



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

PARTES:	El cliente	BT Spain
Nombre o razón social	XXXXXXXXXXXX (en lo sucesivo, "El Cliente")	BT GLOBAL ICT BUSINESS SPAIN, S.L.U. (en lo sucesivo, "El Proveedor", "Proveedor" o "BT")
Dirección fiscal	XXXXXXXXXXXX	C/ María Tubau N°3 28050 Madrid
NIF/CIF	XXXXXXXXXXXX	B- 88625496
Representante de la compañía	XXXXXXXXXXXX NIF de representante (Número de identificación) XXXXXXXXXXXX Cargo: XXXXXXXXXXXXXXX	Paul Rhodes (Número de identificación): X0.688.132-H Cargo: Representante legal

BT Managed Firewall Security es un Servicio Asociado de BT Managed Security Services. En consecuencia, las condiciones establecidas en el Anexo de BT Managed Security se aplicarán además del presente Anexo, salvo que se indique explícitamente lo contrario en el mismo.

1 DEFINICIONES Y ABREVIATURAS

Se aplicarán las siguientes definiciones y abreviaturas, además de las que figuran en las Condiciones Generales y el Anexo de BT Managed Security del Contrato.

"**Acceso Fuera de Banda**" es el acceso utilizado para la configuración inicial y para la gestión durante la vida útil cuando el medio principal de acceso al dispositivo de seguridad ha fallado o para ayudar a resolver un fallo del dispositivo de seguridad.

"**Acción de Mitigación**": una acción paliativa recomendada que debería adoptarse para abordar el impacto de los COI identificados por BT.

"**Activo Activo**" tiene el significado que se le da en el Apartado 2.2.10.

"**Activo Pasivo**" tiene el significado que se le da en el Apartado 2.2.10.

"**AD-VPN**" o "**Directorio Activo VPN**" significa un tipo de VPN que permite establecer dinámicamente túneles directos entre radios de una arquitectura hub-and-spoke.

"**Adquisición de BT**" hace referencia al modelo de entrega de BT Managed Firewall Security, en el que BT se hará cargo de la gestión de los Dispositivos de Seguridad del Cliente existentes y BT se encargará de la asistencia in situ y la gestión remota del servicio, tal y como se establece en el Apartado 2.1.1.

"**Anexo del servicio BT Managed Security**" es el Anexo asociado a BT Managed Firewall Security que proporciona una gama de servicios de gestión de seguridad graduados que pueden utilizarse en asociación con el Servicio y como superposición al mismo.

"**BGP**" significa un protocolo de red diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos.

"**Bloqueo Automatizado de COI**" tiene el significado que se le da en el Apartado 2.2.14 (b).

"**BT Managed Firewall Security**" se refiere al servicio tal y como se establece en el presente Anexo. Cuando BT Managed Firewall Security se utilice junto con BT Managed Security Services, también podrá denominarse "Servicio" en su conjunto;

"**Componentes Estándar del Servicio**" tiene el significado que se le da en el Apartado 2.1.

"**Disponibilidad**" significa el periodo de tiempo en el que el Servicio está funcionando.

"**DMZ**" significa "**zona desmilitarizada**" (a veces denominada red perimetral), una subred física o lógica que contiene y expone los servicios de cara al exterior de una organización a una red que no es de confianza, normalmente una red mayor como Internet.

"**Ethernet**" se refiere a una familia de tecnologías de redes informáticas para redes LAN.

"**Fin de Vida Útil**" se refiere a cualquier hardware o software que ya no reciba asistencia por parte del fabricante, vendedor o proveedor y que no pueda actualizarse a una versión compatible de forma rentable. BT sólo puede proporcionar asistencia limitada si el hardware o el software alcanzan esta fase.

"**FortiGate**" significa un cortafuegos de nueva generación, proporcionado por Fortinet.

"**Guía de Planificación del Emplazamiento**" hace referencia a una guía proporcionada por BT al Cliente en la que se detallan las especificaciones de hardware, incluidos los detalles ambientales, físicos y eléctricos de cualquier Equipo de BT proporcionado al Cliente con el cortafuegos gestionado de seguridad de BT.



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

"**Horario de Mantenimiento Contratado**" se refiere a las horas en las que BT realizará el mantenimiento de los Dispositivos de Seguridad solicitados como equipo de BT. Serán horas laborables, a menos que se indique lo contrario.

"**Inspección SSL/TLS**" se refiere a la Opción de Servicio establecida en el Apartado 2.2.9.

"**IOCs**" o "**Indicadores de Compromiso**" tienen el significado que se les da en el Apartado 2.2.14 (a) (i).

"**IPSec**" significa seguridad IP; es un marco basado en estándares que proporciona servicios de capa 3 para confidencialidad, privacidad, integridad de datos, autenticación y prevención de repeticiones.

"**Límite de Gestión del Servicio**" tiene el significado que se le da en el Apartado 3.6.

"**Lista de Bloqueo de BT**" se refiere a cualquier COI que BT haya identificado utilizando su plataforma Eagle-I.

"**Localizador uniforme de recursos**" o "**URL**": cadena de caracteres que apunta a un recurso en una intranet o en Internet.

"**Mejora de la Lista de Bloqueo Existente**" tiene el significado que se le da en el Apartado 2.2.14 (a) (ii).

"**Mitigación Cooperativa**" tiene el significado que se le da en el Apartado 2.2.15.

"**MPLS**" significa Multi-Protocol Label Switching, un servicio VPN privado y global basado en IP y en estándares de la industria que proporciona al Cliente conectividad de cualquiera a cualquiera y niveles de rendimiento diferenciados, priorización del tráfico sensible al retardo y no sensible al retardo, así como aplicaciones de voz y multimedia, todo ello en una única red.

"**Opciones de Servicio**" tiene el significado que se le da en el Apartado 2.2.

"**Plataforma Eagle-I**" se refiere a la solución a través de la cual BT identificará los COI.

Apartado 2.2.3.

"**Propiedad de BT**" es el modelo de entrega de BT Managed Firewall Security, en el que BT proporcionará, instalará y pondrá en servicio nuevos dispositivos de seguridad como equipos de BT, incluido cualquier hardware y software, acuerdos de licencia y asistencia para los dispositivos de seguridad, y se encargará de cualquier asistencia in situ y gestión remota del servicio, tal como se establece en el Apartado 2.1.1.

"**Propiedad del Cliente**" hace referencia al modelo de entrega de Seguridad de cortafuegos gestionada por BT en el que, por recomendación de BT, el Cliente solicitará nuevos Dispositivos de seguridad como Equipo del cliente y en el que BT se encargará de la asistencia in situ y de la gestión remota del servicio, tal y como se establece en el apartado 2.1.1.

"**Pruebas de Aceptación**" son las pruebas objetivas realizadas por el Cliente que, una vez superadas, confirman que el Cliente acepta que BT Managed Firewall Security está libre de fallos materiales y listo para su uso, salvo por alguna disconformidad menor, que se resolverá sin demoras indebidas tras la Fecha de Servicio Operativo.

"**Representante Designado**": persona de la organización del Cliente designada como punto de contacto para las notificaciones de vulnerabilidad.

"**Router**": dispositivo que reenvía paquetes de datos entre redes informáticas, creando una red interna superpuesta.

"**RTPC**" significa Red Telefónica Pública Conmutada, que es la concentración de las redes telefónicas públicas de conmutación de circuitos del mundo.

"**Servicio de Cortafuegos Mejorado de Eagle-I**" es la Opción de Servicio especificada en el Apartado 2.2.134.

"**Servicio de Detección y Prevención de Intrusiones Firewall**" significa la Opción de Servicio establecida en el

"**Servicio de Emulación de Amenazas**" se refiere a la Opción de Servicio establecida en el apartado 2.2.7.

"**Servicio de Cobertura**" tiene el significado que se le da en el Párrafo 2.1.1.

"**Servicio de Habilitación**" tiene el significado que se le da en el Apartado 4.1.2.

"**Servicio Resiliente**" significa un Servicio o parte de un Servicio, según lo establecido en el Pedido que está diseñado para tener alta disponibilidad y sin puntos únicos de fallo, de tal manera que si un componente falla el Servicio sigue estando disponible.

"**SSL**" significa capa de conexión segura.

"**Tiempo de Inactividad**" significa el periodo durante el cual existe(n) una(s) Incidencia(s) Cualificada(s).

"**Tráfico cifrado SSL**" se refiere al tráfico cifrado transferido a través de los siguientes protocolos que BT admitirá para la inspección SSL/TLS:

- (a) HTTPS;
- (b) SMTPS;
- (c) POP3S;
- (d) IMPAS; y
- (e) FTPS.

"**Túnel(es) IPSec**" significa una ruta de comunicación virtual estática o dinámica entre dos puntos finales que puede estar cifrada y tener diferentes niveles de autenticación para garantizar que el Cliente tenga una conectividad segura.



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

"VPN" significa una red privada virtual con el uso de cifrado para proporcionar una red de comunicaciones que parezca privada a los Usuarios del Cliente mientras se proporciona a través de una infraestructura de red que se comparte con otros clientes. A menos que se acuerde lo contrario por escrito, las comunicaciones del Cliente a través de la VPN del Cliente están restringidas a los Emplazamientos de la VPN del Cliente.

"Wide Area Network" o "WAN" significa la infraestructura que permite la transmisión de datos entre Sitios.

2 DESCRIPCIÓN DEL SERVICIO

BT Managed Firewall Security proporciona al Cliente un Servicio de cortafuegos gestionado ubicado en un Emplazamiento del Cliente o alojado en un Emplazamiento de BT. El Servicio controla el acceso entrante y saliente a Internet, realizando funciones que pueden incluir el control del tráfico entrante según excepciones controladas (cortafuegos), la gestión del acceso web saliente de los Usuarios según una política predefinida (filtrado de URL) y el análisis del tráfico para bloquear malware (antivirus). El Servicio se compone de varias "capas" con opciones según los requisitos del Cliente y se proporciona como un Servicio asociado con BT Managed Security Services, tal y como se establece en el Anexo de BT Managed Security. El Servicio y/o algunos de los componentes del Servicio pueden no estar disponibles en todas las ubicaciones. En tales circunstancias, las Partes podrán acordar por escrito que el Cliente organice -en su propio nombre o a través de un tercero- la prestación de los elementos del Servicio en las ubicaciones en las que BT no pueda suministrarlos, así como las condiciones aplicables para hacerlo.

Por el momento, BT Managed Firewall Security BT sólo está disponible con dispositivos de seguridad proporcionados por Fortinet Inc, proveedor de BT.

