Nombre legal del cliente ("Cliente")	XXXXXXXXXXX	**Nombre legal de BT ("BT")**	BT Global ICT Business Spain SLU
Dirección y número de registro del cliente	XXXXXXXXXXX XXXXXXXXXXX	**Dirección y número de registro de BT**	Calle María Tubau, nº 3, 6ª planta, 28050 Madrid. CIF: B-88625496
Fecha de entrada en vigor	XX XXXXX XXXX	**Nº de referencia BT**	N/A

1 Definiciones y Abreviaturas

Se aplican las siguientes definiciones y abreviaturas, además de las que figuran en las Condiciones Generales.

"**Administrador**" se refiere a la persona autorizada por el Cliente que es responsable de gestionar el Servicio BT Managed Cloud Security (Zscaler) mediante el Portal del Cliente.

"**Ancho de Banda**" significa el volumen de varias clases de información que fluye a través del tráfico de Internet del Cliente y según lo definido por el Cliente en el Pedido.

"**Cambio Complejo**" significa un cambio que no es un Cambio Simple. En el Apéndice 2 figuran ejemplos de Cambios Complejos.

"**Cambio de Emergencia**" significa un Cambio Simple altamente crítico que debe implementarse tan pronto como sea posible específicamente para abordar un problema que tenga un impacto adverso en las operaciones comerciales, o para prevenir o resolver una Incidencia P1.

"**Cambio Estándar**" significa, con respecto a un Cambio Simple, las actualizaciones y modificaciones necesarias como resultado de los desarrollos previstos y las mejoras de seguridad.

"**Cambio Simple**" significa los cambios simples que figuran en el Apéndice 2 de este Anexo.

"**Cambio Urgente**" significa, con respecto a un Cambio Simple, las actualizaciones y modificaciones necesarias como resultado de actividades no planificadas o imprevistas, pero que no son críticas para mantener la seguridad de la organización.

"**Cargos**" se refiere a los Cargos establecidos en la Orden.

"**Cargos de Instalación**" se refiere a los Cargos establecidos en cualquier Pedido aplicable en relación con la instalación del Servicio BT Managed Cloud Security (Zscaler), según corresponda.

"**Cargos Recurrentes**" se refiere a los Cargos por el Servicio BT Managed Cloud Security (Zscaler) (o la parte aplicable del mismo) que se facturan repetidamente en cada periodo de pago (por ejemplo, cada mes), según lo establecido en el Pedido.

"**Centro de Operaciones de Seguridad**" o "**SOC**" hace referencia al equipo de BT responsable de la Supervisión y Gestión de los Servicios BT Managed Cloud Security (Zscaler) prestados en virtud del Nivel de Servicio Graduado solicitado por el Cliente.

"**Centros de Datos de Recargo**" hace referencia a la infraestructura del Proveedor que se puede utilizar para prestar el Servicio BT Managed Cloud Security (Zscaler) ubicada en los territorios definidos por el Proveedor y actualizados periódicamente, cuyos detalles están disponibles previa solicitud a BT.

"**Componentes del Servicio Estándar**" tiene el significado que se le da en el Apartado 2.2.

"**Configuración Inicial**" se refiere a la facilitación de la configuración y entrega del Servicio BT Managed Cloud Security (Zscaler) según lo establecido en el Apartado 4.1.

"**Contacto del Cliente**" tiene el significado que se le da en el Apartado 12.1.

"**Crédito de Servicio**" significa cualquier solución acordada para el incumplimiento por parte del Proveedor de BT de un Nivel de Servicio, y, en su caso, como se describe más detalladamente en este Anexo o se establece en un Pedido.

"**Crédito de Servicio de Zscaler Private Access**" tiene el significado que se le atribuye en el Apartado 18.

"**Crédito de Servicio de Disponibilidad**" tiene el significado que se le da en el Apartado 18.

"**Crédito de Servicio de Latencia**" tiene el significado que se le da en el Apartado 18.

"**Crédito de Servicio de Tasa de Captura de Virus**" tiene el significado que se le da en el Apartado 18.

"**Datos del Cliente**" se refiere a los datos introducidos por el Cliente o los Usuarios con el fin de utilizar los Servicios de BT Managed Cloud Security (Zscaler).

"**Derechos de Propiedad Intelectual del Proveedor**" tiene el significado que se le da en el Párrafo 7.

"**Despliegue Controlado**" hace referencia a la fase de despliegue controlado del Nivel de Servicio Graduado solicitado y del Servicio BT Managed Cloud Security (Zscaler), tal y como se establece en el Apartado 4.2.

"**Dirección IP":** número único en Internet de una tarjeta o controlador de red que identifica un dispositivo y es visible por todos los demás dispositivos en Internet.

"Dispositivos" se refiere a cualquier equipo, incluidos, entre otros, ordenadores portátiles y servidores, utilizado por el Cliente o los empleados del Cliente para proporcionar u obtener un acceso a las aplicaciones, sistemas y plataformas del Cliente.
"**Equipo del Cliente**" hace referencia a cualquier equipo, incluido cualquier software, que no sea Equipo de BT, utilizado por el Cliente en relación con un Servicio BT Managed Cloud Security (Zscaler).
"**Fecha Comprometida del Cliente**" hace referencia a la fecha en la que BT se compromete a prestar el Servicio BT Managed Cloud Security (Zscaler) (o cada parte del mismo).
"**Fecha de Servicio Operativo**" hace referencia a la fecha en la que BT pone a disposición del Cliente por primera vez cualquier Servicio gestionado de seguridad en la nube de BT (Zscaler) o parte del mismo, o a la fecha en la que el Cliente comienza a utilizar por primera vez dicho Servicio gestionado de seguridad en la nube de BT (Zscaler) (o parte del mismo), la que sea anterior.
"**Guías del Usuario**" se refiere a los documentos que establecen detalles sobre cómo el Cliente:

(a) pueden acceder al Portal BT;
(b) realizar cambios en los CSP; y
(c) pueden acceder a los informes.

"**Horario Comercial**" significa entre las 08:00 y las 17:00 horas de un Día Hábil.
"Identidades de Usuario Final" se refiere a los nombres de usuario y contraseñas que utilizan los empleados del Cliente para acceder a las aplicaciones, sistemas y plataformas del Cliente.
"**In the Wild**" significa un virus que ya está suelto en Internet por un mínimo de tres (3) participantes en la Wild List.
"**Incidencia**" significa una interrupción no planificada o una reducción de la calidad del Servicio de seguridad en la nube gestionada de BT (Zscaler) o de un elemento concreto del mismo.
"I**ndicadores de Compromiso**" o **"IOCs"** son fragmentos de datos forenses, como los que se encuentran en las entradas o archivos de registro del sistema, que identifican actividades potencialmente maliciosas en un sistema o red.
"**Inteligencia sobre Amenazas para la Seguridad**" o "**STI"**: el servicio de inteligencia sobre amenazas para la seguridad establecido en el Apartado 5.1.1.
"**Internet"** significa un sistema global de redes interconectadas que utilizan un Protocolo de Internet estándar para enlazar dispositivos en todo el mundo.
"**Jurisdicción Prohibida**" tiene el significado que se le da en el Apartado 12.3.
"**Límite de Gestión del Servicio**" tiene el significado que se le da en el Apartado 6.
"Línea de Base del Ancho de Banda del Cliente" hace referencia al consumo medio de ancho de banda por puesto calculado por el Proveedor durante el periodo de 90 días posterior al inicio de la suscripción del Cliente al Servicio BT Managed Cloud Security (Zscaler).
"**Localizador Uniforme de Recursos**" o "**URL":** cadena de caracteres que apunta a un recurso en una intranet o en Internet.
"**Manual del Cliente**" hace referencia a un documento que se proporciona al Cliente una vez finalizada la fase de Configuración Inicial y que proporciona información específica del Cliente relevante para el Servicio BT Managed Cloud Security (Zscaler) y el Nivel de Servicio Graduado adquirido. El Manual del Cliente no es un documento contractual.
"**Máquina Virtual de NSS**" significa una máquina que recibe copias de registros de tráfico en tiempo real a través de un túnel seguro en un formato altamente comprimido desde la nube de Zscaler, descomprime y destokeniza estos registros y, a continuación, aplica filtros y formatos especificados para su transmisión a una solución de gestión de Incidencias y eventos de seguridad.
"**Medida de Mitigación**" significa una medida recomendada que debería adoptarse para abordar el impacto de los COI identificados por BT.
"**Mejora Continua**" se refiere a la fase de mejora continua tal y como se establece en el Apartado 5.2.
"Mitigación Cooperativa" tiene el significado que se le otorga en el Apartado 2.3.4.
"**Nivel de Servicio**": cualquier nivel mínimo de servicio acordado que deban alcanzar BT y su Proveedor, tal y como se establece en el Apartado 18.
"**Nivel de Servicio de Acceso Privado de Zscaler**" tiene el significado que se le atribuye en el Apartado 18.
"**Nivel de Servicio de Disponibilidad**" tiene el significado que se le da en el Apartado 18.
"**Nivel de Servicio de Entrega a Tiempo**" tiene el significado que se le da en el Apartado 18.
"**Nivel de Servicio de Latencia**" tiene el significado que se le da en el Apartado 18.
"**Nivel de Servicio de Tasa de Captura de Virus**" tiene el significado que se le da en el Apartado 18.
"**Nivel de Servicio Graduado**" es el término utilizado para describir el nivel de las características de gestión establecidas en este Anexo de Servicios y se clasifica como Soporte, Soporte Plus o Premium.
"**Objetivo de Servicio**" se refiere a cualquier objetivo que BT pretenda cumplir según lo establecido en este Anexo de Servicio, pero para el que no se disponga de solución.
"**Opciones de Servicio**" tiene el significado que se le da en el Apartado 2.3.

"**Optimización del CSP de Despliegue Controlado**" se refiere a la puesta a punto de la(s) CSP(s) del Cliente, llevada a cabo por el Cliente o con respecto a Soporte Plus o Premium, únicamente ambas Partes conjuntamente.
"P1", "**P2**", "**P3"**, "**P4**" y "**P5" tienen** el significado que se les da en la tabla del Apartado 5.4.1.
"**Paquete de Datos":** unidad de datos constituida en un único paquete de Protocolo de Internet (IP) que viaja a lo largo de una ruta de red determinada.
"**Periodo de Optimización del CSP de Despliegue Controlado**" significa, con respecto a:

(a) Soporte, 48 horas después de recibir la notificación de BT;
(b) Soporte Plus, hasta 30 Días Hábiles después de recibir la notificación de BT; y
(c) Premium, hasta 30 Días Hábiles después de recibir la notificación de BT.

