar Capas de protección de Gravity Zone, datos del hardware y de los sistemas operativos.

Siguiendo un marco cliente-servidor, los metadatos se recopilan y procesan en ambos lados. Este componente aporta información detallada sobre los incidentes detectados y un mapa interactivo de incidentes, así como acciones de reparación e integración con Sandbox Analyzer y HyperDetect.

Bitdefender HyperDetect es una capa adicional de seguridad específicamente diseñada para detectar ataques avanzados y actividades sospechosas en la fase previa a la ejecución. HyperDetect incorpora modelos de aprendizaje automático y una tecnología de detección de ataques sigilosos contra amenazas como las de día cero, amenazas persistentes avanzadas (APT), malware ofuscado, ataques sin archivos (uso ilegítimo de PowerShell, Windows Management Instrumentation, etc.), robo de credenciales, ataques selectivos, malware personalizado, ataques basados en scripts, exploits, herramientas de pirateo informático, tráfico de red sospechoso, aplicaciones potencialmente no deseadas (APND) y Ransomware.

Para las amenazas que logran eludir incluso el motor heurístico, existe otra capa de seguridad denominada Advanced Threat Control (ATC). Advanced Threat Control monitoriza continuamente los procesos en ejecución y detecta las conductas sospechosas, como por ejemplo los intentos de ocultar el tipo de proceso, ejecutar código en el espacio de otro proceso (secuestro de memoria del proceso para escalado

de privilegios), replicar, descartar archivos, ocultarse a las aplicaciones de listado de procesos, etc. Cada comportamiento sospechoso aumenta la calificación del proceso. Cuando se alcanza un límite, salta la alarma.

3.15 ANÁLISIS DE VULNERABILIDADES IP

Alcance del Servicio:

Este servicio le ayudará al CLIENTE a conocer el nivel de seguridad y las posibles vulnerabilidades de su entorno y de los servicios accesibles desde redes externas.

Se realizará una revisión de seguridad para identificar el nivel de seguridad de la plataforma tecnológica, además de los servicios a los que se puedan acceder desde redes externas, así se detectarán las vulnerabilidades existentes, riesgos y procesos afectados.

Las principales funcionalidades de este servicio son las siguientes:

- Revisión de la caja negra externa

- Identificación de redes y direccionamientos
- Identificación de:
    - Servidores
    - Protocolos
    - Aplicativos

- Análisis de vulnerabilidad

3.16 PROTECCIÓN DE IDENTIDAD DIGITAL: TARJETA BANCARIA

Alcance del Servicio:

Este servicio le ayudará al CLIENTE a proteger sus tarjetas de crédito y a estar informado en todo momento en caso de que se produzca alguna vulnerabilidad de seguridad con las mismas.

Las principales funcionalidades de este servicio son:

- Rastreamos en la web no indexada a motores de búsqueda y buscamos los números de tarjetas bancarias de los CLIENTES por si sus tarjetas fueron robadas y están a la venta.

- Monitorización continua y alerta inmediata si encontramos la tarjeta en la web..
- Reduce el riesgo de que el ciberdelincuente use las tarjetas bancarias para realizar compras y pagos en su nombre.
- Seguridad en la utilización del servicio. El CLIENTE solo facilitará parte de la numeración de la tarjeta, en ningún caso la fecha de validez ni el CCV ni ningún otro dato.
- Comunicación de la alerta mediante correo electrónico.

3.17 PROTECCIÓN DE IDENTIDAD DIGITAL: EMAIL

Alcance del Servicio:

Este servicio le ayudará al CLIENTE a monitorizar la protección de su identidad. Buscamos en la web no indexada a motores de búsqueda la presencia de tus cuentas de correo por si cualquiera de ellas hubiese sido vulnerada.

Las principales funcionalidades de este servicio son las siguientes:

- Monitorización de la identidad y notificación al CLIENTE. Comunicación proactiva de alerta mediante correo electrónico.

- Notificación especial al CLIENTE si se detectan robos de credenciales y éstas están a la venta en la web.

- Reducción del riesgo de que ciberdelincuentes se hagan pasar por el CLIENTE haciendo cargos y compras ilegítimas, publicaciones en RRSS o acciones ilícitas sin su consentimiento.

- Seguridad en la utilización del servicio. El CLIENTE sólo facilita la credencial de acceso, en ningún caso la contraseña.