2.1 Componentes Estándar del Servicio

BT proporciona los siguientes elementos de Servicio estándar.

- 2.1.1 **Dispositivo de Seguridad.** El Cliente podrá elegir entre una gama de dispositivos de seguridad. Como alternativa, BT recomendará un dispositivo (o dispositivos) como parte del diseño general del servicio. El Cliente podrá solicitar el uso de Equipo del Cliente para el Servicio. La aceptación de dicha solicitud por parte de BT estará sujeta a la evaluación por parte de BT de que el Equipo del Cliente es adecuado para su uso con el Servicio y a la confirmación por escrito de BT de que BT puede prestar asistencia al Equipo del Cliente. El Cliente seleccionará uno de los siguientes modelos de entrega. La siguiente tabla establece las responsabilidades de las Partes en relación con el suministro y la gestión de los dispositivos de seguridad, otros equipos, la instalación, la puesta en servicio, los acuerdos de asistencia (incluido el software y las licencias), la gestión remota del servicio y la asistencia in situ, a menos que se especifique lo contrario en el Pedido:

Descripción	Propiedad de BT	Propiedad del Cliente	Adquisición de BT	Servicio de Cobertura
Dispositivo de Seguridad	BT (nuevo)	Cliente (nuevo)	Cliente (preexistente)	Cliente (nuevo)
Otros equipos (incluidos los de BT), incluidos el acceso fuera de banda y los conmutadores	BT (nuevo)	BT (nuevo)	BT (nuevo) o Cliente (preexistente) según se especifique	Cliente (nuevo)
Instalación	BT	BT	Cliente (preexistente)	Cliente
Puesta en servicio	BT	BT	Cliente (preexistente)	BT
Acuerdos de asistencia, software y licencias	BT	BT	BT	Cliente
Gestión remota de servicios	BT	BT	BT	BT
Asistencia in situ	BT	BT	el proveedor del Cliente; no obstante, BT presentará las solicitudes de asistencia necesarias en nombre del Cliente para cualquier fallo en el Equipo del Cliente que BT detecte.	el proveedor del Cliente; pero BT informará al Cliente de cualquier fallo en el Equipo del Cliente que BT detecte

- 2.1.2 **Licencias de Aplicaciones de Seguridad.** BT proporcionará una licencia de aplicación de seguridad adecuada (por ejemplo, para software de cortafuegos o filtrado de URL) como parte del Servicio.



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 2.1.3 **Entrega - Instalación Gestionada.** BT coordinará la instalación del Servicio y su puesta en servicio, actuando de enlace con el Cliente, los instaladores, los proveedores de equipos y los proveedores de red, según proceda (por ejemplo, en función de si se utiliza el Equipo de BT o el Equipo del Cliente) de acuerdo con el Nivel de Servicio solicitado por el Cliente, tal y como se establece en el Anexo BT Managed Security.
- 2.1.4 **Gestión de incidencias.** BT proporcionará un servicio de asistencia 24 horas al día, 7 días a la semana para responder a las averías, mantenimiento de equipos in situ respaldado por proveedores de aplicaciones y dispositivos, y supervisión continua del servicio en tiempo real. El nivel de Gestión de incidencias depende del Nivel de Servicio solicitado por el Cliente, tal y como se establece en el Anexo BT Managed Security.
- 2.1.5 **Supervisión proactiva.** BT supervisará el rendimiento de la seguridad del cortafuegos gestionado por BT tal y como se establece en el Anexo BT Managed Security.
- 2.1.6 **Información sobre Amenazas a la Seguridad.** BT proporcionará boletines e informes de información general para BT Managed Firewall Security, tal y como se establece en el Anexo BT Managed Security .
- 2.1.7 **Informes de Rendimiento del Servicio .** BT proporcionará informes casi en tiempo real o históricos de las principales métricas de rendimiento del Servicio y de los eventos relacionados con BT Managed Firewall Security, tal y como se establece en el Anexo BT Managed Security.
- 2.1.8 **Actualizaciones de Firmas.** BT identificará e implementará las Actualizaciones de Firmas en BT Managed Firewall Security, tal y como se establece en el Anexo BT Managed Security.
- 2.1.9 **Captura de Registros.** BT implementará una función de registro en BT Managed Firewall Security en función del Nivel de Servicio solicitado por el Cliente, tal y como se establece en el Anexo BT Managed Security.
- 2.1.10 **Gestión de Licencias y Acuerdos de Soporte de Proveedores.** BT se encargará de la gestión de los acuerdos de licencia y asistencia técnica para BT Managed Firewall Security, tal y como se establece en el Anexo BT Managed Security.
- 2.1.11 **Mejoras Continuas con Revisión.** BT proporcionará mejoras continuas con revisión en BT Managed Firewall Security en función del Nivel de Servicio según lo solicitado por el Cliente, tal y como se establece en el Anexo BT Managed Security.
- 2.1.12 **Gestión de vulnerabilidades y aplicación de parches a los dispositivos de seguridad.** BT se encargará de la gestión de vulnerabilidades y la aplicación de parches en BT Managed Firewall Security según el Nivel de Servicio solicitado por el Cliente, tal y como se establece en el Anexo de BT Managed Security.
- 2.1.13 **Cambios en el CSP.** BT proporcionará asistencia para los cambios en el CSP. El nivel de asistencia de BT para los cambios en el CSP dependerá del Nivel de Servicio solicitado por el Cliente, tal y como se establece en el Anexo BT Managed Security. En el caso de BT Managed Firewall Security, se aplicará además lo siguiente:

- 2.1.6.1 la siguiente cantidad de solicitudes de cambio por Dispositivo de Seguridad están incluidas en los Cargos:

Tipo de cambio	Foundation	Foundation Plus	Premium
Cambio Estándar	seis al mes	ocho al mes	diez al mes
Cambio Urgente	uno al mes	dos al mes	tres al mes

- 2.1.6.2 el Cliente solicitará por separado cualquier cambio en el Servicio que sea necesario y que implique cambios físicos en el Servicio, incluidas las actualizaciones de los Dispositivos de Seguridad y las reorganizaciones de LAN;

- 2.1.6.3 No se incluyen los cambios que requieran hardware adicional, licencias o cambios en los Cargos (incluidos los cambios en los Cargos recurrentes en curso) o cuando sea necesario redefinir la solución. El Cliente:

- podrá solicitar a los Servicios Profesionales de BT que asesoren al Cliente sobre lo que necesita exactamente; y
- Acordará los cambios necesarios emitiendo un nuevo Pedido.

2.2 Opciones de Servicio

Las siguientes Opciones de Servicio pueden estar disponibles sujetas a Cargos y condiciones adicionales, tal y como se establece en el Pedido. Es posible que no todos los proveedores de Dispositivos de Seguridad ofrezcan todas las Opciones de Servicio.

2.2.1 VPNs.



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (a) BT instalará y configurará los siguientes tipos de VPN de acuerdo con las normas técnicas vigentes de BT:
 - (i) acceso remoto IP Sec/SSL VPN, para que los Usuarios remotos obtengan acceso seguro a la red interna del Cliente. BT implementará las reglas del Cliente para autenticar contra el servidor de autenticación del Cliente. El Cliente es responsable de proporcionar y gestionar su propio software VPN de usuario final;
 - (ii) VPN IP Sec de sitio a sitio entre dos Dispositivos de Seguridad propiedad del Cliente y gestionados por BT; y
 - (iii) VPN IP Sec de terceros (extranet), para crear una VPN de sitio a sitio entre el dispositivo de seguridad del cliente gestionado por BT y un dispositivo de seguridad propiedad del cliente o de un tercero o gestionado por ellos. BT solo proporcionará VPN a Security Appliances gestionados por terceros después de la Fecha de servicio operativa.
- (b) Cuando el Cliente proporcione el certificado digital a BT, según lo establecido en el Pedido:
 - (i) BT lo instalará en un plazo de siete días a partir de la recepción del Cliente.
 - (ii) BT notificará al Cliente la fecha de expiración del certificado digital tres meses antes de la fecha de expiración. El Cliente comunicará por escrito a BT, en el plazo de un mes a partir de la fecha de la notificación de BT, si desea o no renovar su certificado digital;
 - (iii) si el Cliente desea renovar su certificado digital, el Cliente proporcionará el nuevo certificado digital a BT al menos siete días antes de la expiración del certificado digital original; y
 - (iv) BT no será responsable de los problemas causados por certificados digitales caducados si el Cliente no confirma a BT que desea renovar su certificado digital en; o el Cliente no proporciona a BT un certificado digital actualizado.

2.2.2 **Zonas Desmilitarizadas (DMZ).** BT proporcionará interfaces de segmento LAN adicionales en el dispositivo de seguridad o en un conmutador de red adyacente, según los requisitos del Cliente. Esto está sujeto a que haya suficientes puertos físicos disponibles y se aplicarán cargos adicionales si se requiere hardware adicional para proporcionar la interfaz.

2.2.3 Servicio de Detección y Prevención de Intrusiones (IPS) del Cortafuegos:

- (a) BT:
 - (i) supervisará el tráfico que pasa por el Dispositivo de Seguridad del Cliente en busca de ataques, de conformidad con los archivos de firmas de intrusión aplicables;
 - (ii) implementará esta Opción de Servicio con una configuración por defecto. BT también mantendrá una suscripción a las actualizaciones de firmas necesarias y se encargará de que se apliquen una vez emitidas por el proveedor, pero no será responsable de evaluar estas firmas de antemano;
 - (iii) no será responsable de evaluar previamente estas firmas.
- (b) BT informará al Cliente sobre el funcionamiento del IPS que haya seleccionado en relación con las alertas o los informes específicos del IPS;
- (c) Si BT acepta una solicitud del Cliente de modificar los parámetros de aplicación de nuevas firmas en modo "bloqueo", para dar una mayor o menor sensibilidad a los ataques, el Cliente acepta la responsabilidad por el mayor riesgo de falsos positivos (bloqueos a tráfico legítimo) o el mayor riesgo de que se pasen por alto ataques.

2.2.4 Filtrado de URL del Cortafuegos y Control de Aplicaciones:

- (a) BT:
 - (i) bloqueará el acceso a aquellas URL que el Cliente solicite a BT, de conformidad con el CSP. Los sitios de Internet se organizan en grupos que se actualizan periódicamente. El Cliente puede optar por bloquear o restringir el acceso a alguno o a todos los grupos;
 - (ii) enviará un mensaje apropiado a un usuario que intente acceder a un sitio bloqueado o restringido para advertirle de lo siguiente:
 - i. que la solicitud del Usuario ha sido bloqueada; o
 - ii. que el Usuario confirme primero la aceptación de la política de uso aceptable del Cliente (o advertencia similar). Una vez aceptada, se entregará la página; y
 - (iii) aplicará las modificaciones necesarias mediante el proceso estándar de gestión de la configuración en caso de que se produzca algún cambio en el CSP.