"**Periodo de Renovación**" significa para cada Servicio BT Managed Cloud Security (Zscaler) el periodo inicial de 12 meses posterior al Periodo Mínimo de Servicio y cada periodo posterior de 12 meses, o cualquier periodo acordado por ambas Partes.
"**Plataforma Eagle-i**" hace referencia a la solución a través de la cual BT proporcionará alertas de incidencias enriquecidas e identificará cualquier COI como parte del Servicio Eagle-i.
"**Plazo de Implementación Objetivo**" hace referencia al plazo de implementación objetivo a partir de la aceptación por parte de BT de la solicitud de cambio de CSP del Cliente, tal y como se establece en la tabla del Apartado 5.3.11.
"**Política de Seguridad del Cliente**" o "**CSP**" significa la política de seguridad del Cliente que contiene las reglas de seguridad, establecidas y propiedad del Cliente, que se aplican al Servicio Asociado aplicable y determinan el funcionamiento del Servicio Asociado aplicable.
"**Política de Uso Aceptable del Proveedor**" significa la Política de Uso Aceptable de Zscaler tal y como se establece en el Apéndice 1 de este Anexo.
"**Política de Uso Razonable**" tiene el significado que se le da en el apartado 5.3.6.
"**Portal de BT**" hace referencia a una o varias páginas web que BT pone a disposición del Cliente para permitir la gestión de los Servicios BT Managed Cloud Security (Zscaler) solicitados.
"**Portal del Cliente**" tiene el significado que se le da en el Apartado 2.2.2.
"**Proceso de Gestión de Cambios del CSP**" significa el proceso en relación con los cambios del CSP(s) según lo establecido en el Apartado 5.3.
"**Protocolo de Internet**" o "**IP"** significa un protocolo de comunicaciones para dispositivos conectados a Internet que especifica el formato de las direcciones y unidades de datos transmitidos.
"**Protocolo de Transferencia de Archivos**" o "**FTP":** protocolo de red estándar utilizado para transferir archivos de un host a otro host a través de una red basada en TCP, como Internet.
"**Protocolo de Transferencia de Hipertexto**" o "**HTTP":** un protocolo de aplicación para sistemas de información hipermedia distribuidos y colaborativos.
"**Protocolo de Transferencia de Hipertexto Seguro**" o "**HTTPS"**: protocolo de comunicaciones para la comunicación segura a través de una red informática, con una implantación especialmente amplia en Internet.
"**Proveedor**" se refiere a Zscaler, Inc, una sociedad de Delaware, con domicilio social en 110 Baytech Drive, Suite 100, San Jose, CA 95134-2304, EE.UU..
"**Registros de Transacciones del Cliente**" significa, los metadatos de todo el tráfico de red enviado o recibido por el Proveedor desde o hacia el Cliente en el uso por parte del Cliente del Servicio BT Managed Cloud Security (Zscaler).
"**Registros de Transacciones Resumidos**": las versiones resumidas de los Registros de Transacciones sin Procesar.
"**Registro de Transacciones sin Procesar**" se refiere a los metadatos de todo el tráfico de red enviado o recibido del Cliente a través de su uso del Servicio BT Managed Cloud Security (Zscaler).
"**Service Desk**" hace referencia al servicio de asistencia al que el Cliente puede dirigirse para enviar solicitudes de servicio, informar de Incidencias y realizar preguntas sobre el Nivel de Servicio Graduado solicitado y el Servicio BT Managed Cloud Security (Zscaler).
"**Servicio BT Managed Cloud Security (Zscaler)**" se refiere al servicio tal y como se establece en este Anexo.
"Servicios BT Managed Security" se refiere a los Niveles de Servicio Graduados prestados por BT como servicio de envoltura, tal y como se establece en este Anexo.
"**Servicio de Nombres de Dominio**" o "**DNS"** significa un sistema de directorio que traduce las direcciones IP numéricas en Nombres de Dominio para identificar a los Usuarios en Internet.
"Servicio Eagle-i" hace referencia al componente del Servicio descrito en el apartado 2.3.3.
"**Servicio NSS**" tiene el significado que se le atribuye en el Apartado 2.3.3.
"**Servicios Profesionales**" se refiere a aquellos servicios probados por BT que son servicios relacionados con el trabajo.
"**Sesión**" hace referencia a cualquier solicitud no HTTP o HTTP enviada al Cliente o desde él a través de su uso de los Servicios de BT Managed Cloud Security (Zscaler).
"**Solicitud de Adición de Servicio**" tiene el significado que se le da en el Apartado 14.

"**Software de Servicio**" significa la plataforma "**Zscaler Internet Access**" o "**Zscaler Private Access"** basada en la nube del Proveedor, según corresponda.
"**Soporte**" se refiere al Nivel de Servicio Graduado según lo establecido en este Anexo.
"**Soporte Plus**" significa el Nivel de Servicio Graduado Plus que figura en este Anexo.
"**Supervisión y Gestión**" hace referencia a la fase de supervisión y gestión del Servicio BT Managed Cloud Security (Zscaler), tal y como se establece en el Apartado 5.1.
"**Suscripción de Usuario**" hace referencia al derecho de un Usuario Individual específico a acceder a Internet mediante el Servicio BT Managed Cloud Security (Zscaler). (Nota: en un entorno en el que no exista autenticación de Usuario, cada 2.000 Transacciones DNS por día que fluyan a través del Servicio BT Managed Cloud Security (Zscaler) se atribuirán a una Suscripción de Usuario (es decir, el número de Suscripciones de Usuario utilizadas se calcularía dividiendo el número total de Transacciones DNS que fluyen a través del Servicio BT Managed Cloud Security (Zscaler) por día entre 2.000).
"**Tecnología del Proveedor**" tiene el significado que se le da en el Apartado 7.1.
"**Ticket"**: número de referencia único proporcionado por BT para una Incidencia que también puede conocerse como "**número de referencia de avería"**.
"**Tiempo de Restablecimiento Objetivo**" tiene el significado que figura en la tabla del Apartado 5.4 para el nivel de prioridad y el Nivel de Servicio Graduado correspondientes.
"**Transacción**" hace referencia a una solicitud HTTP o HTTPS enviada a o desde el Cliente a través de su uso del Servicio BT Managed Cloud Security (Zscaler).
"**Transacción DNS**" se refiere a una consulta DNS recursiva enviada por el Cliente a través de su uso del Servicio BT Managed Cloud Security (Zscaler).
"**Ubicación**" se refiere a un derecho de punto de acceso específico a Internet en relación con el Servicio BT Managed Cloud Security (Zscaler).
"**Uso Aceptable del Proveedor**" tiene el significado que se le da en el Párrafo 12.2.
"**Virus Conocido**" se refiere a un virus que, en el momento de la recepción del contenido por parte del Proveedor: (i) ya se ha hecho pública una firma, durante un mínimo de una hora para su configuración por parte del escáner comercial de terceros del Proveedor; y (ii) está incluido en la Wild List que se encuentra en http://www.wildlist.org e identificado como In the Wild.
"**Wild List":** significa la lista de virus "In the Wild" mantenida por la Organización Wild List.
"**Zscaler Client Connector**" hace referencia a la aplicación que permite acceder al Servicio BT Managed Cloud Security (Zscaler) a través de determinados sistemas operativos móviles y ordenadores.
"**Zscaler Internet Access**" o "**ZIA**" hace referencia a un servicio en la nube basado en software que permite a un Cliente seleccionar varias opciones de seguridad que se aplicarán en centros de datos en la nube de todo el mundo para proteger el tráfico de Internet del Cliente.
"**Zscaler Private Access**" o "**ZPA**" se refiere a un servicio en la nube basado en software que proporciona acceso remoto seguro y sin interrupciones a las aplicaciones internas del Cliente, independientemente de dónde existan, y sin colocar usuarios en la red del Cliente.

2 Descripción del servicio

2.1 El servicio BT Managed Cloud Security (Zscaler) consta de:

- todos los Componentes Estándar del Servicio establecidos en el Apartado 2.2; y
- cualquier Opción de Servicio establecida en el Apartado 2.3 que el Cliente seleccione en cualquier Pedido aplicable.

2.2 **Componentes Estándar del Servicio.**

BT proporcionará al Cliente todos los siguientes Componentes Estándar del Servicio de acuerdo con los detalles establecidos en cualquier Pedido aplicable que comprenderá:

2.2.1 **Software de Servicio**. BT proporcionará al Cliente el derecho a acceder y utilizar el Software de Servicio para el número de Usuarios, Suscripciones de Usuario y/o Ubicaciones adquiridos.

2.2.2 **Portales**. BT proporcionará al Cliente acceso (a) al Portal BT y (b) a la interfaz de usuario basada en web del Proveedor ("**Portal del Cliente**").

(a) El Portal BT es un portal administrativo de BT para acceder y gestionar los Servicios BT Managed Security.

(b) El Portal del Cliente es un portal administrativo del Proveedor para la creación y gestión de políticas de seguridad, elaboración de informes y análisis de tráfico y proporciona al Cliente una cuenta de Administrador principal que le permitirá crear múltiples Administradores y habilita al Cliente para:

(i) revisar las estadísticas de todo el malware que se detiene y otros contenidos de Internet que se bloquean;

(ii) crear restricciones de acceso y aplicarlas a Usuarios o grupos de Usuarios específicos;

(iii) personalizar las páginas de alerta del navegador que ven los Usuarios cuando se les deniega el acceso a la web;
(iv) actualizar los datos administrativos para recibir alertas por correo electrónico en tiempo real; y
(v) configurar y programar auditorías e informes automatizados del sistema.

(c) El Cliente podrá permitir que varios Administradores accedan a los portales. El Cliente dará a cada uno de los Administradores del Cliente un inicio de sesión único y proporcionará acceso de gestión o privilegios de sólo lectura específicos para cada Nivel de Servicio Graduado. Esta funcionalidad permite una única cuenta de superusuario que puede crear múltiples Administradores.

(d) BT podrá utilizar sus derechos de acceso como Administrador al Portal del cliente para investigar y resolver cualquier Incidencia notificada por el Cliente a BT de conformidad con el Apartado 13.

(e) BT intentará dar curso a la solicitud del Cliente de crear un nuevo Usuario en el Portal de BT en el plazo de un Día Hábil, excepto durante los periodos de mantenimiento planificado.

2.2.3 **Servicios BT Managed Security: Niveles de Servicio Graduados**. BT proporcionará al Cliente una gama de servicios de gestión de seguridad graduados que pueden utilizarse en asociación con el Servicio BT Managed Cloud Security (Zscaler) y como superposición al mismo, con sujeción a las siguientes condiciones:

(a) El Cliente elegirá uno de los Niveles de Servicio Graduado, algunas de cuyas características se indican en la tabla siguiente, para utilizarlo con el Servicio BT Managed Cloud Security (Zscaler) según lo establecido en cualquier Pedido aplicable:

	Soporte	**Soporte Plus**	**Premium**
Configuración Inicial del servicio BT Managed Cloud Security (Zscaler) según lo establecido en el Apartado 4.1			
Política de seguridad del cliente			
Servicio BT Managed Cloud Security (Zscaler)	Políticas estándar de buenas prácticas	Políticas específicas para cada sector/escenario	Política de seguridad a medida
BT Project Manager asignado para la Configuración Inicial	✗ Opciones disponibles tal y como se indica en el Apartado 5.1	✓ Nombre Opciones disponibles tal y como se indica en el apartado 5.1	✓ Nombramiento y posible visita a la Ubicación en función de la localización.
Créditos de Servicio de Entrega a Tiempo por incumplimiento de la Fecha Comprometida del Cliente	✗	✓	✓
Despliegue controlado de los Servicios Asociados según lo establecido en el apartado 4.2			
Despliegue Controlado El Periodo de Optimización del CSP comienza al finalizar la Instalación Inicial			
Despliegue controlado del Servicio BT Managed Cloud Security (Zscaler) Periodo de optimización del CSP	48 horas	Hasta 30 días	Hasta 30 días
Prueba y ajuste conjuntos de BT y el cliente CSP	✗	✓	✓
Supervisión y Gestión del servicio BT Managed Cloud Security (Zscaler) según lo establecido en el Apartado 5.			
Inteligencia sobre Amenazas a la Seguridad	Boletines e informes de inteligencia sobre amenazas	Según Soporte	Según Soporte
Gestionar las incidencias del servicio			
Service Desk 24x7x365	✓	✓	✓
Centro de Operaciones de Seguridad (SOC)	BT selecciona el SOC adecuado	BT selecciona el SOC adecuado	BT selecciona el SOC adecuado

	Soporte	Soporte Plus	Premium
Idioma del Service Desk	Según lo acordado con BT (inglés por defecto)	Según lo acordado con BT (inglés por defecto)	Según lo acordado con BT (inglés por defecto)
Mejora continua del servicio BT Managed Cloud Security (Zscaler), tal como se establece en el Apartado 5.			
Revisiones del Servicio BT Graduado y del servicio BT Managed Cloud Security (Zscaler)	6 mensualidades	Trimestral	A intervalos acordados por ambas Partes
Gestión del Cambio	a través del Portal BT	A través del Portal BT o del personal competente de BT	a través del Portal BT o del personal BT competente

(b) El Nivel de Servicio Graduado seleccionado con el Pedido Inicial también se aplicará a cualquier Pedido futuro que el Cliente pueda realizar para los Servicios de BT Managed Cloud Security (Zscaler), ya que el Cliente no puede tener más de un Nivel de Servicio Graduado.