3.18 ANÁLISIS DE VULNERABILIDADES DE RED

Alcance del Servicio:

Se realizará una revisión del estado de la red del CLIENTE, se detectarán las vulnerabilidades y serán clasificadas de acuerdo con su criticidad usando normas como las CVSS (Common Vulnerability Score System).

Técnicos expertos ayudarán al CLIENTE a la interpretación del informe obtenido y le asesorará sobre las medidas necesarias para intentar mitigar las vulnerabilidades obtenidas, con el fin de mejorar la seguridad de su entorno.

Las principales funcionalidades de este servicio son las siguientes:

- Análisis de vulnerabilidades de la red.
- Clasificación de las vulnerabilidades detectadas.
- Asesoramiento para interpretación del informe.
- Asistencia para la mitigación de las vulnerabilidades.

3.19 ANÁLISIS DE VULNERABILIDADES WEB

Alcance del Servicio:

El servicio utiliza una herramienta que escanea todos los posibles "agujeros" de seguridad en los entornos web tanto de páginas como de aplicaciones.

La herramienta también analiza todos los entornos web tanto de protocolos HTTP como HTTPS y realiza un informe detallado de las vulnerabilidades detectando y valorando la criticidad de cada uno de los riesgos.

El informe estará accesible en la plataforma conectada del servicio. Existen diferentes recurrencias de los informes que pueden ser contratadas, 30 días, 90 días, 180 días. Todos los informes quedarán accesibles desde la plataforma con el fin de poder ver la evolución con las mejoras implementadas por el CLIENTE.

Exclusiones:

Como parte del servicio, no se realiza tratamiento del contenido del informe. Ante cualquier duda, el CLIENTE puede contactar con el soporte técnico para el asesoramiento en la interpretación del mismo. Sin embargo, no se incluyen las acciones necesarias a realizar para mitigar las vulnerabilidades detectadas.

El CLIENTE deberá contactar con su proveedor de páginas Web para la revisión de las vulnerabilidades detectadas.

3.20 RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES

Alcance del Servicio:

Servicios de soporte a la configuración, mantenimiento, despliegue, definición de políticas de seguridad de las soluciones o herramientas de seguridad definidas en la propuesta. Las tareas incluidas son:

- Integración de herramientas con Dashboard de control. El servicio tiene incluido una plataforma de soporte en la que el CLIENTE podrá interactuar y ver el estado de su servicio. En el caso de plataforma conectada además podrá visualizar parámetros de control de las herramientas de seguridad contratadas.

- Soporte funcional de las herramientas de seguridad. Servicio de soporte a cualquier necesidad de configuración, mantenimiento y soporte de las herramientas de seguridad contratadas.

- Despliegue y configuración de las herramientas. Ayudamos al despliegue, instalación y configuración de las herramientas de seguridad.

- Configuración de las herramientas. Si después del despliegue el CLIENTE necesita una configuración adicional o mantenimiento nuestro servicio le dará soporte.

- Definir nuevas políticas y cambiarlas. Damos soporte a la definición de políticas de seguridad necesarias de las herramientas de seguridad.

- Respuesta e identificación a incidentes de seguridad. Damos una primera respuesta y propuesta de resolución a incidentes de seguridad. Si en algún caso la resolución se pudiera realizar a través de las herramientas de seguridad contratadas, nuestros técnicos la realizan.

Incluye un soporte SOC que ayudará a la resolución o propuesta de las medidas necesarias ante incidentes de seguridad más complejos (malware, ataques de aplicaciones, etc.). Los servicios diferenciales del soporte SOC son los siguientes:

- **Alerta antivirus**: Incidencia reactiva a causa de un virus, se procederá a ejecutar un análisis completo del sistema. Una vez finalizado se eliminarán los archivos en cuarentena encontrados en el análisis. Se almacenarán en el registro del CLIENTE: el virus detectado, la fecha y el método de infección.

- **Configuración del filtro de contenidos**: Daremos soporte y configuraremos el servidor DNS seguro para filtro de contenidos, configuraremos el módulo de seguridad Web del antivirus y sus componentes y estableceremos los filtros de control parental, con el fin de evitar accesos no deseados.