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (b) Esta Opción de Servicio no incluye la elaboración de informes de forma estándar. La generación de informes está disponible si el cliente ha solicitado la opción de generación de informes de eventos de seguridad, tal y como se establece en el Apartado 2.2.8.

2.2.5 Cortafuegos Antivirus:

- (a) BT:
 - (i) comprobará el tráfico del navegador web (http) en busca de malware conocido;
 - (ii) inspeccionará las solicitudes de los Usuarios de un archivo ejecutable de un sitio en Internet, contra el archivo de definición antivirus actual. Si no se detecta ningún virus, el archivo se pasará al usuario. Si se detecta un virus, el archivo se bloqueará y se eliminará.
 - (iii) mantendrá actualizados los archivos de definición del antivirus mediante descargas periódicas directas del Servicio antivirus.
- (b) La prestación de esta Opción de Servicio está sujeta a un tamaño máximo de archivo y a límites de archivo comprimido, en función del Dispositivo de Seguridad seleccionado.
- (c) Esta Opción de Servicio no incluye la elaboración de informes de forma estándar. La generación de informes está disponible si el Cliente ha solicitado la opción de generación de informes de eventos de seguridad, tal y como se establece en el Apartado 2.2.8.

2.2.6 Servicio Firewall Anti-Bot:

- (a) BT comprobará y bloqueará el tráfico saliente en busca de comunicaciones con servidores conocidos de "**comando y control**" utilizados por propietarios de software malicioso.
- (b) Esta Opción de Servicio no incluye informes de serie. Los informes pueden estar disponibles como opción en función del Dispositivo de Seguridad utilizado.

2.2.7 Servicio Adicional de Emulación de Amenazas (sólo disponible con el Nivel de Servicio Premium):

- (a) BT cifrará los archivos sospechosos de ser maliciosos y los enviará a la infraestructura basada en la nube del proveedor, donde serán descifrados y analizados en busca de malware mediante la revisión de su comportamiento en un entorno virtual (sandbox).
- (b) Dependiendo del Dispositivo de Seguridad que seleccione el cliente, éste podrá elegir entre retener el archivo mientras se analiza (para aumentar la seguridad) o liberarlo y analizarlo en segundo plano (para mejorar la respuesta del Usuario). El procesamiento en segundo plano puede dar lugar a que se permitan archivos maliciosos hasta que se generen posteriormente actualizaciones de firmas y se apliquen a los Dispositivos de Seguridad del Cliente.
- (c) Si un archivo se considera malicioso, sus características se añadirán a la lista de firmas antivirus del proveedor.
- (d) BT determinará el país en el que se realiza esta inspección y análisis.
- (e) Si el Cliente necesita que el Servicio le proteja contra malware contenido en archivos adjuntos SMTP (correo electrónico), el Cliente dispondrá que los registros de intercambio de correo DNS del Cliente se redirijan al Dispositivo de Seguridad para que el correo electrónico se entregue a dicho Dispositivo de Seguridad. BT configurará el Dispositivo de Seguridad para que envíe el correo electrónico al servidor de correo electrónico del Cliente.
- (f) El envío y procesamiento de los datos del Cliente a través del Servicio de Emulación de Amenazas se realizarán a discreción del Cliente y por su cuenta y riesgo. Aparte de las obligaciones de BT establecidas en las Condiciones Generales, BT no asume responsabilidad alguna por la recepción y el tratamiento de dichos datos.

2.2.8 Notificación de Sucesos de Seguridad:

- (a) BT proporcionará servicios de generación de informes, ya sea en línea o en un servidor alojado en el Emplazamiento del Cliente, que permitan analizar los sucesos relacionados con la seguridad, pero no visualizará de forma proactiva los informes y sucesos del Cliente para detectar incidentes de seguridad.
- (b) Si esta Opción de Servicio se presta a través de una plataforma de informes compartida, BT configurará la plataforma de modo que el Cliente sólo tenga acceso a los informes del Cliente. Esto puede significar que algunas de las funciones de la plataforma estén restringidas para preservar la confidencialidad de todos los clientes que utilicen dicha plataforma.
- (c) El periodo durante el cual pueden analizarse los datos depende de la capacidad de los Dispositivos de Seguridad o del espacio asignado en la plataforma de elaboración de informes.

2.2.9 Inspección SSL/TLS



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (a) BT interceptará y descifrá el tráfico cifrado SSL para llevar a cabo la inspección de acuerdo con el CSP. Una vez inspeccionado el tráfico, se volverá a cifrar y se retransmitirá a su destino original (si lo permite el CSP).
- (b) BT no interceptará ni descifrá el tráfico cifrado SSL para todas las categorías de contenido web debido a la elevada posibilidad de que surjan problemas con las aplicaciones asociadas a determinados sitios web, por ejemplo, algunos sitios web pueden no permitir el descifrado.
- (c) Si se selecciona la opción de servicio de inspección SSL/TLS, BT podrá analizar el tráfico cifrado SSL del mismo modo que el tráfico no cifrado, siempre que el CSP del cliente permita dicho análisis.

2.2.10 Conciencia de Identidad / Grupos de Usuarios:

- (a) BT configurará las funciones del Dispositivo de Seguridad compatibles con la Opción de Servicio Conciencia de Identidad para aplicar determinadas reglas del CSP en función de la identidad autenticada del Usuario y no sólo de su dirección IP.
- (b) Para ello, puede ser necesario instalar el Software cliente en la red del Cliente o en los dispositivos de los usuarios finales, o asegurarse de que BT tenga acceso remoto, de sólo lectura, al servidor de autenticación del directorio activo del Cliente.
- (c) El Cliente mantendrá la base de datos de autenticación de Usuarios, grupos y cualquier credencial de acceso que el Cliente requiera.

2.2.11 Soluciones de Alta Disponibilidad (doble dispositivo):

- (a) BT configurará un par de Dispositivos de Seguridad en un único emplazamiento para aumentar la resistencia frente a fallos.
- (b) Cada Dispositivo de Seguridad puede conectarse a un circuito de Internet independiente para proporcionar una mayor capacidad de recuperación, tal y como se establece en el Pedido.
- (c) Esta Opción de Servicio requerirá que se incluyan conmutadores adicionales como parte de la solución, que serán proporcionados por BT o por el Cliente según lo establecido en el Apartado 2.1.1. Si es responsabilidad del Cliente proporcionar los conmutadores adicionales, BT informará al Cliente del número y tipo de conmutadores necesarios.
- (d) Dependiendo de los Dispositivos de Seguridad utilizados y del CSP, BT puede configurar los Dispositivos de Seguridad como "**Activo Activo**" (ambos Dispositivos de Seguridad comparten la carga en condiciones normales) o "**Activo Pasivo**" (un Dispositivo de Seguridad gestiona la carga en condiciones normales, con conmutación por error a un Dispositivo de Seguridad secundario en caso de que falle el principal).
- (e) Para configuraciones "**Activas Activas**", el rendimiento puede reducirse en condiciones de fallo a menos que cada Dispositivo de Seguridad tenga capacidad para gestionar toda la carga de forma independiente.

2.2.12 **Asistencia técnica ad hoc / Servicio Profesional** . El Cliente podrá solicitar Servicios Profesionales a BT según lo establecido en el Anexo de Servicios BT Manage Security.

2.2.13 Servicio de Cortafuegos Mejorado Eagle-I

BT proporcionará al Cliente el Servicio Eagle-I Enhanced Firewall, sujeto a los requisitos establecidos a continuación.

- (a) Mejora de la lista de bloqueo existente
 - (i) Siempre que BT confirme que el Dispositivo de Seguridad del Cliente es apto para su uso con el Servicio de Cortafuegos Mejorado Eagle-I, BT utilizará su plataforma Eagle-I para identificar cualquier IP o URL maliciosa única con el fin de complementar la lista de bloqueo de IP o URL maliciosas del Dispositivo de Seguridad del Cliente ("Indicadores de Compromiso" o "IOC").
 - (ii) Una vez confirmada la idoneidad del Dispositivo de Seguridad del Cliente, BT añadirá nuevos IOC a la lista de bloqueo de BT para su consumo por parte del Dispositivo de Seguridad del Cliente ("Mejora de la Lista de Bloqueo Existente").
- (b) Bloqueo Automático de COI
 - (i) Sujeto a que BT confirme la viabilidad técnica de aplicar el bloqueo automatizado de COI al Dispositivo de Seguridad del Cliente, como parte de su gestión de servicios remotos del Dispositivo de Seguridad del Cliente, BT implementará automáticamente cambios en el Dispositivo de Seguridad del Cliente para que bloquee los COI propagados desde la lista de bloqueo de BT ("Bloqueo Automatizado de COI").
 - (ii) Para evitar cualquier duda, cuando se especifique el Servicio de Cortafuegos Mejorado Eagle-I, sujeto a los requisitos de viabilidad técnica (como se indica en el Apartado 2.2.14(b)(i)), BT aplicará el bloqueo automático de COI. Al especificar el Servicio de



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- Cortafuegos Mejorado de Eagle-I, el Cliente consiente por la presente que BT implemente el bloqueo de IOC automatizado con respecto al Dispositivo de Seguridad del Cliente.
- (iii) BT no será responsable de ningún impacto más amplio de cualquier Bloqueo Automatizado de COI, incluido, entre otros, cualquier impacto del Bloqueo Automatizado de COI en el Equipo del Cliente o en la red más amplia del Cliente.

3 RESPONSABILIDADES DE BT

Además de cualesquiera otras obligaciones de BT establecidas en el Contrato:

3.1 **Requisitos previos.** Durante la prestación del Servicio, BT:

- 3.1.1 facilitar al Cliente los datos de contacto del Service Desk;
- 3.1.2 cumplir todas las normas y reglamentos de salud y seguridad razonables, así como los requisitos de seguridad razonables que se apliquen en el/los Emplazamiento(s) y que el Cliente haya notificado a BT por escrito, siempre y cuando dicho cumplimiento por parte de BT no suponga el incumplimiento por parte de BT de ninguna de sus obligaciones en virtud del presente Contrato.