(c) Durante el Periodo Mínimo de Servicio o durante cualquier periodo de renovación posterior, el Cliente podrá cambiar a una Categoría de Servicio superior, pero no podrá bajar a una Categoría de Servicio inferior. Los nuevos Cargos y el nuevo Periodo Mínimo de Servicio para la Categoría de Servicio mejorada se acordarán mediante un nuevo Pedido. No se aplicarán Cargos por Cancelación a partir del Nivel de Servicio Graduado al que se traslade el Cliente.

(d) En caso de conflicto entre las disposiciones de los Niveles de Servicio Graduados, el orden de prioridad de la disposición correspondiente, en función del Nivel de Servicio Graduado solicitado por el Cliente, será el siguiente:

(i) Premium;
(ii) Soporte Plus;
(iii) Soporte.

2.3 **Opciones de Servicio**

El Cliente puede solicitar cualquiera de las siguientes opciones, tal y como se especifica con más detalle (incluidos los Cargos adicionales) en cualquier Pedido aplicable:

2.3.1 **Centros de Datos de Recargo**: En determinados países o regiones, BT o el Proveedor pueden sugerir que los datos del Cliente se alojen y procesen en Centros de Datos de Recargo. Cuando el Cliente elija esta opción, incurrirá en Cargos adicionales, que se establecerán en el Pedido. El Cliente puede optar por utilizar centros de datos del Proveedor distintos de los Centros de Datos de Recargo, pero reconoce que el rendimiento del Servicio puede verse afectado; y

2.3.2 **Servicios Profesionales**: BT puede proporcionar, con un Cargo adicional, Servicios Profesionales con cada Pedido, para respaldar la Configuración Inicial del Servicio por parte del Cliente y el funcionamiento continuo del Servicio.

2.3.3 **Servicio Eagle-i:** Para los Niveles de Servicio Graduado Soporte Plus y Premium, BT incluirá una suscripción al Servicio Eagle-i con cada Pedido sujeto a lo siguiente.

(a) El servicio Eagle-i ingiere los registros del Servicio Zscaler Nanolog Streaming Service ("Servicio NSS") desde el Servicio Managed Cloud Security Service, a través del cual BT:

(i) supervisará los registros del Servicio NSS en busca de eventos y los enriquecerá con la información sobre amenazas de BT;
(ii) alertará al Cliente de incidencias de seguridad de alta prioridad; y
(iii) recomendará, en su caso, una propuesta de Medida de Mitigación.

(b) Si el Cliente ya dispone de un Servicio NSS, deberá proporcionar a BT una fuente de datos del Servicio NSS existente del Cliente.

(c) Si el Cliente no tiene un Servicio NSS existente, deberá seleccionar uno de los siguientes al inicio de un Pedido;

(i) alojamiento de la Máquina Virtual NSS por parte de BT; o bien
(ii) alojamiento de la Máquina Virtual NSS por parte del Cliente. En tal caso, el Cliente, al realizar el Pedido a BT, informará a BT de que la Máquina Virtual NSS será alojada por el Cliente y proporcionará a BT una alimentación de datos del Servicio de NSS al Servicio.

(d) Si el Cliente seleccionó el Nivel de Servicio Graduado Soporte Plus en el Pedido, el Cliente será responsable de implementar cualquier Medida de Mitigación, que se llevará a cabo accediendo a la herramienta de gestión de servicios pertinente para los componentes afectados.

(e) Si el Cliente seleccionó el Nivel de Servicio Graduado Premium en el Pedido, podrá también seleccionar la Mitigación Cooperativa. Sin perjuicio de lo dispuesto en el Apartado 12.1.12, en caso de que se detecte una Incidencia, BT aplicará una Medida de Mitigación en Dispositivos de punto final o Identidades de Usuario Final específicos identificados por BT en los casos siguientes:

(i) se contenga el impacto de la Incidencia detectada; y
(ii) BT realice los cambios oportunos en la política de seguridad u otros servicios de Eagle-i en el nivel de servicio Premium.

2.3.4 **Cogestión**: BT proporcionará al Cliente un Perfil RBAC ("**Perfil de Control de Cuentas Basado en la Función**") para un máximo de 5 Usuarios designados autorizados en el Portal del Cliente. Los Usuarios que utilicen el perfil RBAC tendrán acceso restringido a la implementación de Cambios Simples. Si el Cliente solicita la Cogestión:

(a) el Cliente será responsable de garantizar que los Usuarios designados autorizados completen la formación del Portal del Cliente disponible a través del Proveedor, a cargo del Cliente, antes de que se permita a dichos Usuarios aplicar Cambios Simples;
(b) BT proporcionará al Cliente una guía de usuario independiente en la que se detallará cómo gestionar los Cambios Simples;
(c) Además de lo establecido en el apartado 5.3, el Cliente será responsable de la implementación de los Cambios Simples, incluido el impacto de dichos cambios, y BT no será responsable de ninguna consecuencia derivada de esta acción, incluidos, entre otros, los problemas de rendimiento o las interrupciones del Servicio; y
(d) si un Cambio Simple implementado por cualquier Usuario usando el Perfil RBAC ha resultado en una Incidencia,

(i) el Cliente notificará la Incidencia de conformidad con el apartado 13;
(ii) BT proporcionará asistencia para resolver la Incidencia de conformidad con el Apartado 5.4 utilizando la capacidad de auditoría y registro del Portal del Cliente para respaldar cualquier análisis de causa raíz realizado para confirmarlo; y
(iii) BT se reserva el derecho a aplicar los Cargos correspondientes por cualquier Medida de Mitigación que sea necesaria para rectificar.

3 Periodo Mínimo de Servicio y Periodos de Renovación

3.1 Salvo que se acuerde lo contrario en un Pedido, el Periodo Mínimo de Servicio será un periodo de doce (12) meses consecutivos a partir de la Fecha de Servicio Operativo. El Servicio finalizará automáticamente al término del Período Mínimo de Servicio, a menos que las Partes acuerden renovar el Servicio con un Período de Renovación al menos 90 días antes del final del Período Mínimo de Servicio o de cada Período de Renovación mediante la firma de un nuevo Pedido.

3.2 En caso de que ambas Partes deseen continuar suministrando y utilizando el Servicio BT Managed Cloud Security (Zscaler), BT podrá proponer cambios en este Anexo, en los Cargos y/o en las Condiciones Generales mediante notificación por escrito al Cliente con una antelación mínima de 60 días antes de la finalización del Periodo Mínimo de Servicio y de cada Periodo de Renovación.

3.3 Cualquier cambio de este tipo deberá ser acordado por escrito entre las Partes en un plazo de 30 días a partir de la recepción de la notificación de modificación de BT.

3.4 En caso de que las modificaciones sean acordadas entre las Partes, éstas se aplicarán desde el inicio del siguiente Periodo de Renovación y el contrato prorrogado, durante el cual:

(a) BT seguirá prestando el servicio BT Managed Cloud Security (Zscaler); y
(b) cada Parte seguirá cumpliendo sus obligaciones de conformidad con el Contrato.

3.5 En caso de que las Partes no puedan acordar los cambios necesarios, el Servicio BT Managed Cloud Security (Zscaler) finalizará y BT dejará de prestar el Servicio BT Managed Cloud Security a las 23:59 del último día del Periodo Mínimo de Servicio o del Periodo de Renovación posterior, según corresponda.

4 Prestación de Servicios

4.1 **Configuración Inicial**

BT acordará con el Cliente una fecha para la implementación del Servicio. Se aplicarán las siguientes opciones de entrega en función del Nivel de Servicio Gradual seleccionado por el Cliente:

4.1.1 **Soporte**

- **Incluido de serie con Soporte.**

(a) Responsabilidades de BT:

(i) BT mantendrá informado al Cliente durante todo el proceso de entrega.
(ii) BT proporcionará políticas estándar que reflejen las buenas prácticas.
(iii) BT coordinará la prestación de los Servicios BT Managed Cloud Security (Zscaler).
(iv) BT pondrá en servicio los Servicios BT Managed Cloud Security (Zscaler) de forma remota de acuerdo con las políticas de CSP seleccionadas por el Cliente, a menos que se establezca lo contrario en este Anexo de Servicio.
(v) en la fecha en la que BT haya completado sus actividades de entrega según lo establecido en el Anexo de Servicio de BT Managed Cloud Security (Zscaler) y en este Anexo de Servicio, BT confirmará al Cliente la fecha en la que se ha completado la Configuración Inicial. Esta será la Fecha de Servicio Operativo y, a partir de esa fecha, comenzará el Periodo de Optimización del CSP de Despliegue Controlado.

(b) Responsabilidades del Cliente:

(i) El Cliente seleccionará las pólizas adecuadas para utilizarlas como CSP(s) del Cliente cuando el Cliente realice el Pedido y se asegurará de que las pólizas estándar que el Cliente seleccione cumplan los requisitos del Cliente. El Cliente seguirá siendo responsable de definir los CSP en curso del Cliente más allá de lo establecido en las políticas seleccionadas por el Cliente después de la Fecha de Servicio Operativo.
(ii) El Cliente podrá solicitar cambios en los CSP del Cliente después de la Fecha de Servicio Operativa de conformidad con el Apartado 14.

- **Opcional con Soporte.**

El Cliente podrá solicitar que BT, con un Cargo adicional que acordarán las Partes y que se establecerá en el Pedido:

(a) designe a un Project Manager de BT para que sea el único punto de contacto del Cliente durante la Configuración Inicial. El Project Manager de BT llevará a cabo cualquier actividad de forma remota y no visitará las instalaciones del Cliente;
(b) proporcione un Project Manager de BT designado que estará disponible para asistir a reuniones en las instalaciones del cliente, en función de la ubicación de éste, durante la duración de la Configuración Inicial; o bien
(c) proporcione al Cliente Servicios Profesionales para ayudarle en la creación de su(s) CSP(s). La responsabilidad de los CSP seguirá recayendo en el Cliente.