- **Amenaza interna**: Daremos soporte para detectar posibles amenazas internas por parte de espías, empleados etc., que puedan tener intenciones maliciosas de comprometer la seguridad, exfiltrar información o generar algún tipo de daño a la organización. y si se produjera un incidente se realizarán las siguientes acciones para intentar mitigarlos:

    - Identificar y clasificar los activos sensibles de la organización
    - Asegurar la disponibilidad, confidencialidad e integridad de dichos activos
    - Minimizar los privilegios de acceso a recursos a los CLIENTES
    - Monitorizar los activos sensibles y controlar los posibles puntos de filtración: correo electrónico, unidades USB, otras herramientas
    - Monitorizar la red en busca de tráfico sospechoso

- **Ataque Phishing**: Daremos soporte para detectar posibles amenazas relacionadas con ataques Phishing vía correo electrónico, etc., Si el CLIENTE no ha caído en el ataque, eliminaremos el correo y ayudaremos al CLIENTE a fortificar la seguridad de se cuenta. En el caso de que el CLIENTE haya facilitado algún tipo de credencial al atacante, se procederá a un cambio de urgencia de las credenciales de acceso y se fortificará la seguridad de la cuenta, en el caso de que no fuera posible restablecer la contraseña ayudaremos al CLIENTE a denunciar el robo de la cuenta mediante los mecanismos de comunicación que disponga el proveedor del servicio.

- **Ataque Malware**: En el caso de que haya un incidente de software malicioso, malware, ransomware, gusanos, etc., resolveremos y estabilizaremos los sistemas informáticos y una vez resuelto configuraremos las herramientas de seguridad para intentar mitigarlos.

- **Ataque de denegación de servicio**: En el caso de que alguno de los servicios del CLIENTE sufra de una indisponibilidad a causa de un ataque de DDoS, localizaremos el recurso afectado y se realizarán las siguientes comprobaciones:
    - Si se trata de un recurso alojado en un VPS, AWS, Azure, etc. se contactará con el proveedor para gestionar el incidente
    - Si se tiene control sobre el servidor en atacado, examinaremos los logs para detectar el incremento del tráfico.
    - En caso de que el sistema, sitio web, aplicación web sea gestionado o desarrollado por una empresa de software, contactaremos con ellos para gestionar el incidente.
    - Localizar posibles vulnerabilidades en servicios expuestos al exterior o el código de aplicaciones web que pudiesen ser explotadas para causar una denegación de servicio.

- **Ataque de contraseña**: Las organizaciones pueden tener incidentes relacionados con robo de contraseñas, en caso de incidente daremos soporte de las mejores prácticas de control de contraseñas evitando tener un sistema de contraseñas poco seguras (autentificación multifactor, software específico etc..), también revisaremos las políticas de seguridad de las herramientas de seguridad para intentar mitigar nuevos ataques.

- **Defacement Página Web**: El sitio web del CLIENTE ha sido comprometido y muestra un aspecto diferente al original. Se intentará localizar el problema que puede haber llevado al defacement. Ayudaremos al CLIENTE a restablecer la imagen del sitio web utilizando una copia de seguridad de este.

- **Ataque con robo de cuenta de correo**: Comprobaremos que el CLIENTE haya podido ser víctima de un ataque de phishing/smishing/vishing relacionado con el robo de la cuenta en cuestión y comprobaremos si sus credenciales han estado expuestas en alguno de los leaks.

- **Ataque Smishing**: Identificamos junto con el CLIENTE la información que ha podido compartir con el atacante y le ayudaremos a fortificar la seguridad de su cuenta mediante cambio de credenciales y establecimiento del doble factor de autentificación.

- **Ataque Ransomware**: Identificamos la infección y se activará el protocolo de detección de Ransomware. En primer lugar, solicitaremos al CLIENTE el apagado, aislamiento y desconexión del equipo de la red. Se asignará a un recurso encargado de revisar remotamente el estado de los recursos compartidos con la colaboración, en caso necesario, de personal presencial, a fin de descartar la propagación del malware a otros sistemas. Evaluará el estado del equipo para ejecutar la restauración sin riesgos en caso de la

existencia de copias de seguridad. Se aconsejará al CLIENTE la comunicación del incidente a las autoridades estatales o locales según la legislación.

3.21 SOPORTE DE RECUPERACIÓN DE SISTEMAS

Alcance del Servicio:

Si después de un incidente de seguridad tus sistemas quedan inoperativos o con funcionalidades reducidas, con este servicio nuestros técnicos especializados te ayudarán a restaurar el sistema.