3.2 **Prestación de Servicios**

Antes de la Fecha de Servicio Operativo y, en su caso, durante toda la prestación del Servicio, BT :

- 3.2.1 proporcionará al Cliente una fecha de entrega objetivo que, si el Cliente ha pedido Foundation Plus o Premium, será la Fecha Comprometida del Cliente a efectos de medir el Nivel de Servicio de Entrega a Tiempo;
- 3.2.2 cuando proceda, organizar la realización de cualquier estudio para confirmar la disponibilidad de un entorno adecuado para la prestación del Servicio (incluida la confirmación de la presencia de Servicios de Habilitación);
- 3.2.3 instalará, o se encargará de que terceros proveedores instalen en nombre de BT, los Dispositivos de Seguridad en un Emplazamiento de la siguiente manera:
- (a) si el Cliente elige el modelo de entrega Propiedad de BT, BT proporcionará, instalará y pondrá en servicio cualquier Equipo de BT, incluido cualquier hardware y software, acuerdos de licencia y asistencia para el Dispositivo de Seguridad y se encargará de cualquier asistencia in situ y gestión remota del Servicio; y
 - (b) si el Cliente elige el modelo de entrega Propiedad del Cliente, BT instalará y pondrá en servicio dicho Equipo del Cliente, incluidos el hardware y el software, las licencias y los acuerdos de asistencia para el Dispositivo de Seguridad según las especificaciones de BT, y proporcionará asistencia in situ y gestión remota del servicio;
- 3.2.4 proporcionar al Cliente la Guía de Planificación del Emplazamiento;
- 3.2.5 designar a un representante para que sea el único punto de contacto del Cliente para la prestación del Servicio; y

3.3 **Puesta en Marcha del Servicio** . Antes de la Fecha de Servicio Operativo, BT:

- 3.3.1 se pondrá en contacto con el Cliente y acordará la(s) fecha(s) de instalación, incluido el acceso de terceros instaladores;
- 3.3.2 una vez instalados los Dispositivos de Seguridad, BT configurará el Servicio BT a distancia según el CSP;
- 3.3.3 desplegará y configurará la(s) Opción(es) de Servicio seleccionada(s) por el Cliente;
- 3.3.4 realizará una serie de pruebas estándar en el Servicio para garantizar que está configurado correctamente; y
- 3.3.5 en la fecha en que BT haya completado las actividades del presente Apartado 3.3, confirmará al Cliente que el Servicio está disponible para la realización de las Pruebas de Aceptación. La Fecha de Servicio Operativo se produce cuando BT ha configurado y puesto en marcha el Servicio, a menos que el Cliente retrase la puesta en servicio por cualquier motivo, en cuyo caso la Fecha de Servicio Operativo se produce en la fecha de instalación de los aparatos.

3.4 **Durante el funcionamiento.** A partir de la Fecha de Servicio Operativo, BT:

- 3.4.1 durante un periodo de cinco (5) Días Hábiles tras la Fecha de Servicio Operativo, implementará cualquier Cambio Simple o corrección en el CSP que pueda ser necesario para el funcionamiento del Servicio. BT implementará dichos Cambios Simples tan pronto como sea razonablemente factible y, por lo general, implicarán cambios en líneas individuales de puerto/protocolo, enrutamiento o traducción de direcciones de red. Cualquier Cambio Complejo del CSP no incurrirá en Cargos adicionales según lo acordado en un Pedido y podrá programarse para su implementación tras este periodo de cinco (5) Días Hábiles;



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 3.4.2 si el Cliente elige el modelo de prestación Propiedad de BT, Propiedad del Cliente o Adquisición de BT, gestionará el mantenimiento, la supervisión y la configuración continuos del Equipo de BT o del Equipo del Cliente durante la vigencia del Servicio. Además, a menos que se acuerde específicamente lo contrario, BT podrá instalar Equipos de BT adicionales en el Emplazamiento del Cliente, con el fin de supervisar y gestionar el Servicio de BT;
- 3.4.3 si el Cliente elige cualquiera de los modelos de prestación Propiedad de BT, Propiedad del Cliente o Adquisición de BT, será responsable de garantizar que las licencias de software y los contratos de asistencia necesarios se renueven durante la vigencia del presente Contrato. A menos que el Cliente notifique por escrito a BT su intención de rescindir el Servicio 90 días antes de que finalice el periodo de vigencia de la licencia de software, BT prorrogará las licencias de software y los contratos de asistencia necesarios durante otros doce (12) meses;
- 3.4.4 utilizará protocolos seguros o proporcionará un enlace de gestión seguro para conectarse al Dispositivo de Seguridad a través de Internet u otra conexión de red acordada, con el fin de supervisar el Servicio de forma proactiva y ayudar en el diagnóstico de Incidencias;
- 3.4.5 proporcionará un enlace de acceso fuera de banda que se conectará directamente al/los Dispositivo/s de Seguridad a través de un módem proporcionado por BT y una línea de intercambio directo RTC proporcionada por el Cliente para permitir una mayor capacidad de diagnóstico y gestión remota;
- 3.4.6 responderá y solucionará cualquier incidencia notificada por el Cliente según lo establecido en el Anexo de Servicio BT Managed Security. Para cualquiera de los modelos de entrega Propiedad de BT, Propiedad del Cliente o Adquisición de BT, BT proporciona una respuesta de mantenimiento in situ 24x7x365 cuando esté disponible localmente. Cuando este nivel de cobertura no esté disponible, se proporcionará asistencia in situ entre las 08:00 y las 17:00 horas, de lunes a viernes, excepto los días festivos locales del país correspondiente;
- 3.4.7 notificará al Cliente si BT prevé que el hardware o software del Cliente llegará al final de su vida útil y, como consecuencia, dejará de recibir asistencia por parte de BT en virtud de este Servicio. Como parte de esta notificación, BT recomendará al Cliente los detalles de cualquier sustitución o actualización necesaria del hardware o software aplicable, los plazos respectivos y los costes previstos;
- 3.4.8 cuando el Cliente seleccione el modelo de entrega Propiedad de BT o Adquisición de BT, realizará cualquier cambio (sustitución o actualización) en el hardware y/o Software durante el Periodo Mínimo de Servicio para evitar que el hardware y el Software lleguen al Final de su Vida Útil; y
- 3.4.9 cuando el Cliente haya seleccionado la Mitigación Cooperativa con el Nivel de Servicio Premium, aplicará la Acción de Mitigación tan pronto como sea técnicamente posible.
- 3.5 **Finalización del Servicio.** A la finalización del Servicio por cualquiera de las Partes, BT:
- 3.5.1 pondrá fin a cualquier derecho de acceso al Portal de seguridad de BT y al Software correspondiente y dejará de prestar todos los demás elementos del Servicio;
- 3.5.2 desconectará y retirará cualquier Equipo BT situado en los Emplazamientos;
- 3.5.3 eliminará cualquier Contenido; y
- 3.5.4 cuando lo solicite el Cliente, proporcionará, siempre que sea razonablemente práctico, información de configuración relativa al Servicio prestado en el/los Emplazamiento(s) en un formato que BT especifique, siempre que el Cliente haya abonado, en ese momento, todos los Cargos pendientes en el momento de la rescisión y resultantes de la misma (tanto si se adeudaban en la fecha de rescisión como si no).
- 3.6 Límite de Gestión del Servicio (SMB) y exclusiones.**
- 3.6.1 BT proporcionará y gestionará la seguridad del BT Managed Firewall Security según lo establecido en este Anexo y en el Anexo BT Managed Security hasta:
- (a) el lado Internet/WAN: el cable que conecta el cortafuegos al router del Cliente;
 - (b) el lado LAN: el puerto o puertos Ethernet del cortafuegos o el conmutador proporcionado por BT; y/o
 - (c) la línea telefónica analógica: el cable que conecta el módem suministrado por BT a la toma RTC,
- 3.6.2 BT no tendrá responsabilidad alguna por el Servicio fuera de los Límites de Gestión del Servicio, incluyendo:
- (a) problemas en los equipos de los Usuarios, software de proveedores de descarga gratuita no proporcionado por BT o servidores del Cliente (por ejemplo, sistema operativo, lenguajes de codificación y configuración de seguridad);
 - (b) conectividad de red de extremo a extremo (por ejemplo, la red del Cliente o la conectividad a Internet); o
 - (c) gestionar las identidades de los Usuarios.
- 3.6.3 BT no hace ninguna declaración, ya sea expresa o implícita,



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (a) sobre si el Servicio funcionará en combinación con cualquier Equipo del Cliente u otro equipo y software; o
 - (b) en cuanto a cualquier resultado del Bloqueo IOC Automatizado llevado a cabo como parte de la Opción de Servicio de Cortafuegos Mejorado de Eagle-I, incluyendo, pero sin limitarse a, cualquier reducción en Incidencias de seguridad o al impacto de amenazas en cualquier Equipo del Cliente o en la red más amplia del Cliente.
- 3.6.4 sobre si el Servicio funcionará en combinación con cualquier Equipo del Cliente u otro equipo y software.
- 3.6.5 BT no será responsable si no puede prestar el Servicio por falta de capacidad en los Dispositivos de Seguridad seleccionados por el Cliente.
- 3.6.6 BT no puede garantizar a) que el Servicio funcione sin Incidencias o interrupciones o que intercepte o desactive todos los programas maliciosos y b) la seguridad del Servicio frente a accesos o usos no autorizados o ilegales.
- 3.6.7 BT prestará el Servicio al Cliente "tal cual" y "según disponibilidad". BT no garantiza que el Servicio:
- (a) se realizará sin errores ni interrupciones o que BT corregirá todos los errores del Servicio;
 - (b) funcionará en combinación con los contenidos o aplicaciones del Cliente o con cualquier otro software, hardware, sistemas o datos;
 - (c) incluyendo cualquier producto, información u otro material que el Cliente obtenga en virtud de este Contrato o en relación con el mismo, satisfará los requisitos del Cliente; y
 - (d) detectará o bloqueará todas las amenazas maliciosas;
- 3.6.8 BT no será responsable en caso de que las actualizaciones de Software del proveedor utilizadas para identificar y controlar el tráfico de red del Cliente (incluidas firmas de malware, categorías de URL o definiciones de aplicaciones) contengan errores u omisiones, más allá de realizar las correcciones oportunas (siempre que sea razonablemente posible) tan pronto como sea razonablemente práctico;
- 3.6.9 Excepto si se indica explícitamente que forma parte de las responsabilidades de BT según lo establecido en este Apartado 3, BT no será responsable cuando el hardware y/o Software llegue al Final de su vida útil y el Cliente no haya sustituido o actualizado el hardware y/o Software respectivo de acuerdo con la recomendación de BT según lo establecido en el Apartado 3.4.12. En tal caso:
- (a) BT ya no podrá proporcionar al Cliente asistencia completa para dicho hardware y/o software al final de su vida útil y el Cliente recibirá un Servicio limitado; y
 - (b) dejarán de aplicarse los Niveles de Servicio;
- 3.6.10 El Cliente poseerá todos los derechos, títulos e intereses sobre toda la información del Cliente y será el único responsable de la legalidad, fiabilidad, integridad, exactitud y calidad de cualquier información del Cliente; y
- 3.6.11 El Cliente será responsable de los resultados obtenidos del uso del Servicio y de las conclusiones extraídas de dicho uso. BT no será responsable de ningún daño causado por errores u omisiones en la información, instrucciones o guiones proporcionados a BT por el Cliente en relación con el Servicio, ni de ninguna acción realizada por BT siguiendo las instrucciones del Cliente.
- 3.6.12 Aunque el Servicio Eagle-i (si se selecciona como parte del Pedido) tiene como objetivo reducir significativamente el impacto de las amenazas en el dispositivo de punto final o las Identidades de usuario final identificadas a BT, BT no hace ninguna declaración ni ofrece ninguna garantía, ya sea expresa o implícita, de que se mitigarán todas las amenazas.
- 3.6.13 Cuando el Cliente seleccione la Mitigación Cooperativa con Nivel de servicio Premium, la responsabilidad de BT se limitará a proporcionar Mitigación Cooperativa en Dispositivos de punto final o Identidades de usuario final distintos de los identificados para ser excluidos por BT, y BT no será responsable de ningún impacto en otros Dispositivos de punto final excluidos ni en ningún otro Equipo propiedad del Cliente o de la red más amplia del Cliente. Si el Cliente ha seleccionado que desea aprobar cada Acción de Mitigación, BT solo aplicará esta Acción de Mitigación una vez que el Cliente haya dado dicha aprobación.