4.1.2 **Soporte Plus.** Además de lo dispuesto en el Apartado 4.1.1, Soporte;

- **Incluido de serie con Soporte Plus.**

(a) BT designará a un Project Manager de BT para que sea el único punto de contacto del Cliente durante la Configuración Inicial. El Project Manager de BT llevará a cabo cualquier actividad de forma remotadistancia y no visitará las instalaciones del Cliente; y
(b) BT proporcionará una política de seguridad personalizable para utilizarla como CSP del Cliente.

- **Opcional con Soporte Plus.**

El Cliente podrá solicitar que BT le proporcione un Project Manager de BT designado que estará disponible para asistir a reuniones en las instalaciones del Cliente, en función de la ubicación del Cliente, durante la duración de la Configuración inicial por un Cargo adicional que acordarán las Partes y se establecerá en el Pedido .

4.1.3 **Premium.** Además de lo dispuesto en el Apartado 4.1.1, Soporte y en el apartado 4.1.2, Soporte Plus;

(a) BT proporcionará un Project Manager BT designado que estará disponible para asistir a reuniones con el Cliente en las instalaciones del Cliente en función de la ubicación del Cliente durante la duración de la Configuración Inicial; y
(a) el Cliente designará a un Project Manager y a un equipo técnico del Cliente que trabajarán con BT durante la Configuración Inicial; en particular, durante el Periodo de Optimización del Despliegue Controlado, tal y como se establece en el Apartado 5 a continuación.

4.2 **Despliegue Controlado**

BT proporcionará soporte de activación al Cliente para que éste tenga acceso al Portal del Cliente para la configuración del Servicio. BT desplegará el Servicio utilizando uno o varios de los métodos de suministro establecidos en: https://zscaler.zendesk.com/hc/en-us/articles/205118615 - Choosing-Traffic-Forwarding-Methods (o cualquier otra dirección en línea que BT pueda indicar al Cliente) y, si el Cliente ha optado por incluir la opción de servicios de despliegue en los Servicios, BT trabajará con el Cliente para decidir qué método de despliegue utilizar. BT trabajará con el Cliente para preparar un plan de despliegue durante el Periodo de Optimización del CSP de Despliegue Controlado de acuerdo con las siguientes disposiciones en función del Nivel de Servicio Graduado seleccionado por el Cliente:

4.2.1 **Soporte**

(a) BT proporcionará al Cliente las Guías de Usuario.
(b) El Cliente respetará las Guías de Usuario.
(c) El Cliente llevará a cabo la Optimización del CSP de Despliegue Controlado dentro del Periodo de Optimización del CSP de Despliegue Controlado.
(d) El Cliente notificará a BT cuando haya completado la Optimización del CSP de Despliegue Controlado. Si el Cliente no proporciona a BT dicha notificación antes de que finalice el Periodo de Optimización del CSP de Despliegue Controlado, se considerará que el Cliente ha completado la Optimización del CSP de Despliegue Controlado.
(e) BT notificará al Cliente la fecha de finalización de la Optimización del CSP de Despliegue Controlado.
(f) El Cliente presentará cualquier cambio que el Cliente requiera al CSP como resultado de la Optimización del CSP de Despliegue Controlado a través del Proceso de Gestión de Cambios del CSP, tal y como se establece en el Apartado 5.3.
(g) Si el Cliente ha solicitado cambios en el/los CSP durante el Periodo de Optimización del CSP de Despliegue Controlado, BT dirigirá al Cliente al mecanismo de gestión de cambios del CSP en el Portal de Seguridad si la solicitud del Cliente para el cambio en el/los CSP está fuera del Servicio BT Managed Security y de los Servicios BT Managed Cloud Security (Zscaler). El Cliente seguirá el Proceso de Gestión de Cambios de CSP establecido en el Párrafo 5.3. Si BT tiene conocimiento de que el Cliente no puede acceder al Portal de BT, o si el Cliente se lo comunica, BT dirigirá el Cliente al personal de BT adecuado para que revise la solicitud del Cliente.

4.2.2 **Soporte Plus y Premium.** Además de lo dispuesto en el apartado 4.2.1, Soporte;

Ambas Partes llevarán a cabo conjuntamente la Optimización del CSP de Despliegue Controlado. El Cliente hará todo lo razonablemente posible para completar la Optimización del CSP de Despliegue Controlado lo antes posible dentro del Periodo de Optimización del CSP de Despliegue Controlado.

4.3 **Notificación de prestación del Servicio**

BT notificará al Cliente que el Servicio ha sido habilitado y le proporcionará asistencia para la activación. La Fecha de Servicio Operativo se produce una vez que BT notifica al Cliente que el Servicio se ha habilitado. BT enviará al Cliente un correo electrónico de aprovisionamiento con información sobre el inicio de sesión en el Portal del Cliente y una carta de bienvenida al Cliente.

5 Gestión en vida

5.1 **Seguimiento y Gestión**

BT prestará los siguientes servicios de supervisión y gestión a partir de la fecha de entrada en funcionamiento del servicio:

5.1.1 **Inteligencia sobre Amenazas para la Seguridad .** Con cada Nivel de Servicio, BT proporcionará al cliente los siguientes boletines e informes de información general en inglés a una lista acordada de contactos del cliente:

(a) avisos diarios sobre amenazas: ofrecen una visión de los últimos titulares sobre seguridad, actores, objetivos, operaciones y campañas, vulnerabilidades y direcciones IP sospechosas;
(b) resúmenes de amenazas globales: ofrecen una visión amplia y de alto nivel de los sucesos y ataques significativos ocurridos en todo el mundo y en todos los sectores;
(c) sesiones informativas mensuales a nivel ejecutivo: ofrecen una visión a nivel de CISO del panorama de las amenazas, centrándose en los acontecimientos que afectan a las organizaciones globales desde una perspectiva estratégica; y
(d) boletines críticos globales: proporcionan una evaluación técnica de sucesos de seguridad globales significativos, como WannaCry, para que pueda obtenerse una comprensión más detallada.

5.1.2 **Incidencias de Gestión del Servicio**

BT actuará como único punto de contacto para la resolución de Incidencias relacionadas con los Servicios BT Managed Cloud Security (Zscaler); en función del Nivel de Servicio Graduado respectivo seleccionado por el Cliente:

5.1.2.1 **Soporte**

(a) El Cliente sólo notificará las Incidencias a través del Portal BT.
(b) Todas las comunicaciones con el Service Desk se harán en inglés.
(c) El Service Desk que gestionará las notificaciones de Incidencias está disponible 24 horas al día, 7 días a la semana, 365 días al año y cuenta con profesionales formados en seguridad.
(d) BT entregará al Cliente un Ticket.
(e) BT evaluará el Incidente de acuerdo con los criterios establecidos en la tabla siguiente:

Prioridad	Descripción
P1	Impacto grave e Incidencia que no se puede eludir, normalmente cuando el Servicio BT Managed Cloud Security (Zscaler) está completamente caído / no disponible; por ejemplo: la Ubicación del Cliente está aislada o hay una pérdida completa de Servicio en una Ubicación o se impide el funcionamiento de funciones empresariales críticas.
P2	Gran impacto en una parte del Servicio BT Managed Cloud Security (Zscaler) y no se puede evitar, causa una pérdida significativa del Servicio BT Managed Cloud Security (Zscaler), pero la función empresarial afectada no se detiene; por ejemplo: se produce una pérdida completa del enlace primario y se invoca el enlace de reserva de BT (si se proporciona) o las funciones empresariales se interrumpen pero no se impide su funcionamiento.
P3	Pequeño impacto en el Servicio BT Managed Cloud Security BT (Zscaler) o cuando se ve afectado un único Usuario o componente y causa algún impacto en el negocio del Cliente; por ejemplo: hay una perturbación intermitente u ocasional que no tiene un impacto importante en el Servicio BT Managed Cloud Security (Zscaler) o cuando se ha proporcionado una solución temporal.
P4	Incidencia de impacto menor o intermitente a un elemento no operativo del Servicio BT Managed Cloud Security (Zscaler); por ejemplo: un fallo temporal de informes o facturación.
P5	La Incidencia no tiene un impacto directo en el Servicio BT Managed Cloud Security (Zscaler). Los registros que normalmente se guardan para las Incidencias se utilizan con fines informativos. Ejemplo: para realizar un seguimiento de las actualizaciones, para obtener un Informe de Motivo de Interrupción (RFO), para interrupciones planificadas o para consultas, así como Incidencias provocados por el cliente.

(f) BT revisará el estado de la Incidencia y modificará el nivel de prioridad asignado inicialmente si fuera necesario.

(g) BT mantendrá informado al Cliente durante el transcurso de la resolución de la Incidencia a intervalos regulares mediante la publicación de actualizaciones en el Portal de BT o a través de correos electrónicos al Contacto del Cliente.

5.1.2.2 **Soporte Plus.** Además de lo dispuesto en el apartado 5.1.2.1, Soporte;

el Cliente también podrá notificar todas las Incidencias directamente al Service Desk.

5.1.2.3 **Premium .** Además de lo dispuesto en el apartado 5.1.2.1, Soporte y en el apartado 5.1.2.2, Soporte Plus;

el Cliente también podrá notificar todas las Incidencias directamente al Centro de Operaciones de Seguridad regional.

5.2 **Mejora Continua**

BT prestará los siguientes servicios adicionales de Mejora Continua, a partir de la Fecha de Servicio Operativo:

5.2.1 **Reseñas**

5.2.1.1 **Soporte**

(a) El Responsable de Optimización de la Seguridad llevará a cabo una revisión semestral (6) de la siguiente manera:

(i) una revisión del servicio centrada en el rendimiento del Nivel de Servicio Graduado de BT y el Servicio BT Managed Cloud Security (Zscaler); y

(ii) una revisión de fin de vida útil de forma continua. El Gestor de Optimización de la Seguridad proporcionará al Cliente un informe que resuma las aplicaciones y el software gestionados por BT en nombre del Cliente como parte de los Servicios BT Managed Cloud Security (Zscaler) que llegarán al final de su vida útil en los seis meses siguientes. El informe incluirá las aplicaciones y el software notificados previamente al Cliente que hayan llegado al final de su vida útil y que requieran una acción inmediata por parte del Cliente.

(b) Si el cliente lo solicita y BT está de acuerdo, ambas partes podrán celebrar una conferencia telefónica para debatir el informe.

(c) Si BT ha acordado participar en una conferencia telefónica, el Cliente se asegurará de que el personal debidamente cualificado del Cliente que participe en la conferencia telefónica revise cualquier informe que el Responsable de Optimización de la Seguridad proporcione al Cliente antes de que ésta tenga lugar.

(d) El Cliente tomará las medidas oportunas para resolver los problemas según las recomendaciones del Responsable de Optimización de la Seguridad:

(i) con respecto al Nivel de Servicio Graduado de BT y al Servicio BT Managed Cloud Security (Zscaler), incluida la aplicación de mejoras de seguridad según lo acordado con el Gestor de Optimización de la Seguridad o según lo aconsejado por el Gestor de Optimización de la Seguridad como responsabilidad del Cliente; y

(ii) con respecto a la revisión al final de la vida o según lo establecido en el informe de revisión al final de la vida.