Entre los métodos de recuperación más comunes incluidos dentro del alcance se contemplan:

- Restauración: En el caso de existir puntos de restauración anteriores al incidente, se recupera una versión anterior válida para restaurar la normalidad del sistema.
- Arranque con la última configuración válida conocida.
- Restauración en modo seguro con sólo símbolo del sistema.
- Reparación de inicio de Windows o recuperación automática del sistema.

Si no fueran válidos ninguno de los métodos anteriores, nuestros técnicos realizarán las siguientes acciones para restaurar el sistema:

- Reinstalación del sistema operativo del CLIENTE en caso de ser necesario (licencia facilitada por el CLIENTE).
- Instalación de software facilitado por el CLIENTE.
- Actualización de controladores Hardware.
- Instalación de nuevos controladores Hardware.
- Restauración de backup en el supuesto de que el CLIENTE disponga de copia de seguridad.
- Creación manual de puntos de restauración con la funcionalidad recuperada.

No se incluye en el Servicio:

Para la restauración de los sistemas el CLIENTE debe disponer de una versión legítima del sistema operativo y software a instalar. Este servicio **no tiene límites, pero está condicionado ante el hecho de que se haya desarrollado un incidente de seguridad.**

3.22 INFORME ANTE BRECHAS DE SEGURIDAD

Alcance del Servicio:

Con este servicio ante un incidente de seguridad y gracias a las herramientas instaladas, incluidas en el alcance, en los equipos del CLIENTE podremos realizar un informe de cómo, cuándo, dónde tuvo lugar la vulnerabilidad y propondremos acciones de mejora y resolución.

El CLIENTE responsable deberá solicitar el servicio y autorizar a nuestro equipo técnico para la elaboración del mismo.

El servicio incluye:

- Protección de la escena previo a la realización de la recolección de evidencias.
- Identificación de evidencias.
- Recopilación de evidencias:
    - En primer lugar, se recopilan las evidencias volátiles (registros, contenidos de caché, procesos, enrutamientos, Memoria RAM, temporales, etc.).
    - A continuación, se recopilan las evidencias de las herramientas instaladas incluidas dentro del alcance del servicio.
- Documentación de las evidencias obtenidas.
- Análisis de los resultados obtenidos, tratándolos en contextos globales y coherencia de información para aumentar la fiabilidad.
- Elaboración de informe técnico forense con detalle pormenorizado, enumerando herramientas usadas, creadas, información obtenida de terceros, citando fuentes
- Conclusiones con recomendaciones sobre medidas preventivas y controles adicionales para intentar minimizar los riesgos de un nuevo incidente de seguridad.

- Reunión con el CLIENTE responsable para explicar el informe facilitado, el significado de los registros y evidencias con relación a la información recabada y/o detectada en el análisis.

- El informe será accesible desde la plataforma de servicios.

Los técnicos mantendrán la integridad y la cadena de custodia, preservando los originales y trabajando con copias siempre que sea posible.

El informe generado no es válido judicialmente, se trata de un informe complementario que no tiene validez ante la autoridad competente.

Exclusiones:

Entel no proporcionará evidencias digitales ni sistematiza la identificación, recolección, adquisición y preservación de esta. Este servicio no tiene límites, pero está condicionado ante el hecho de que se haya desarrollado un incidente de seguridad.

3.23 COPIA DE SEGURIDAD EN LA NUBE

Alcance del Servicio:

Este servicio le ayudará al CLIENTE a proteger sus datos gracias a un agente instalado en sus dispositivos. Las copias se realizan todos los días evitando la posible pérdida de datos. Una de las ventajas de este servicio es que la información se almacena encriptada (AES256) en servidores en la nube evitando así el acceso a ciberdelincuentes. En caso de necesitar recuperar y acceder a la información, el CLIENTE podrá hacerlo desde cualquier dispositivo y en cualquier lugar.

Este servicio se solicitará a través de nuestra plataforma en la sección Copia de seguridad. Una vez procesada la petición, deberá acceder a su correo electrónico y seguir las instrucciones del email recibido.

Técnicos expertos le asesorarán sobre la información susceptible de ser almacenada en su copia de seguridad y le ayudarán en todo el proceso si tiene alguna consulta.

Requisitos:

- Dispositivo Windows, MacOS, Android, IOS (en versiones actualizadas y soportadas por el fabricante)
- Conexión Internet para realizar la copia de seguridad
- GB máximo según términos y condiciones del acuerdo