4 RESPONSABILIDADES DEL CLIENTE

4.1 Requisitos previos

4.1.1 Servicio de Habilitación

- 4.1.1.1 El Cliente dispondrá de los siguientes Servicios de Habilitación necesarios para el funcionamiento del Servicio y se asegurará de que dichos Servicios de Habilitación cumplen los requisitos proporcionados por BT en la contratación:

- (a) Conexión a Internet;



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (b) Conectividad WAN;
- (c) Línea conmutada directa RTC, para permitir la gestión del Acceso Fuera de Banda;
- (d) Conectividad LAN/DMZ e infraestructura asociada;
- (e) Conectividad RTPC; y
- (f) entorno informático más amplio, incluidos los dispositivos de seguridad cuando sean responsabilidad del Cliente, incluidos los servicios de autenticación, los conmutadores adicionales cuando sean necesarios, las plataformas de servidor/cliente y las soluciones de gestión de Incidencias y eventos de seguridad (SIEM),

4.1.1.2 Si BT proporciona al Cliente otros servicios distintos del Servicio (incluido, entre otros, cualquier Servicio de Habilitación), el presente Anexo no se aplicará a dichos servicios, que se regirán por sus propias condiciones.

4.1.2 Importación y Exportación

4.1.2.1 El Servicio incluye componentes sujetos a control de exportación, tal y como se establece en las Condiciones Generales. Esto se aplica específicamente a los países en los que el uso y la importación de software y dispositivos de cifrado pueden estar restringidos por la legislación y la normativa locales, o en los que la exportación y reexportación del software o los dispositivos de cifrado pueden estar sujetos a la legislación de control de exportaciones de los Estados Unidos de América. El incumplimiento de estas condiciones de control de las exportaciones se considerará una infracción grave de conformidad con las Condiciones Generales.

4.1.2.2 Si se acuerda prestar la totalidad o parte del Servicio utilizando Equipos de BT, BT prestará el Servicio teniendo debidamente en cuenta la legislación local del país. Esto incluye la obtención (si es necesario) de licencias locales de importación y exportación y la autorización por escrito de todas las autoridades respectivas. En los países en los que se apliquen licencias de usuario, el Cliente acepta que es responsable de cumplir todos los requisitos normativos y de concesión de licencias aplicables para el uso del Servicio, incluidos, entre otros, la legislación y la normativa locales aplicables a la exportación y reexportación de cualquier software o dispositivo de cifrado. BT se reserva el derecho a exigir al Cliente que presente pruebas del cumplimiento de dichos requisitos normativos y de concesión de licencias antes de la prestación del Servicio. Si el Cliente no puede presentar dicha prueba, BT se reserva el derecho de suspender la prestación del Servicio o cancelar el Pedido. Si BT cancela el Pedido, se aplicarán las disposiciones relativas a la cancelación establecidas en las Condiciones Generales. El Cliente es responsable de obtener cualquier licencia de usuario local y la autorización por escrito de todas las autoridades respectivas que sean necesarias.

4.1.2.3 Si se acuerda prestar la totalidad o parte del Servicio utilizando el Equipo del Cliente, para lo cual el Cliente ha organizado la conexión, ya sea por su cuenta o a través de un tercero, desde ubicaciones en las que BT no puede prestar el Servicio, el Cliente es responsable de garantizar el cumplimiento de todas las leyes y normativas aplicables, incluida la obtención (si es necesaria) de licencias locales de importación, exportación y uso, así como la autorización por escrito de todas las autoridades respectivas sin coste alguno para BT.

4.1.3 Obligaciones al solicitar la Mitigación Cooperativa.

4.1.3.1 cuando el Cliente solicite la opción de Mitigación Cooperativa con Niveles de Servicio Premium; el Cliente deberá:

- (a) acordar en la Orden que BT está autorizada a no tomar Medidas de Mitigación en relación con controles de seguridad específicos y, en su caso, con dispositivos de punto final o Identidades de usuario final específicos;
- (b) seleccionar en el Pedido si se hace de forma automática o sujeta a la aprobación del Cliente; y
- (c) proporcionar de forma segura a BT las credenciales de acceso necesarias a las plataformas que utiliza el Cliente para realizar cambios de política en los puntos finales o las Identidades de usuario final que requieren Mitigación Cooperativa y notificar a BT cualquier cambio posterior en dichas credenciales.

4.2 Prestación del Servicio

Antes de la Fecha de Servicio Operativo y, en su caso, durante toda la prestación del Servicio; el Cliente será responsable de lo siguiente:

4.2.1 **Información.** El Cliente proporcionará cualquier información o acceso que BT solicite sin demora indebida. Esto incluye:



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 4.2.1.1 los datos de contacto del cliente;
- 4.2.1.2 todas las normas y reglamentos de salud y seguridad y los requisitos de seguridad que se apliquen en un centro;
- 4.2.1.3 el nombre y los datos de contacto de un Representante designado responsable de la comunicación con BT en relación con la Opción de Servicio de notificación de vulnerabilidades y aplicación de parches. El Cliente informará a BT si el Representante designado cambia y se asegurará de que BT dispone de los datos actuales del Representante designado. El Cliente se asegurará de que el Representante designado:
 - (a) solicite la aplicación de parches para cada Dispositivo de Seguridad afectado para la Opción de Servicio de notificación de vulnerabilidades y aplicación de parches;
 - (b) acuerde con BT una franja horaria para la aplicación de dichos Parches;
 - (c) evalúe la idoneidad para la implantación de los parches que BT indique que están disponibles para abordar las vulnerabilidades notificadas en los entornos específicos del Cliente y para cualquier prueba posterior a la implantación; y
 - (d) solicite y autorice que se anule el parche en caso de que éste introduzca problemas.
- 4.2.1.4 acceso al Emplazamiento durante el Horario Comercial, o según se acuerde, para permitir a BT configurar, prestar y gestionar el Servicio;
- 4.2.1.5 cuando el Cliente haya seleccionado un modelo de Adquisición de BT y el Cliente esté realizando la transición de los servicios existentes del Cliente a BT, el Cliente proporcionará a acceso de gestión remota a los Equipos del Cliente y una lista de inventario con información relativa a los Equipos del Cliente que vayan a ser objeto de transición con las especificaciones pertinentes, incluyendo:
 - (a) marca y modelo del Equipo del Cliente, y cualquier componente opcional de hardware o software;
 - (b) ubicación del Equipo del Cliente;
 - (c) números de serie;
 - (d) versiones de software e información sobre licencias;
 - (e) diagramas de red;
 - (f) nombre del Equipo del Cliente y direccionamiento IP;
 - (g) detalles de cualquier contrato con terceros, acuerdos de nivel de servicio y equipos; y
 - (h) datos de los CSP existentes del Cliente;

Cualquier cambio en el inventario facilitado se hará mediante acuerdo por escrito; en el que las Partes se pondrán de acuerdo:

 - (a) los respectivos cambios en el inventario;
 - (b) ya que los cambios en el inventario pueden causar retrasos en la transición del servicio del Cliente o en la Fecha de Servicio Operativo; si procede, una nueva fecha de entrega; y
 - (c) Dado que los cambios pueden dar lugar a una modificación de los Cargos para reflejar el alcance revisado del Servicio BT, si procede, cualquier nuevo Cargo.
- 4.2.2 **Preparación.** El Cliente completará todas las actividades de preparación que BT pueda solicitar para que el Cliente pueda recibir el Servicio con prontitud y de acuerdo con los plazos razonables. Esto incluye:
 - 4.2.2.1 **Guía de planificación del Emplazamiento;** dado que el Cliente recibirá una guía de planificación del Emplazamiento con información detallada sobre los requisitos medioambientales y las guías de dimensionamiento de los equipos suministrados por BT, es responsabilidad del Cliente asegurarse de que el Emplazamiento cumple con esta guía antes de la instalación del Servicio. Cualquier defecto dará lugar a un retraso en la fecha de entrega y no se aplicarán los Niveles de Servicio.
 - 4.2.2.2 **Cooperación con las inspecciones** organizadas por BT según lo establecido en el Apartado 3.2.2. En caso de que el Cliente no coopere con dichas inspecciones, es posible que se modifique la Fecha comprometida del Cliente y que se apliquen Cargos por una visita a las instalaciones cancelada. En tal caso, BT proporcionará un nuevo presupuesto al Cliente, detallando los Cargos adicionales que el Cliente deberá pagar por el trabajo adicional que deba completarse y una nueva Fecha comprometida del Cliente propuesta. Cuando el Cliente:
 - (a) acepte el nuevo presupuesto, BT cancelará el Pedido existente para el/los Emplazamiento(s) afectado(s) y generará un nuevo Pedido para el/los Emplazamiento(s) afectado(s); o bien modificará el Pedido existente para reflejar los nuevos requisitos.
 - (b) no acepte el nuevo presupuesto o el Cliente no de instrucciones a BT para que proceda con el Pedido existente, BT cancelará el Pedido existente del Cliente para la prestación del



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

Servicio al Sitio o Sitios afectados según lo establecido en las Condiciones Generales y BT no tendrá obligación de prestar el Servicio a dicho Emplazamiento.