5.2.1.2 **Soporte Plus.** Además de lo dispuesto en el Apartado 5.2.1.1, Soporte;

(a) El Responsable de Optimización de la Seguridad llevará a cabo una revisión trimestral del siguiente modo:

(i) una revisión del servicio centrada en el rendimiento del Nivel de Servicio Graduado de BT y del servicio BT Managed Cloud Security (Zscaler) con respecto a los niveles y objetivos de servicio y la gestión de la capacidad del servicio BT Managed Cloud Security (Zscaler);

(ii) una revisión de los CSP del Cliente centrada en la eficacia de las normas aplicadas a los CSP y en la necesidad de afinar o modificar las normas de los CSP del Cliente; y

(b) Además de tomar las medidas establecidas en el Apartado 5.2.1.1(d), el Cliente será responsable de iniciar las solicitudes de cambio apropiadas de conformidad con el Proceso de Gestión de Cambios del CSP para abordar los problemas relacionados con el ajuste o la modificación del CSP del Cliente según lo recomendado por el Responsable de Optimización de la Seguridad.

5.2.1.3 **Premium.** Además de lo dispuesto en el Apartado 5.2.1.1, Soporte y en el Apartado 5.2.1.2, Soporte Plus;

(a) El Responsable de Optimización de la Seguridad llevará a cabo las revisiones establecidas en el Apartado 5.2.1.2 (a) a intervalos acordados por ambas Partes, pero no inferiores a una vez al mes.

(b) El Responsable de Optimización de la Seguridad proporcionará al Cliente un informe sobre la revisión a través del Portal BT o directamente al Cliente por correo electrónico, si así lo acuerdan ambas Partes.

(c) Si el Cliente lo solicita y BT lo acepta, ambas Partes podrán celebrar una conferencia telefónica para debatir el informe o BT podrá asistir a una reunión en las Instalaciones del Cliente, en función de la ubicación de éste, para debatir el informe con el Cliente. En tal caso, el Cliente se asegurará de que el personal debidamente cualificado del Cliente que participe en la conferencia telefónica o asista a la reunión revise cualquier informe que el Administrador de Optimización de la Seguridad proporcione al Cliente antes de que se celebre la conferencia telefónica.

5.3 **Proceso de Gestión de Cambios del CSP**

5.3.1 BT implementará cambios en los CSP en respuesta a la solicitud del Cliente de acuerdo con el siguiente proceso ("Proceso de Gestión de Cambios de CSP") y en función del Nivel de Servicio Graduado establecido en el Pedido:

Soporte BT	Soporte	Soporte Plus	Premium
Solicitudes de los clientes que se van a iniciar.	a través del Portal BT	a través del Portal BT o directamente al Gestor de Optimización de la Seguridad	a través del Portal BT o directamente al Gestor de Optimización de la Seguridad
Identificación por BT de errores o posibles consecuencias imprevistas de los Cambios Simples y Cambios Complejos solicitados por los Clientes	✗	✗	✓
Cambios Simples - Cambios Estándar (*)	ZIA 6 al mes	ZIA 8 al mes ZPA 8 al mes	ZIA 10 al mes ZPA 10 al mes
Cambios Simples - Cambios Urgentes	1 al mes	2 al mes	3 al mes
Cambios Sencillos - Cambios Urgentes	Se cobra a razón de un simple cambio.	Se cobra a razón de un simple cambio.	Se cobra a razón de un simple cambio.
Cambios Complejos	Se acordará mediante una nueva Orden	Se acordará mediante una nueva Orden	Se acordará mediante una nueva Orden

Nota: Las restricciones de la Política de Uso Razonable para las solicitudes de Cambio Estándar establecidas en el Apartado 5.3.6 de este Anexo se aplicarán tanto a Zscaler Internet Access como a Zscaler Private Access.

5.3.2 El Contacto Autorizado del Cliente presentará solicitudes para cambiar el/los CSP y proporcionará detalles suficientes e instrucciones claras sobre los cambios necesarios. El Cliente no presentará

cambios no autorizados, y se asegurará de que los Usuarios con acceso al Portal de BT no lo hagan. Si BT tiene conocimiento de que el Cliente no puede acceder al Portal de BT, o si el Cliente se lo comunica, BT dirigirá el Cliente al personal de BT adecuado para que revise la solicitud del Cliente.

5.3.3 BT comprobará la complejidad de cada solicitud y evaluará si el cambio (i) debe completarse mediante el Proceso de Gestión de Cambios de CSP, (ii) requiere un nuevo Pedido o (iii) requiere un cambio de contrato que debe acordarse mediante una modificación por escrito del Contrato.

5.3.4 Sólo los cambios del CSP en los conjuntos de reglas que definen el funcionamiento del Servicio se completarán a través del Proceso de Gestión de Cambios del CSP.

5.3.5 Para evitar cualquier duda; cualquier cambio por el que el Cliente solicite cambios en el Servicio que no se califiquen como Cambio Simple (por ejemplo, incluyendo licencias adicionales) requiere un nuevo Pedido.

5.3.6 Los Cambios Estándar y Urgentes están incluidos en los Cargos sujetos a las limitaciones establecidas en la tabla anterior ("**Política de Uso Razonable**"). Cuando los Cambios Estándar y/o Urgentes se planteen con mayor frecuencia, las Partes podrán acordarlo:

(a) agrupar las solicitudes de los clientes a lo largo de un periodo de tiempo, de modo que puedan ejecutarse con mayor eficacia. En este caso, pueden producirse algunos retrasos en la ejecución;

(b) revisar los requisitos del Cliente y acordar con él un proceso de aplicación alternativo adecuado y los gastos asociados mediante un nuevo Pedido; o bien

(c) cobrar dicha solicitud de cambio adicional según la tarifa establecida en la Orden.

5.3.7 Las solicitudes de Cambios Complejos se acordarán entre el Cliente y BT mediante un nuevo Pedido, incluidos los Cargos adicionales por la implementación de dichos Cambios Complejos.

5.3.8 BT aplicará cualquier Cambio de Emergencia tan pronto como sea razonablemente posible y sin la aprobación previa del Cliente; siempre que BT demuestre posteriormente por qué era necesario dicho cambio de emergencia.

5.3.9 BT comunicará el estado de las solicitudes de cambio por correo electrónico al Contacto del Cliente que solicita el cambio y el estado estará disponible también en el Portal BT durante un periodo de seis meses.

5.3.10 Excepto para Cambios de Emergencia,

(a) se considerará que el Cliente ha aprobado todos los cambios en el/los CSP que se presenten a BT; y

(b) el Cliente es responsable del impacto de la aplicación de los cambios por parte de BT. Esto significa que si BT implementa este cambio de acuerdo con la solicitud del Cliente, BT no será responsable de ninguna consecuencia derivada del impacto de la implementación de los cambios; incluida cualquier especificación errónea de los requisitos de seguridad del Cliente en los CSP o cualquier consecuencia imprevista de un CSP correctamente especificado e implementado.

5.3.11 En caso de que el Cliente haya solicitado Soporte Plus o Premium; BT intentará implementar los cambios en el/los CSP del Cliente de acuerdo con la tabla que figura a continuación:

Solicitar	Plazo de aplicación previsto
Cambio Simple - Cambio Estándar	8 Horas calculadas a partir del momento en que BT aceptó la solicitud de cambio del Cliente.
Cambio Simple - Cambio Urgente	4 Horas calculadas a partir del momento en que BT aceptó la solicitud de cambio del Cliente.
Cambio Simple - Cambio de Emergencia	4 Horas calculadas desde el momento en que se identifica la necesidad de un Cambio de Emergencia.
Cambio Complejo	Según lo acordado en el Pedido

5.3.12 El Cliente puede solicitar Servicios Profesionales para ayudarle a redactar la solicitud de cambio.

5.4 **Tiempos de Respuesta - Objetivos de Servicio para la Gestión de Incidencias**

5.4.1 BT responderá a las Incidencias, en función del Nivel de Servicio Graduado seleccionado por el cliente, de acuerdo con la siguiente tabla y a partir del momento en que el servicio de atención al cliente proporcione al Cliente un Ticket:

Prioridad	Actualización del progreso de los objetivos			Tiempo de restauración objetivo
	Soporte	Soporte Plus y Premium		Soporte, Soporte Plus y Premium
P1-P5	siempre que haya una actualización disponible	confirmación de la Incidencia dentro de los 15 minutos siguientes a la notificación de la Incidencia y primera actualización 30 minutos después de la notificación de la Incidencia y, seguirdamente, a intervalos como se indica a continuación:	hacer un seguimiento si el Cliente no responde a las preguntas de BT en los intervalos que se indican a continuación:	
P1		cada 60 minutos o cada vez que se disponga de una actualización del progreso	cada 2 horas	5 horas
P2		cada 60 minutos o cada vez que se disponga de una actualización del progreso	cada 4 horas	12 horas
P3		cada 2 horas	cada 12 horas	24 horas
P4		cada 4 horas	cada 24 horas	72 horas
P5		cada 6 horas	N/A	N/A

5.4.2 BT intentará proporcionar al Cliente información actualizada sobre el progreso de una Incidencia de acuerdo con la tabla anterior.

5.4.3 BT no proporcionará información actualizada sobre el progreso mientras esté esperando las aportaciones o comentarios del Cliente.

5.4.4 BT intentará restablecer el servicio BT Managed Cloud Security (Zscaler) afectado por la Incidencia en el plazo establecido en la tabla anterior.

5.4.5 Los tiempos de actualización del progreso y de restablecimiento son sólo objetivos y BT no será responsable de su incumplimiento.

5.4.6 El Cliente permitirá a BT ejecutar herramientas de descubrimiento en la red del Cliente para mejorar y ajustar el/los CSP del Cliente o para ayudar en la resolución de Incidencias.

6 Límite de Gestión del Servicio (SMB)

6.1 BT prestará y gestionará el Servicio tal y como se establece en este Anexo y en el Pedido. El Límite de Gestión del Servicio es el punto en el que el tráfico entra y sale de la infraestructura propiedad del Proveedor o controlada por éste.

6.2 BT no tendrá responsabilidad alguna por el Servicio fuera de los Límites de Gestión del Servicio, incluidos, entre otros:

6.2.1 problemas en las máquinas de los Usuarios (por ejemplo, sistema operativo, lenguajes de codificación y configuración de seguridad);

6.2.2 conectividad de red de extremo a extremo (por ejemplo, la red o el equipo de red del Cliente, conectividad a Internet);

6.2.3 gestión de fuentes de identidad;

6.2.4 titularidad de la póliza; o

6.2.5 análisis de la información de seguridad y gestión de eventos.

6.2.6 Cuando BT deba conectarse o utilizar una red no suministrada por BT para poder prestar el Nivel de Servicio Graduado al cliente y se produzca un fallo posterior en la red de terceros que interrumpa la capacidad de BT para prestar el Nivel de Servicio Graduado,

(a) BT no tendrá ninguna responsabilidad ante el Cliente en relación con la prestación y el rendimiento del Nivel de Servicio Graduado y la incapacidad de BT para prestar el Nivel de Servicio Graduado, o su efecto en otros servicios asociados;

(b) no se aplicarán los niveles y objetivos de servicio; y

(c) si BT debe realizar trabajos adicionales para resolver cualquier problema que surja, las Partes acordarán por escrito en un Pedido los trabajos adicionales y los Cargos adicionales por dichos trabajos.

6.3 BT no garantiza que el Servicio detecte o bloquee todas las amenazas maliciosas. El Cliente reconoce que el Servicio no puede garantizar la prevención o detección de todas las amenazas y acciones no autorizadas.

6.4 BT no hace ninguna declaración, ya sea expresa o implícita, sobre la interoperabilidad entre el Servicio y cualquier Equipo del Cliente.

6.5 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.

6.6 Cuando el Cliente seleccione la Mitigación Cooperativa con Nivel de Servicio Graduado Premium, la responsabilidad de BT se limitará a proporcionar Mitigación Cooperativa en Dispositivos de punto final o Identidades de Usuario Final siempre que no formen parte de los 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 individualmente cada Medida de Mitigación, BT solo aplicará la Medida de Mitigación una vez que el Cliente haya dado dicha aprobación.

6.7 Determinadas Opciones de Servicio pueden requerir que el Cliente disponga de un Equipo de Cliente específico que cumpla unas especificaciones mínimas, comunicadas al Cliente por BT o el Proveedor, para beneficiarse de una funcionalidad completa. BT no será responsable de la imposibilidad de prestar el Servicio o de la degradación del mismo cuando el Cliente utilice el Servicio sin el Equipo de Cliente necesario

7 Propiedad Intelectual de los Proveedores

7.1 El Proveedor utiliza:

7.1.1 nombres de productos asociados al Servicio y otras marcas comerciales;

7.1.2 determinadas informaciones sonoras y visuales, documentos, programas informáticos y otras obras de autor; y

7.1.3 otras tecnologías, software, hardware, productos, procesos, algoritmos, interfaces de usuario, know-how y otros secretos comerciales, técnicas, diseños, invenciones y otro material o información técnica tangible o intangible,

(en conjunto, la "**Tecnología del Proveedor**").

7.2 La Tecnología del Proveedor está protegida por derechos de propiedad intelectual propiedad del Proveedor o cedidos bajo licencia por éste ("**Derechos de Propiedad Intelectual del Proveedor**").

7.3 Todos los derechos, títulos e intereses sobre el Software y el Software de Servicio, así como todos los Derechos de Propiedad Intelectual del Proveedor asociados, seguirán perteneciendo en todo momento al Proveedor y a sus licenciantes, y, aparte de los derechos concedidos en este Anexo de Servicios, el Cliente no adquirirá ningún otro derecho, expreso o implícito, sobre el Servicio.

8 Registros de Transacciones del Cliente

8.1 BT y el Proveedor podrán utilizar, reproducir, almacenar, modificar y mostrar la información de los Registros de Transacciones del cliente con el fin de prestar el Servicio.

8.2 BT y el Proveedor pueden, utilizar el malware, spam, botnets u otra información relacionada con el Servicio con el propósito de:

(a) mantener y mejorar el Servicio;
(b) cumplir todos los requisitos legales o contractuales;
(c) poner a disposición de sus licenciantes contenidos maliciosos o no deseados de forma anónima con el fin de seguir desarrollando y mejorando el Servicio;
(d) la agregación anónima y el análisis estadístico de los contenidos; y
(e) otros usos relacionados con el análisis del Servicio.

8.3 En el caso del Acceso a Internet de Zscaler, el Proveedor conservará los Registros de Transacciones sin Procesar, los Registros de Transacciones Resumidos y cualesquiera otros Registros de Transacciones del Cliente durante periodos renovables de seis meses durante la prestación del Servicio.

8.4 En el caso de Zscaler Private Access, el Proveedor conservará los Registros de Transacciones sin Procesar durante periodos renovables de dos semanas durante la prestación del Servicio.

8.5 Una vez finalizado el Servicio, el Proveedor eliminará los Registros de Transacciones del Cliente, de acuerdo con el ciclo de conservación de dos semanas o seis meses establecido anteriormente, a menos que el Cliente solicite por escrito a BT que los Registros de Transacciones del Cliente se mantengan durante un periodo de tiempo adicional, que estará sujeto a acuerdo y a un cargo adicional que se acordará entre el Cliente y BT mediante Pedido por escrito.

9 Sugerencias, ideas y comentarios

El Cliente acepta que el Proveedor y/o BT tendrán derecho a utilizar o actuar sobre la base de cualquier sugerencia, idea, solicitud de mejora, comentario, recomendación u otra información proporcionada por el Cliente en relación con el Servicio, en la medida en que no se trate de información confidencial del Cliente.

10 Consumo excesivo de ancho de banda

10.1 Si el consumo medio de ancho de banda por puesto del Cliente aumenta por encima de la línea de base de ancho de banda del Cliente en más del cien por cien (100 %) durante un periodo continuado de noventa (90) días, se notificará al Cliente, que acepta colaborar con BT y el Proveedor de buena fe para investigar los motivos del aumento de ancho de banda del Cliente (por ejemplo, tráfico adicional no adquirido que utiliza el Servicio BT Managed Cloud Security (Zscaler), cambios en la red del Cliente, etc.).p. ej., puestos adicionales no adquiridos que utilicen el Servicio BT Managed Cloud Security (Zscaler), tráfico ajeno a los puestos que utilice el Servicio BT Managed Cloud Security (Zscaler), cambios en la red del Cliente, etc.). El Cliente y BT acordarán un plan de reducción del ancho de banda o el Cliente solicitará capacidad adicional (gigabytes adicionales de tráfico mensual que se prorratearán y coincidirán con el Periodo mínimo de servicio vigente en ese momento.

10.2 Si el Cliente no reduce su tráfico mensual o solicita capacidad adicional (por ejemplo, puestos, servidores y/o gigabytes adicionales de tráfico mensual) en un plazo de noventa (90) días a partir de la notificación, se le facturará la capacidad adicional necesaria a partir de la fecha de notificación.

11 Software de Servicio

BT y su Proveedor no garantizan que el Software de Servicio para acceder al Portal del Cliente esté libre de fallos; pero BT y su Proveedor harán todo lo razonablemente posible para resolver cualquier problema sin demoras indebidas.

12 Responsabilidades del Cliente

12.1 El Cliente será responsable de lo siguiente:

12.1.1 facilitar a BT los nombres y datos de contacto de los Administradores autorizados para actuar en nombre del Cliente en asuntos relacionados con la gestión del Servicio ("**Contacto del Cliente**") suministro y mantenimiento y pago de su conexión de acceso a Internet o de cualquier equipo necesario para realizar dicha conexión;

12.1.2 notificar cualquier Incidencia en las conexiones a Internet o de las conexiones a Internet compatibles directamente a BT;

12.1.3 dirigir solicitudes externas HTTP, HTTPS y FTP sobre HTTP (incluidos todos los archivos adjuntos, macros o ejecutables) a través del Servicio. Los ajustes de configuración necesarios para dirigir este tráfico externo a través del Servicio son realizados y mantenidos por el Cliente (con la asistencia y el soporte de BT según sea razonablemente necesario) y dependen de la infraestructura técnica del Cliente. El Cliente debe asegurarse de que el tráfico HTTP/HTTPS/FTP sobre HTTP interno (por ejemplo, a la intranet corporativa) no se dirija a través del Servicio;

12.1.4 suministrar a BT cualquier dato técnico y cualquier otra información que BT pueda solicitar de vez en cuando para permitir a BT suministrar el Servicio;

12.1.5 informar a BT con 14 días de antelación y proporcionar detalles de cualquier cambio en la red del Cliente que pueda afectar al funcionamiento del Servicio. Si no se proporciona esta información, BT puede retrasarse o no ser capaz de organizar cualquier cambio necesario en la configuración del Servicio y no tendrá ninguna responsabilidad por dicho retraso o fallo;

12.1.6 crear sus propias combinaciones de inicio de sesión/contraseña ("**ID")** para el acceso al Portal del Cliente para su uso por el Cliente o sus Usuarios. A discreción del Cliente, éste podrá asignar una (1) combinación de inicio de sesión al personal de BT. El Cliente es responsable del uso de estos ID por parte de sus Usuarios y de la descarga e instalación del Software en caso necesario;

12.1.7 todos los aspectos de la configuración de la política de seguridad, incluida la configuración de los grupos de usuarios que puedan ser necesarios en el servidor de autenticación del Cliente, que éste reflejará en su política de seguridad. Esto se realiza a través del Portal del Cliente. Cuando el Cliente haya solicitado a BT que configure la política de seguridad, BT lo hará, antes de la Fecha de Servicio Operativo, y posteriormente, con un Cargo adicional, y el Cliente será responsable de definir la política de seguridad del Cliente y de cualquier consecuencia derivada de una especificación errónea de los requisitos de seguridad del Cliente, o de consecuencias imprevistas de una configuración del Servicio que contenga especificaciones erróneas pero que BT implemente correctamente;

12.1.8 garantizar que cada Suscripción de Usuario adquirida por el Cliente será utilizada únicamente por un único Usuario individual y que una Suscripción de usuario nunca podrá ser compartida ni utilizada por más de una persona. El Cliente reconoce y acepta que una Suscripción de usuario solo podrá transferirse de una persona a otra si la persona original ya no tiene permiso para acceder, y ya no accede, a Internet en relación con el Servicio BT Managed Cloud Security(Zscaler).

12.1.9 asegurarse de solicitar las características del servicio BT Managed Cloud Security (Zscaler) adecuadas a sus necesidades;

12.1.10 llevar a cabo todas sus demás responsabilidades establecidas en este Anexo de forma puntual y eficiente. Si se produce algún retraso en el cumplimiento de las responsabilidades del Cliente, BT podrá ajustar cualquier calendario o programa de entrega acordado según sea razonablemente necesario;

12.1.11 cuando proceda, la implementación de Zscaler Client Connector en los dispositivos de los Usuarios y la configuración y gestión de todos los ajustes relevantes para Zscaler Client Connector.

12.1.12 cuando el Cliente solicite la opción de Mitigación Cooperativa con Nivel de Servicio Graduado Premium; el Cliente deberá:

(a) acordar en el Pedido que BT está autorizada a no tomar Medidas de Mitigación en relación con controles de seguridad específicos y, en su caso, Dispositivos de punto final o Identidades de Usuario Final específicos

(b) seleccionar en el Pedido si se realiza de forma automát9ica 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 Identidades de Usuario Final que requieran Mitigación Cooperativa y notificar a BT cualquier cambio posterior en dichas credenciales

12.2 **Uso aceptable del proveedor**

12.2.1 El Cliente utilizará el Servicio BT Managed Cloud Security (Zscaler) únicamente para fines comerciales del Cliente y solo permitirá el acceso al Servicio BT Managed Cloud Security (Zscaler) a los empleados, agentes y terceros autorizados por el Cliente para utilizar el Servicio BT Managed Cloud Security (Zscaler).