- 4.2.2.3 **trabajos adicionales;** cuando los estudios de BT según lo establecido en el Apartado 3.2.2 identifiquen que el Cliente debe realizar trabajos adicionales para proporcionar un entorno adecuado, completar estos trabajos antes de la instalación del Servicio;
- 4.2.2.4 **aspectos de compatibilidad;** en los que el Cliente se asegurará de que los protocolos LAN y las aplicaciones que utilice el Cliente sean compatibles con el Servicio, se ajusten a las normas pertinentes del sector, el ancho de banda del circuito de acceso MPLS/Internet del Cliente sea suficiente para satisfacer los requisitos del Cliente y el requisito de acceso de gestión en banda de BT. El Cliente proporcionará una confirmación por escrito a BT si así se le solicita;
- 4.2.2.5 **enrutamiento;** por lo que el Cliente modificará el enrutamiento de red del Cliente para garantizar que el tráfico adecuado se dirige al Dispositivo de Seguridad. El Cliente reconoce que los conmutadores proporcionados como parte del Servicio solo proporcionan conectividad física directa entre los Dispositivos de Seguridad y no están destinados a soportar ninguna funcionalidad de enrutamiento de red;
- 4.2.2.6 **actualizaciones;** el Cliente se asegurará de que los dispositivos de seguridad puedan recibir actualizaciones, como firmas de vulnerabilidad, directamente a través de Internet, o a través de una ruta alternativa acordada con BT a tal efecto;
- 4.2.2.7 **Asistencia de software para los equipos del Cliente;** el cliente obtendrá y proporcionará asistencia durante la vida útil de cualquier software que se ejecute en los Dispositivos de Seguridad del Cliente. Cuando sea necesario, el Cliente proporcionará y gestionará servidores físicos o virtuales en el Emplazamiento del Cliente con una especificación que BT acepte para ejecutar cualquier Software que BT proporcione;
- 4.2.2.8 **Acceso Fuera de Banda;** si no se incluye un módem de acceso fuera de banda como parte del Servicio, el Cliente acordará una alternativa adecuada con BT para permitir el diagnóstico de fallos y la configuración de base, permitiendo a BT establecer el control dentro de banda del Dispositivo de Seguridad, en el momento de la instalación y tras un fallo del dispositivo de seguridad;
- 4.2.2.9 **Equipo del Cliente;** si BT ha acordado prestar la totalidad o parte del Servicio utilizando el Equipo del Cliente, el Cliente se asegurará de que el Equipo del Cliente funcione correctamente. Si se descubre que está defectuoso antes de la Fecha de Servicio Operativo:
 - (a) el Cliente será responsable de resolver cualquier fallo;
 - (b) BT aumentará las tarifas para cubrir las visitas adicionales a los Emplazamientos; y
 - (c) las fechas de instalación acordadas y la Fecha Comprometida del Cliente pueden dejar de aplicarse;
- 4.2.3 **Pruebas de Aceptación.** Tras recibir la notificación de BT, el Cliente realizará sin demora las Pruebas de Aceptación del Servicio. Si el Servicio no ha superado las Pruebas de Aceptación debido a fallos graves, el Cliente lo notificará por escrito a BT en un plazo de cinco (5) Días Hábiles. La Fecha de Servicio Operativo comenzará según lo establecido en el Apartado 3.3 anterior.
- 4.3 **Durante el Funcionamiento**

A partir de la Fecha de Servicio Operativo, el Cliente deberá:

 - 4.3.1 asegurarse de que los Usuarios comunican las Incidencias al interlocutor del Cliente y no al Service Desk;
 - 4.3.2 asegurarse de que el interlocutor del cliente reciba los informes de incidencias de los usuarios y los transmita al Service Desk mediante los procedimientos de notificación acordados entre BT y el Cliente, y esté disponible para todas las comunicaciones posteriores de gestión de incidencias;
 - 4.3.3 cuando el Cliente haya proporcionado un Servicio de Habilitación propio o de terceros, garantizar y confirmar a BT que el Servicio de Habilitación propio o de terceros funciona correctamente antes de informar de las Incidencias a BT. BT no registrará el Tiempo de Inactividad de las Incidencias notificadas hasta que el Cliente haya proporcionado esta confirmación a ;
 - 4.3.4 informar puntualmente a BT de cualquier obra prevista en cualquier Servicio de Habilitación prestado por terceros que pueda repercutir en la disponibilidad del Servicio;
 - 4.3.5 conservar la responsabilidad del CSP;
 - 4.3.6 proporcionar asistencia de garantía de servicio, cuando lo solicite BT, para el progreso de Incidencias de cualquier Dispositivo de Seguridad instalado en un Servicio de Habilitación que no haya sido proporcionado por BT;
 - 4.3.7 garantizar que todo el Software proporcionado se utilice exclusivamente para el funcionamiento del Servicio;



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 4.3.8 supervisar y mantener cualquier Equipo del Cliente conectado al Servicio o utilizado en relación con el Servicio y garantizar que dicho Equipo del Cliente:
- (a) se conecte utilizando el punto de terminación de red aplicable, a menos que el Cliente cuente con el permiso de BT para conectarse por otro medio;
 - (b) sea técnicamente compatible con el Servicio y no perjudique ni dañe ningún Servicio de Habilitación, ni ninguna red o equipo de los proveedores o subcontratistas de BT; y
 - (c) está aprobado y es utilizado de conformidad con las instrucciones, normas y leyes aplicables, así como con los procedimientos de seguridad y protección aplicables al uso de dicho Equipo del Cliente. En particular, el Cliente será responsable, para cualquier Equipo del Cliente utilizado con el Servicio, de garantizar el cumplimiento de la legislación aplicable, incluida la obtención (en caso necesario) de licencias locales de importación y de usuario y la autorización por escrito de todas las autoridades respectivas, en particular para los países en los que el uso y la importación de Software y dispositivos de cifrado puedan estar restringidos por la legislación aplicable, o la exportación y reexportación del Software o los dispositivos de cifrado puedan estar sujetos a la legislación de control de exportaciones de los Estados Unidos de América, y de no actuar para hacer un uso indebido del Servicio proporcionado por BT con el fin de contravenir o eludir estas leyes. BT se reserva el derecho a exigir al Cliente que presente pruebas del cumplimiento de dichos requisitos normativos y de concesión de licencias. Si el Cliente no puede presentar dichas pruebas a satisfacción de BT, BT se reserva el derecho a suspender la prestación del Servicio o a rescindirlo por incumplimiento grave, tal y como se establece en las Condiciones Generales.
- 4.3.9 desconectar inmediatamente cualquier Equipo del Cliente, o avisar a BT para que lo haga a expensas del Cliente, cuando el Equipo del Cliente:
- (a) no cumple las instrucciones, normas o legislación aplicable; o
 - (b) contenga o cree material que infrinja la legislación aplicable y las condiciones del presente Contrato y BT se ponga en contacto con el Cliente en relación con dicho material,
- y solucionar los problemas con el Equipo del Cliente antes de la reconexión al Servicio;
- 4.3.10 distribuir, gestionar y mantener perfiles de acceso, contraseñas y otra información de administración de sistemas relacionada con el control del acceso de los Usuarios y del Cliente al Servicio. Si el Cliente así lo decide, podrá asignar una combinación de inicio de sesión al personal de BT;
- 4.3.11 hacerse responsable del uso que los Usuarios del Cliente hagan de los perfiles de acceso y contraseñas;
- 4.3.12 mantener una lista por escrito de los Usuarios actuales y proporcionar una copia de dicha lista a BT en un plazo de cinco (5) Días Hábilés tras la solicitud por escrito de BT en cualquier momento;
- 4.3.13 garantizar la seguridad y el uso adecuado de todos los perfiles de acceso de Usuario válidos, contraseñas y demás información de administración de sistemas utilizada en relación con el Servicio y:
- (a) cancelar inmediatamente el acceso a cualquier persona que deje de ser Usuario;
 - (b) informar inmediatamente a BT si el identificador o la contraseña de un usuario han llegado o pueden llegar a conocimiento de una persona no autorizada, o están siendo o pueden ser utilizados de forma no autorizada;
 - (c) tomar todas las medidas razonables para impedir el acceso no autorizado al Servicio;
 - (d) cumplir los controles de seguridad de BT en caso de pérdida u olvido de la contraseña; y
 - (e) cambiar cualquiera o todas las contraseñas u otra información de administración de sistemas utilizada en relación con el Servicio si BT se lo solicita al Cliente para garantizar la seguridad o integridad del Servicio;
- 4.3.14 cuando el Cliente haya seleccionado los modelos de entrega Propiedad de BT, Propiedad del Cliente o Adquisición de BT, y en caso de avería de un Dispositivo de Seguridad, permitirá a BT o a sus agentes, a discreción de BT, retirar y sustituir los componentes defectuosos o retirar el Dispositivo de Seguridad defectuoso en su totalidad y sustituirlo por otro que funcione correctamente. BT hará todo lo posible por garantizar que los datos del dispositivo o los componentes recuperados sean ilegibles antes de su eliminación o reciclaje;
- 4.3.15 para el modelo de suministro Adquisición de BT, proporcionará acceso a BT a cualquier centro de usuarios de licencias, contratos de asistencia existentes, código(s) de autorización u otra información requerida por vendedores específicos y facilitada en el momento del suministro para el registro de productos;
- 4.3.16 cuando el hardware y/o el Software lleguen al final de su vida útil, será responsable de solicitar y/o implementar oportunamente cualquier cambio recomendado por BT de conformidad con el Apartado 3.4.12, lo que implicará, en función del modelo de entrega seleccionado:
- (a) en caso de que el Cliente haya elegido el modelo de entrega "Propiedad del Cliente"; el Cliente será en todo momento plenamente responsable de llevar a cabo dicha sustitución o actualización y de pagar cualquier gasto relacionado; o bien