12.2.2 El Cliente no permitirá ni animará a los Usuarios a:

(a) modificar, copiar o realizar trabajos derivados basados en la Tecnología del Proveedor;

(b) desensamblar, aplicar ingeniería inversa o descompilar cualquier parte de la Tecnología del Proveedor;

(c) crear "**enlaces" de** Internet hacia o desde el Servicio BT Managed Cloud Security (Zscaler), o "**enmarcar**" o "**reflejar"** cualquier contenido del Proveedor que forme parte del Servicio BT Managed Cloud Security (Zscaler) (que no sea en la propia intranet interna del Cliente); o bien

(d) utilizar el servicio BT Managed Cloud Security (Zscaler) para realizar consultas automáticas a sitios web.

12.2.3 El Cliente cumplirá con la Política de Uso Aceptable del Proveedor tal y como se establece en el Apéndice 1.

12.2.4 BT o el Proveedor podrán bloquear las direcciones IP de origen o suspender el acceso del Cliente al Servicio BT Managed Cloud Security (Zscaler) si el uso que hace el Cliente del Servicio BT Managed Cloud Security (Zscaler) no cumple este Anexo de Servicio o el Contrato.

12.3 **Jurisdicciones prohibidas**

12.3.1 Además de cualesquiera otras obligaciones de cumplimiento; el Cliente no accederá ni permitirá que los Usuarios del Cliente accedan o utilicen el Servicio BT Managed Cloud Security (Zscaler) directa o indirectamente infringiendo cualquier ley de control de exportaciones o sanciones económicas de EE.UU. u otras leyes aplicables; ("**Jurisdicción prohibida**").

12.3.2 El Cliente garantiza que:

(a) el Cliente no figura en ninguna lista del Gobierno de EE.UU. de personas o entidades a las que se prohíbe recibir exportaciones de EE.UU. o realizar transacciones con cualquier persona de EE.UU.; y

(b) el Cliente no es un nacional de, o una empresa registrada en cualquier Jurisdicción Prohibida.

13 Notificación de Incidencias

Cuando el Cliente tenga conocimiento de una Incidencia:

13.1 el Contacto del Cliente informará al Service Desk de BT;

13.2 BT entregará al Cliente un Ticket;

13.3 BT informará al Cliente cuando considere que se ha resuelto la Incidencia y cerrará el Ticket de problema cuando:

(a) el Cliente confirme que la Incidencia se ha resuelto en un plazo de veinticuatro (24) horas desde que fue informado; o bien

(b) BT ha intentado sin éxito ponerse en contacto con el Cliente, de la forma acordada entre ambos, en relación con la Incidencia y el Cliente no ha respondido en un plazo de veinticuatro (24) horas desde el intento de BT de ponerse en contacto con el Cliente.

13.4 Si el Cliente confirma que la Incidencia no se ha resuelto en un plazo de veinticuatro (24) horas tras ser informado, el Ticket permanecerá abierto, y BT seguirá esforzándose por resolver la Incidencia, hasta que el Ticket se cierre según lo establecido en el Apartado 13.3.

13.5 Cuando BT tenga conocimiento de una Incidencia, se aplicarán los Apartados 13.1 y 13.4.

14 Cambios en los requisitos del cliente / Solicitud de Adición de Servicio

14.1 El Cliente podrá presentar una Solicitud de Adición de Servicio para solicitar a BT:

14.1.1 realizar algún cambio en el Servicio BT Managed Cloud Security (Zscaler) existente;

14.1.2 aumentar el número de Usuarios que utilizan el servicio BT Managed Cloud Security (Zscaler); y/o

14.1.3 seleccionar Funciones Adicionales además de las seleccionadas como parte del Pedido inicial del Cliente,

y cuando BT acepte el cambio, el Cliente pagará los cargos adicionales.

14.2 Si el número de Usuarios supera el límite ordenado, según demuestre BT a través de los informes de gestión, BT lo notificará al Cliente y las Partes podrán:

14.2.1 Acordar un nuevo Pedido con el mayor número de Usuarios y los nuevos Cargos en un plazo de 30 días; o bien

14.2.2 Acordar que el Cliente reduzca el número de Usuarios que utilizan el Servicio BT Managed Cloud Security (Zscaler) en un plazo de cinco (5) Días Hábiles a partir de la fecha, cuando cualquiera de las partes declare que no hay acuerdo sobre un aumento del Pedido y los nuevos Cargos.

14.3 Si las Partes acuerdan aumentar el número de Usuarios y/o seleccionar Funciones Adicionales a las seleccionadas como parte del pedido inicial del Cliente:

(a) más de seis meses antes de que finalice el Período Mínimo del Servicio BT Managed Cloud Security (Zscaler) o el Período de Renovación, será necesario acordar nuevos Cargos (incrementados) en el nuevo Pedido acordado; o bien

(b) menos de seis (6) meses antes de que finalice el Período mínimo del Servicio BT Managed Cloud Security (Zscaler) o el Período de Renovación, será necesaria la revisión y aceptación por parte de BT.

14.4 El Cliente no reducirá el número de Usuarios, Suscripciones de Usuario o componentes del Servicio BT Managed Cloud Security (Zscaler) en ningún momento después de la Fecha de Servicio Operativo.

14.5 Cuando el Cliente haya solicitado la Mitigación Cooperativa con Servicio de Grado Premium, el Cliente podrá anular la selección de la opción de Mitigación Cooperativa del Servicio total o parcialmente en cualquier momento, sujeto a lo siguiente:

(a) el Cliente lo notificará a BT y BT confirmará la fecha a partir de la cual se desactivará el componente de Medida de Mitigación del Servicio;

(b) el Cliente eliminará las credenciales de acceso de BT al Dispositivo de punto final o a las Identidades de Usuario Final;

(c) a partir de la fecha de desactivación, el Cliente será responsable de implementar cualquier Medida de Mitigación que BT recomiende; y

(d) como aclaración, la anulación de la selección de la opción de Mitigación Cooperativa del Servicio no dará lugar a ninguna reducción de los Cargos pagaderos en función del Nivel de Servicio seleccionado.

15 Condiciones de Cargos y Pagos

15.1 El Cliente abonará los Cargos de conformidad con las Condiciones Generales del Contrato.

15.2 Salvo que se indique lo contrario en un Pedido aplicable, BT facturará al Cliente a partir de la Fecha de Servicio Operativo por:

15.2.1 Cualquier gasto de instalación detallado en el pedido;

15.2.2 Cargos recurrentes por:

(a) la licencia de Software de Servicio aplicable;

(b) para las Suites y Prestaciones Adicionales aplicables, incluido el uso de Centros de Datos de Recargo si el Cliente lo solicita;

Los cargos se facturarán mensualmente por adelantado. Cuando el Servicio BT Managed Cloud Security (Zscaler) se preste durante un periodo inferior al periodo de facturación correspondiente, los Cargos recurrentes se calcularán sobre una base mensual o diaria, según corresponda.

15.2.3 Cualquier otro Cargo según lo establecido en cualquier Orden aplicable; por ejemplo, Cargos adicionales por acelerar la prestación del Servicio BT Managed Cloud Security (Zscaler) a petición del Cliente.

15.2.4 Cualquier cargo por rescisión de conformidad con el apartado 16 del presente Anexo:

15.3 BT podrá facturar al Cliente cualquiera de los siguientes Cargos, además de los establecidos en el Pedido:

15.3.1 Gastos de investigación de Incidencias comunicadas por el Cliente, en las que BT no encuentra ninguna Incidencia o que la Incidencia está fuera del Límite de Gestión del Servicio;

15.3.2 Cargos por la puesta en servicio del servicio BT Managed Cloud Security (Zscaler) fuera del Horario Comercial;

15.3.3 Cargos por restablecer el Servicio BT Managed Cloud Security (Zscaler) si el Servicio BT Managed Cloud Security (Zscaler) se ha suspendido de conformidad con el Contrato; o bien

15.3.4 Cargos por cancelar el Servicio BT Managed Cloud Security (Zscaler) de acuerdo con las Condiciones Generales.

16 Gastos de cancelación

16.1 Si el Cliente ejerce su derecho en virtud de las Condiciones generales a rescindir el Servicio BT Managed Cloud Security (Zscaler) por conveniencia, el Cliente deberá pagar:

16.1.1 todos los cargos pendientes por los servicios prestados de BT Managed Cloud Security (Zscaler).

16.1.2 todos los gastos adicionales en los que BT incurra por parte del Proveedor debido a la rescisión anticipada, si procede.

16.2 Además de los Cargos establecidos en el Apartado 16.1 anterior, si el Cliente rescinde durante el Periodo mínimo de servicio, el Cliente pagará a BT por cualquier parte del Servicio de seguridad en la nube gestionado por BT (Zscaler) que se haya rescindido durante el Periodo mínimo de servicio, una compensación igual a:

(a) el 100% de los Cargos Recurrentes de los meses restantes de los primeros doce (12) Meses del Período Mínimo de Servicio; y

(b) 50 por ciento de los Cargos Recurrentes por los meses restantes del Período Mínimo de Servicio, distintos de los establecidos en el Párrafo 16.2(a) anterior; y

(c) los gastos de instalación a los que se haya renunciado.

16.3 En caso de cancelación anticipada del Servicio BT Managed Cloud Security (Zscaler) durante un Periodo de renovación, se aplicarán las mismas tarifas de cancelación.

17 Limitaciones de responsabilidad

En variación de la limitación de responsabilidad en los Términos y Condiciones Generales del Acuerdo, la responsabilidad total de cualquiera de las Partes hacia la otra en virtud de este Anexo o en relación con el mismo no superará el 125% del total de todos los Cargos netos pagados por los Servicios BT Managed Cloud Security (Zscaler).

18 Niveles de Servicio

18.1 **Disponibilidad de Nivel de Servicio**

18.1.1 A partir de la Fecha de Servicio Operativo, BT proporcionará el Servicio BT Managed Cloud Security (Zscaler) con una disponibilidad objetivo del 99,999% del total de horas durante cada mes que el Cliente utilice el Servicio BT Managed Cloud Security (Zscaler).

18.1.2 la Disponibilidad de Nivel de Servicio es una relación entre el número de transacciones y sesiones procesadas por el servicio BT Managed Cloud Security (Zscaler) en cualquier mes natural y el número de transacciones y sesiones cualificadas que deberían haberse procesado.

18.1.3 El Proveedor medirá el número de Transacciones y Sesiones. Las siguientes Transacciones y Sesiones no se tendrán en cuenta para la Disponibilidad de Nivel de Servicio:

(a) Transacciones y Sesiones encriptadas, encapsuladas, tunelizadas, comprimidas, modificadas de su forma original para su distribución; y/o

(b) Transacciones y Sesiones que tienen protección de licencia de producto; y/o

(c) Transacciones y sesiones que están bajo el control directo del remitente (por ejemplo, protegidas por contraseña). y/o

(d) Transacciones y sesiones que se producen durante los periodos de mantenimiento programado de Zscaler, tal y como se publica en el portal de confianza: https://trust.zscaler.com/.

18.1.4 Para evitar cualquier duda, no se ofrecerá ninguna Disponibilidad de Nivel de Servicio ni Crédito de Servicio de Disponibilidad en relación con el Servicio Eagle-i.

18.1.5 Disponibilidad Créditos de Servicio

Si no se cumple la Disponibilidad de Nivel de Servicio, el Cliente podrá reclamar un Crédito de Servicio de Disponibilidad de la siguiente manera:

Porcentaje de transacciones y sesiones procesadas durante un mes	Disponibilidad Crédito de servicio
>= 99.999%	No se aplica el crédito por servicio de disponibilidad.
< 99,999% pero >= 99,99%.	(3 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Disponibilidad.
< 99,99% pero >= 99,00%.	(7 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Disponibilidad.
< 99,00% pero >= 98,00%.	(15 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la solicitud de Crédito de Servicio de Disponibilidad.
< 98.00%	(30 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la solicitud de Crédito de Servicio de Disponibilidad.