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- (b) en caso de que el Cliente haya seleccionado el modelo de entrega Propiedad de BT o Adquisición de BT y el Cliente desee continuar con el Servicio después de la fecha de vencimiento del Periodo Mínimo de Servicio; el Cliente deberá solicitar a BT cualquier cambio necesario para evitar que dicho hardware y/o Software llegue al Final de su Vida Útil;
- 4.3.17 cuando se especifique la Opción de Servicio de Cortafuegos Mejorada de Eagle-I, BT aplicará cualquier cambio como parte del bloqueo automatizado de COI tan pronto como sea técnicamente posible; y
- 4.3.18 cuando el Cliente solicite la opción de Mitigación Cooperativa con Nivel de Servicio Premium; informará a BT de cualquier cambio relativo a Dispositivos de punto final o Identidades de Usuario Final específicos para los que BT esté autorizada a tomar Medidas de Mitigación.
- 4.4 **El Fin del Servicio.**
 - 4.4.1 En caso de finalización del Servicio por parte de BT o del Cliente, éste deberá:
 - (a) proporcionar a BT toda la asistencia razonable necesaria para retirar el Equipo de BT del Emplazamiento o Emplazamientos;
 - (b) devolver o eliminar sin demora cualquier información confidencial que el Cliente haya recibido de BT durante la vigencia del Contrato;
 - (c) desconectar cualquier Equipo del Cliente del Equipo de BT situado en el Emplazamiento o Emplazamientos;
 - (d) no disponer ni utilizar el Equipo de BT si no es de acuerdo con las instrucciones o la autorización por escrito de BT;
 - (e) disponer la devolución a BT de cualquier Equipo de BT ubicado en el Emplazamiento o Emplazamientos; y
 - (f) hacerse responsable de los costes razonables de recuperación en los que incurra BT para recuperar el Equipo de BT.
 - 4.4.2 Cuando el Cliente haya solicitado la Mitigación Cooperativa con Nivel de Servicio Premium, el Cliente podrá deseleccionar la opción de Mitigación Cooperativa del Servicio total o parcialmente en cualquier momento, sujeto a lo siguiente:
 - (a) el Cliente lo notificará a BT, tras lo cual BT confirmará la fecha a partir de la cual el componente de Medida de Mitigación se desactivará del Servicio;
 - (b) el Cliente eliminará las credenciales de acceso de BT a las Identidades del Dispositivo o del Usuario Final;
 - (c) a partir de la fecha de desactivación, el Cliente será responsable de aplicar las Medidas de Mitigación que BT recomiende; y
 - (d) para evitar cualquier duda, la desección del componente de Mitigación Cooperativa del Servicio no dará lugar a ninguna reducción de los Cargos que se deban pagar en función del Nivel de Servicio seleccionado.

5 CARGOS Y CONDICIONES DE PAGO

- 5.1 Los cargos por el Servicio, dependiendo de las Opciones de Servicio y del Nivel de Servicio Seleccionado, se establecerán en el Pedido.
- 5.2 La fecha de inicio de facturación es la Fecha de Servicio Operativo, excepto si el Cliente requiere que BT retrase la instalación o configuración de Dispositivos de Seguridad durante más de 30 días. En tal caso, la facturación comenzará 30 días después de la fecha de instalación prevista originalmente.
- 5.3 Los gastos de instalación se cobrarán a partir de la Fecha de Servicio Operativa o a mes vencido antes de la Fecha de Servicio Operativa por cualquier trabajo realizado cuando el periodo de instalación previsto sea superior a un mes.
- 5.4 Además, BT facturará al Cliente:
 - 5.4.1 cualquier Cargo acordado por escrito por cambios en el CSP que excedan la "política de uso razonable";
 - 5.4.2 cualquier Cargo acordado por escrito por Cambios Urgentes o de Emergencia que el cliente haya emitido por error;
 - 5.4.3 cualquier Cargo acordado por escrito por cualquier actualización o mejora de dispositivos o aplicaciones que necesite el Cliente, a menos que la actualización o mejora sea necesaria desde el punto de vista operativo para que BT pueda seguir prestando el Servicio de BT. Esto no se aplica a la aplicación de parches ni a los cambios en el CSP;



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 5.4.4 cualquier Cargo acordado por escrito por cualquier actualización o mejora necesaria como resultado de problemas de capacidad derivados de un aumento del tráfico o de la activación de nuevas funciones;
- 5.4.5 cualquier otro Cargo según lo acordado en el Pedido (por ejemplo, si el Cliente solicita información según lo establecido en el Párrafo 3.5.4 o cambios para evitar que el hardware y/o el Software se lleguen al Fin de Vida según lo establecido en el Apartado 4.3.1.6);
- 5.4.6 cualquier coste adicional en el que BT haya incurrido debido a inexactitudes en la información facilitada por el Cliente a BT, incluidos los requisitos del CSP o las disposiciones del Apartado 4.2.1.5;
- 5.4.7 cualquier coste adicional en que BT haya incurrido de un proveedor por restablecer para el Cliente cualquier contrato de soporte o acuerdo de licencia caducado por el Cliente; y
- 5.4.8 los costes adicionales en los que BT haya incurrido por planificar visitas adicionales a las instalaciones debido al incumplimiento de sus obligaciones por parte del Cliente. Esto puede aplicarse en caso de que el Cliente no coopere con las inspecciones, tal y como se establece en el Apartado 3.2.2, o en caso de que el Equipo del Cliente esté defectuoso, tal y como se establece en el Apartado 4.2.2.11.

6 NIVELES DE SERVICIO

- 6.1 **Entrega puntual.** Si el Cliente solicita Foundation Plus o Premium como Servicio de Seguridad Gestionado por BT, se aplicará el Nivel de Servicio de Entrega Puntual fijado en el Anexo BT Managed Security.
- 6.2 **Disponibilidad.** Se aplicará el siguiente Nivel de Servicio de Disponibilidad:
 - 6.2.1 BT asignará una categoría de disponibilidad ("Categoría de SLA") determinada por la configuración del Dispositivo de Seguridad y la ubicación del Emplazamiento. Esto se indicará en el Pedido. Cada categoría de SLA tiene un objetivo de rendimiento anual (APT) asociado, que se utiliza para calcular el tiempo de inactividad APT. BT contabilizará el Tiempo de Inactividad para cada Incidencia que cumpla los requisitos notificado correctamente y mantendrá un registro del Tiempo de Inactividad acumulado por Emplazamiento, en unidades de minutos completos, para cada Mes y Año del SLA. Si el Tiempo de Inactividad acumulado en un Mes supera el Punto de Inicio del Crédito de Servicio (SCSP), el Cliente podrá reclamar un Crédito de Servicio Estándar, como se indica en la tabla siguiente, para cada Emplazamiento afectado, hasta un máximo de un mes de Cargos Recurrentes por Emplazamiento afectado. Si el Tiempo de Inactividad acumulado en cualquier Año de SLA (o parte de un Año de SLA para Centros instalados durante menos de un Año de SLA) supera el Tiempo de Inactividad APT, BT aplicará el/los Crédito(s) de Servicio Elevado(s) que se muestra(n) en la tabla siguiente para todas las reclamaciones válidas hasta que el Tiempo de Inactividad acumulado en el Año de SLA caiga por debajo del Tiempo de Inactividad APT. Durante este tiempo, el SCSP será inmediato para todas las Categorías de SLA.
 - 6.2.2 Salvo que se indique lo contrario, los Créditos de Servicio se aplican a cada hora iniciada de Tiempo de Inactividad por encima del SCSP.

Categoría SLA	Objetivo Anual de Rendimiento (OAR)	Tiempo de Inactividad de APT	SCSP para Créditos de Servicio Estándar	Créditos de Servicio Estándar	Créditos de Servicio Elevados
Cat A++	=>99.999%	5 minutos	inmediato	4% de los Cargos del Emplazamiento por cada 5 minutos de Inactividad iniciados por encima del SCSP	8% de los Cargos del Emplazamiento por cada 5 minutos de Inactividad iniciados
Cat A+	=>99.99%	1 hora	inmediato	4% de los Cargos del Emplazamiento por cada 5 minutos de Inactividad iniciados por encima del SCSP	8% de los Cargos del Emplazamiento por cada 5 minutos de Inactividad iniciados
Cat A1	=>99.97%	3 horas	inmediato	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Cat A	=>99.95%	4 horas	inmediato	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato B	=>99.90%	8 horas	1 hora	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

Gato C	=>99.85%	13 horas	3 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato D	=>99.80%	17 horas	5 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato E	=>99.70%	26 horas	7 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato F	=>99.50%	43 horas	9 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato G	=>99.00%	87 horas	11 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato H	=>98.00%	175 horas	13 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento
Gato I	=>97.00%	262 horas	15 horas	4% de los Cargos del Emplazamiento	8% de los Cargos del Emplazamiento

- 6.2.3 El Tiempo de Inactividad se mide desde el momento en que se notifica una Incidencia válida al Service Desk de BT y finaliza cuando BT resuelve la Incidencia. El Cliente recibirá un número de referencia de informe de Incidencia (número de "Ticket de problema") por cada Incidencia correctamente notificada.
- 6.2.4 BT informará al Cliente cuando se resuelva la Incidencia y cerrará el Ticket de problema cuando el Cliente confirme en el plazo de 1 hora que se ha resuelto la Incidencia, o bien BT haya intentado ponerse en contacto con el Cliente y no lo haya conseguido y el Cliente no responda en el plazo de 1 hora. Si el Cliente confirma que la Incidencia no se ha resuelto en el plazo de 1 hora desde que se le informó, el Ticket de problema permanecerá abierto y se ajustará el Tiempo de Inactividad.
- 6.2.5 El Tiempo de Inactividad sólo se medirá durante las Horas de Mantenimiento Contratado especificadas en el Pedido.
- 6.2.6 Los siguientes no son Incidentes Cualificados, y no se medirá el Tiempo de Inactividad;
- si el Cliente solicita a BT que pruebe el Servicio aunque no se haya detectado y/o notificado ninguna Incidencia;
 - si el Servicio ha sido modificado o alterado de alguna manera por el Cliente o a petición del Cliente;
 - durante el Mantenimiento Planificado;
 - para Incidencias debidas a cualquier configuración de red realizada por el Cliente y no aprobada por BT;
 - por cambios o alteraciones efectuados fuera de BT en el Servicio o en los Equipos, conexiones, plan de encaminamiento, aplicaciones o equipos de prueba de BT, o en la asignación de aplicaciones
 - si se notifica una Incidencia y BT no puede confirmar su existencia tras realizar pruebas.
- 6.3 **Tiempo de restauración (Resiliencia).** Si el cliente solicita la solución de alta disponibilidad como servicio de recuperación para un Emplazamiento, si el Dispositivo de Seguridad principal o secundario falla y BT no restablece el Servicio de ambos Dispositivos de Seguridad en un plazo de 24 horas desde que el Cliente notifica el fallo o BT lo detecta ("las 24 horas iniciales"), BT concederá al cliente un Crédito de Servicio para reclamaciones válidas. El Crédito de servicio será del 1% de los Cargos Recurrentes mensuales para el Emplazamiento afectado por cada hora iniciada después de las 24 horas iniciales hasta un límite del 100% de los Cargos Recurrentes mensuales para el Emplazamiento afectado. Como el Servicio está disponible durante este periodo, este tiempo no contará como Tiempo de Inactividad. Este Nivel de Servicio sólo se aplica si los Dispositivos de Seguridad se solicitan con mantenimiento 24 horas al día, 7 días a la semana, que puede no estar disponible en todas las ubicaciones.
- 6.4 **Exclusiones.** Además de las exclusiones generales del Nivel de Servicio establecidas en el Anexo BT Managed Security, los Niveles de Servicio anteriores dejarán de aplicarse cuando el hardware y/o el Software lleguen al Final de su Vida Útil y no se sustituyan según lo establecido en el presente Anexo.
- 6.5 **Solicitud de Créditos de Servicio.** Las condiciones para solicitar créditos de servicio se establecen en el Anexo BT Managed Security.

7 DURACIÓN MÍNIMA DEL SERVICIO, RESCISIÓN, RENOVACIÓN Y MODIFICACIONES



BT Managed Firewall Security (Fortinet) Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

- 7.1 **Período Mínimo de Servicio.** A menos que se acuerde lo contrario en un Pedido, el Período Mínimo de Servicio será un período de doce (12) meses consecutivos a partir de la Fecha de Servicio Operativo.
- 7.2 **Baja y renovación.** Al realizar el pedido, el Cliente deberá seleccionar en el Pedido de cada Servicio si prefiere la renovación automática o no.
- 7.2.1 En caso de que el Cliente haya seleccionado la renovación automática, el Servicio se renovará automáticamente al final del Período Mínimo de Servicio o de cada Período de Renovación subsiguiente por un período de Renovación de 12 meses; excepto si el Cliente ha cancelado el Servicio al menos 90 días antes de la fecha de vencimiento del Período Mínimo de Servicio o de un Período de Renovación en curso.
- 7.2.2 En caso de que el Cliente no haya seleccionado la renovación automática, el Servicio finalizará automáticamente al término del Período Mínimo (o de un Período de Renovación posterior), a menos que las Partes acuerden renovar el Servicio -mediante la firma de un nuevo Pedido- con un Período de Renovación al menos 90 días antes de la fecha de vencimiento del Período Mínimo de Servicio o de un Período de Renovación en curso.
- 7.2.3 Además, el Cliente podrá en cualquier momento rescindir anticipadamente el Servicio por conveniencia de acuerdo con las siguientes condiciones:
- (a) el Cliente avisará con antelación a BT de conformidad con las disposiciones de rescisión establecidas en las Condiciones Generales;
 - (b) junto a los Cargos pendientes hasta el día de la rescisión, el Cliente abonará a BT las tasas de rescisión como compensación, equivalentes a:
 - (i) los Cargos de Instalación a los que se haya renunciado y que figuren en el Pedido;
 - (ii) los Cargos de Desinstalación indicados en el Pedido. Si en el Pedido no se establecen Cargos de Desinstalación, los Cargos de Desinstalación serán iguales a los Cargos de Instalación;
 - (iii) todos los gastos en los que razonablemente incurra BT por parte de un proveedor como consecuencia de la rescisión anticipada, incluidos los gastos relativos a licencias de software o acuerdos de asistencia de proveedores;
 - (iv) para cualquier parte del Servicio que haya finalizado durante los 12 primeros meses del Período Mínimo de Servicio:
 - 100 por ciento de los Cargos Recurrentes por cualquier mes restante de los primeros 12 meses del Período Mínimo de Servicio;
 - el 20% de los gastos recurrentes de los meses restantes, excepto los 12 primeros meses del Período Mínimo de Servicio, con la excepción de los Cargos Recurrentes de los Dispositivos de Seguridad suministrados en régimen de alquiler, que serán el 100% de los Cargos Recurrentes; y
 - (v) para cualquier parte del Servicio que haya finalizado después de los primeros 12 meses del Período Mínimo de Servicio o durante un Período de Renovación, el 20 por ciento de los Cargos Recurrentes para cualquier mes restante del Período Mínimo de Servicio o del Período de Renovación, con la excepción de los Cargos Recurrentes para los Dispositivos de Seguridad proporcionados en régimen de alquiler, que serán el 100 por ciento de los Cargos Recurrentes.
 - (c) las tarifas de terminación de los Servicios de Seguridad Gestionados por BT se calcularán sobre las tarifas periódicas una vez aplicado cualquier descuento y, en el caso de la Seguridad de Cortafuegos Gestionada por BT, antes de aplicar cualquier descuento; y
 - (d) Si el Cliente ha abonado por adelantado los Cargos correspondientes a la licencia de software o al contrato de asistencia del proveedor, el Cliente no tendrá derecho al reembolso de los cargos correspondientes a los meses restantes del Período Mínimo de Servicio o del Período de Renovación.
- 7.3 **Modificaciones.** En caso de que ambas Partes deseen continuar prestando y utilizando el Servicio, BT podrá proponer cambios en el Anexo BT Managed Security, en este Anexo, en las Tarifas y/o en las Condiciones Generales de acuerdo con las siguientes condiciones:
- 7.3.1 BT avisará por escrito al Cliente con al menos 60 días de antelación antes de que finalice el Período Mínimo de Servicio y cada Período de Renovación, con una explicación detallada del/de los Cambio(s) requerido(s);
- 7.3.2 cualquier cambio se acordará por escrito entre las Partes en un plazo de 30 días a partir de la recepción de la notificación de modificación de BT;
- 7.3.3 en caso de que se acuerden cambios entre las Partes, éstos se aplicarán a partir del inicio del siguiente Período de Renovación y se prorrogará el contrato, durante el cual:
- (a) BT seguirá prestando el Servicio; y
 - (b) cada Parte seguirá cumpliendo sus obligaciones de conformidad con el Contrato.



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

7.3.4 en caso de que las Partes no puedan acordar los cambios requeridos; el Servicio finalizará y BT dejará de prestar el Servicio a las 23:59 horas del último día del Periodo Mínimo de Servicio o del Periodo de Renovación posterior, según corresponda.

8 TRATAMIENTO DE DATOS

9.1 Condiciones aplicables. Las Partes acuerdan que se prevé que BT y el Proveedor puedan recibir o tratar Datos Personales en nombre del Cliente como Encargado del Tratamiento de Datos en relación con el Servicio o como resultado de la prestación de este Servicio. Cualquier Dato del Cliente está sujeto a la cláusula de "Datos" tal y como se establece en los Términos y Condiciones Generales del Contrato y el correspondiente DPA (Acuerdo de Procesamiento de Datos) cuando sea aplicable.

9.2 Naturaleza y finalidad del Tratamiento de Datos Personales de los Clientes por parte de BT. Con BT Managed Firewall Security, BT podrá:

- (a) proporcionar un servicio que permite al Cliente configurar el Servicio implementando reglas mediante las cuales las Direcciones IP de origen y destino, protocolos, Usuarios y aplicaciones pueden ser controlados a través del CSP;
- (b) supervisar el tráfico que atraviesa el servicio para aplicar las normas y los CSP implementados en el dispositivo de seguridad;
- (c) compartir los Datos Personales del Cliente con los proveedores de Equipos de BT o Equipos del Cliente o subcontratistas, según sea necesario para la prestación y gestión del Servicio, incluidas la instalación, el mantenimiento y la resolución de Incidencias;
- (d) si el Cliente ha seleccionado el Servicio de Emulación de Amenazas, los Datos Personales del Cliente se envían automáticamente desde los Dispositivos de Seguridad o el Software a la infraestructura basada en la nube operada por el proveedor para la emulación y evaluación de amenazas;
- (e) acceder a un registro de las direcciones IP, direcciones MAC y usuarios de los clientes, junto con los intentos de URL y visitas a sitios web por parte de dichas direcciones y usuarios, utilizando un portal en línea con el fin de proporcionar los informes.

9.3 Los tipos de Datos Personales del Cliente tratados por BT o sus Subencargados del tratamiento o el Cliente serán:

- sitio web o dirección IP de destino;
- Dirección IP del dispositivo de origen;
- Dirección MAC del dispositivo de origen;
- datos de contacto de la empresa, incluidos:
 - i. nombre;
 - ii. dirección;
 - iii. número de teléfono;
 - iv. dirección de correo electrónico;
 - v. puesto de trabajo;
 - vi. nombre de la empresa; y
- registros de contacto.

9.4 Los Datos Personales del Cliente afectarán a las siguientes categorías de Interesados:

- los empleados del Cliente;
- los clientes del Cliente o terceros; y
- cualquier Interesado (respecto al cual el Cliente actúe como Responsable).



BT Managed Firewall Security (Fortinet)

Anexo de Servicio BT Managed Security

Referencia de contrato BT:

Referencia del contrato del Cliente (opcional):

Cambios Simples y Complejos

Nota: Cualquier cambio no calificado en la tabla inferior como "Simple" será un Cambio Complejo.

Cambios sencillos en el servicio	
Cambio	Mecanismo para Solicitar Cambios
Cambios en el cortafuegos [AMF] - Establecer Permisos permitiendo Direcciones IP o rango de IP (puertos específicos o todos los puertos)	MyAccount - Gestor de cambios BT
NAT (Simple) [AMF] - NAT simple (NAT estático, mapping 1 a 1)	MyAccount - Gestor de cambios BT
NAT (NAT Oculto) [AMF] – NAT Oculto	MyAccount - Gestor de cambios BT
NAT (Manual) [AMF] - NAT Manual	MyAccount - Gestor de cambios BT
Enrutamiento de Cortafuegos [AMF] - Enruta a Redes no conectadas directamente al FW.	MyAccount - Gestor de cambios BT
Cambios en las Reglas del Proxy [AMF] - Modificación de las reglas de acceso a Internet del servidor proxy	MyAccount - Gestor de cambios BT
Cambios en la Lista Negra/Lista Blanca de URL [AMF] Bloquear/Permitir sitios web en función de los requisitos comerciales de la empresa.	MyAccount - Gestor de cambios BT
Requisitos de Enrutamiento del Proxy [AMF] Rutas a redes no conectadas directamente al proxy	MyAccount - Gestor de cambios BT

En fe de lo cual, las Partes suscriben el presente documento por vía electrónica, siendo efectivo a partir de la fecha del segundo firmante.

Cliente [Incluya el nombre completo del cliente]	BT Global ICT Business España, S.L.U.
Firmado:	Firmado:
(Representante autorizado)	(Representante autorizado)
(Nombre)	Paul Rhodes
Representante legal	Representante legal