18.2 **Nivel de Servicio de Latencia**

18.2.1 A partir de la Fecha de Servicio Operativo, BT proporcionará el Servicio BT Managed Cloud Security (Zscaler) para procesar:

(a) para cualquier otro, Transacciones y Paquetes de datos con una latencia media durante un mes natural de 100 milisegundos o menos para el percentil 95 del tráfico.

18.2.2 El Nivel de Servicio de Latencia sólo se aplicará a las Transacciones si:

(i) menos de 1 MB de solicitud y respuesta HTTP GET;
(ii) no interceptado por SSL;
(iii) no relacionados con aplicaciones de streaming;
(iv) no sujetos a normas de gestión del ancho de banda (aplicación de la QoS); y
(v) haya un número razonable de Transacciones por Suscripción de Usuario (basado en la media del Proveedor en toda la nube).

18.2.3 BT (a través del Proveedor) medirá el procesamiento del contenido desde el momento en que el proxy del Proveedor recibe el contenido hasta el momento en que el proxy del Proveedor intenta transmitir el contenido.

18.2.4 Para evitar dudas, no se ofrecerá ningún Nivel de Servicio de Latencia ni Crédito de Servicio de Latencia en relación con el Servicio Eagle-i.

18.3 **Nivel de Servicio Tasa de Captura de Virus**

18.3.1 A partir de la Fecha de Servicio Operativo, BT proporcionará el Servicio BT Managed Cloud Security (Zscaler) con el objetivo de capturar el 99,999% de los Virus Conocidos durante un mes natural.

18.3.2 El Nivel de Servicio de Tasa de Captura de Virus se aplica al servicio BT Managed Cloud Security (Zscaler).

18.3.3 El Nivel de Servicio de Tasa de Captura de Virus sólo se aplica si:

(a) el Cliente utiliza el Servicio BT Managed Cloud Security (Zscaler) de acuerdo con la configuración antivirus recomendada en la interfaz de usuario del Cliente; y
(b) un Virus Conocido contenido en una Transacción recibida a través del Servicio BT Managed Cloud Security (Zscaler) se ha activado dentro de los sistemas del Cliente, ya sea automáticamente o con intervención manual.

18.3.4 En caso de que BT (o el Proveedor) detecte un Virus Conocido pero no lo detenga, BT lo notificará inmediatamente al Cliente, proporcionándole información suficiente para que pueda identificar y eliminar el virus conocido. Si el Cliente no actúa con prontitud a partir de esta información, el Crédito de Servicio puede quedar invalidado.

18.3.5 En caso de que se produzca dicha notificación BT y una acción posterior por parte del Cliente resulte en la prevención de la infección, no se aplicará el Nivel de Servicio de Tasa de Captura de Virus.

18.3.6 BT (a través del Proveedor) calculará la Tasa de Captura de Virus dividiendo las Transacciones infectadas por virus bloqueadas por el total de Transacciones infectadas por virus recibidas por el Servicio BT Managed Cloud Security (Zscaler) en nombre del Cliente.

18.3.7 Para evitar cualquier duda, no se ofrecerá ningún Nivel de servicio de tasa de captura de virus ni ningún Crédito de servicio de tasa de captura de virus en relación con el Servicio Eagle-i.

18.3.8 Créditos de servicio de tasa de captura de virus. Si no se cumple el Nivel de Servicio de la Tasa de Captura de Virus, el Cliente podrá reclamar un Crédito de Servicio de la Tasa de Captura de Virus de la siguiente manera:

Tasa de captura de virus	Crédito del servicio de captura de virus
>= 99.999%	No hay Crédito de Servicio de Tasa de Captura de Virus disponible.
< 99,999% pero >= 99,00%.	(7 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Tasa de Captura de Virus.
< 99,00% pero >= 98,00%.	(15 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Tasa de Captura de Virus.
< 98.00%	(30 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Tasa de Captura de Virus.

18.4 **Nivel de Servicio de Zscaler Private Access**

18.4.1 A partir de la Fecha de Servicio Operativo, BT proporcionará Zscaler Private Access con una disponibilidad objetivo del 99,999% del total de horas durante cada mes que el Cliente utilice Zscaler Private Access ("Nivel de **Servicio de Zscaler Private Access**").

18.4.2 Créditos de Servicio de Zscaler Private Access. Si no se cumple el Nivel de Servicio de Zscaler Private Access, el Cliente podrá reclamar un Crédito de Servicio de Zscaler Private Access de la siguiente manera:

Porcentaje de transacciones y sesiones procesadas durante un mes	Créditos de Servicio de Zscaler Private Access
>= 99.999%	No se aplica el Crédito de Servicio de Zscaler Private Access.
< 99,999% pero >= 99,99%.	(3 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Zscaler Private Access.
< 99,99% pero >= 99,00%.	(7 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Zscaler Private Access.
< 99,00% pero >= 98,00%.	(15 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Zscaler Private Access.
< 98.00%	(30 / 30) x el Cargo recurrente mensual de la parte correspondiente del Servicio BT Managed Cloud Security (Zscaler) en el mes inmediatamente anterior a la Incidencia que da lugar a la reclamación de Crédito de Servicio de Zscaler Private Access.

18.4.3 Para evitar dudas, no se ofrecerá ningún Nivel de Servicio de Zscaler Private Access ni Crédito de Servicio de Zscaler Private Access en relación con el Servicio Eagle-i.

18.5 **Nivel de Servicio de Entrega Puntual**

En caso de que el Cliente haya solicitado Soporte Plus o Premium, BT proporcionará el siguiente Nivel de Servicio adicional para la Entrega Puntual:

18.5.1 BT hará todo lo razonablemente posible para entregar el Servicio BT Managed Cloud Security (Zscaler) en la Fecha Comprometida con el cliente o antes, según lo acordado con el Cliente. El Nivel de Servicio de Entrega Puntual no se aplica a las actualizaciones o cambios del Servicio BT Managed Cloud Security (Zscaler), a menos que estos tengan una nueva fecha de entrega acordada, en cuyo caso la Fecha Comprometida con el cliente será dicha fecha de entrega acordada. BT puede acelerar la entrega del Servicio BT Managed Cloud Security (Zscaler) por motivos operativos o en respuesta a una solicitud del Cliente, pero esto no revisará la Fecha Comprometida con el cliente.

18.5.2 Créditos de Servicio de Entrega Puntual. Si BT no cumple el Nivel de Servicio de Entrega Puntual, el Cliente podrá reclamar un Crédito de Servicio equivalente a 100,00 EUR por Día Hábil de retraso, calculado desde la Fecha Comprometida con el Cliente acordada hasta la Fecha de Servicio Operativo de dicho Servicio BT Managed Cloud Security (Zscaler), y ello hasta un importe máximo igual a los Cargos de Instalación de dicho Servicio BT Managed Cloud Security (Zscaler).

19 Solicitudes de Créditos de Servicio

19.1 Para poder optar a los Créditos de Servicio, y antes de que se pueda aplicar cualquier Crédito de Servicio, el Cliente debe presentar una reclamación en un plazo de 25 días tras el final del mes en el que el **Servicio BT Managed Cloud Security (Zscaler)** haya tenido un rendimiento inferior al esperado o, en caso de que la legislación local obligatoria exija un periodo de tiempo superior, el periodo más breve que se pueda aplicar.

19.2 Una vez recibida una solicitud válida de Créditos de Servicio, BT revisará la validez de la solicitud y:

(a) BT realizará estas revisiones mensualmente;
(b) si la solicitud de Créditos de Servicio no fuera válida, BT lo notificará al Cliente;
(c) si la solicitud de Créditos de Servicio es válida, BT notificará al Cliente el Crédito de servicio adeudado:
(d) BT deducirá los Créditos de Servicio de la factura del Cliente en el plazo de dos (2) ciclos de facturación desde la recepción de la solicitud; y
(e) tras el vencimiento o la finalización del Servicio BT Managed Cloud Security (Zscaler) cuando BT no deba emitir más facturas, BT abonará los Créditos de Servicio al cliente en un plazo de dos (2) meses.

19.3 El siguiente es un ejemplo de cálculo de Crédito de Servicio donde:

(a) el Cargo Recurrente mensual es de 50.000 euros al mes; y
(b) el Crédito de Servicio debido es de tres (3) días.
(c) BT concederá un crédito en la siguiente factura de 50.000 euros/30 días x 3 días, es decir, 5.000 euros.

19.4 Los Créditos de Servicio para todos los Niveles de Servicio se sumarán y estarán disponibles hasta un importe máximo igual al 100 % del Cargo neto recurrente mensual para el Servicio BT Cloud Managed Security (Zscaler) afectado.

19.5 Todos los Niveles de Servicio y Créditos de Servicio se calcularán de acuerdo con la información registrada por BT, o por el Proveedor en nombre de BT.

19.6 Los siguientes elementos están excluidos del cálculo de los Niveles de Servicio de Disponibilidad:

(a) La red del cliente no está reenviando tráfico al servicio BT Managed Cloud Security (Zscaler); o bien
(b) un ISP intermedio (distinto de los ISP directos del Servicio BT Managed Cloud Security (Zscaler)) no está entregando tráfico al Servicio BT Managed Cloud Security (Zscaler); o bien
(c) el descenso de las Transacciones y Sesiones se debe a un cambio de política solicitado por el cliente; o
(d) no es técnicamente posible escanear el tráfico del Cliente; por ejemplo, elementos que
(ii) se encriptan, encapsulan, tunelizan, comprimen, modifican de su forma original para su distribución; y/o
(iii) tienen protección de licencia de producto; y/o
(iv) están bajo el control directo del remitente (por ejemplo, protegidos por contraseña).

19.7 No se aplicarán los Niveles de Servicio:

(a) cuando la red del Cliente no esté configurada correctamente 24 horas al día x 7 días a la semana x 365 días al año de forma que permita al Cliente hacer uso de la infraestructura global redundante del Proveedor que se pone a su disposición como parte del Servicio BT Managed Cloud Security (Zscaler). BT se lo comunicará al Cliente en el momento en que ponga en servicio el Servicio BT Managed Cloud Security (Zscaler);
(b) durante cualquier periodo de prueba del servicio BT Managed Cloud Security (Zscaler);
(c) a fallos debidos a cualquier Acontecimiento de Fuerza Mayor;
(d) si el Cliente provoca un retraso o no facilita la información solicitada en los plazos acordados;
(e) a cualquier Incidencia no notificada de conformidad con este Anexo; o
(f) si el Cliente incumple las condiciones del Contrato.
(g) si la Incidencia fue consecuencia de Cambios Simples implementados por el Cliente a través de la Opción de Servicio de Cogestión.

19.8 Sin renunciar a ningún otro derecho que el Cliente tenga en virtud del Acuerdo, reconoce que las reclamaciones de Crédito de Servicio de Disponibilidad son el único recurso del Cliente si BT y/o el Proveedor no cumplen el Nivel de Servicio de Disponibilidad aplicable.

20 Protección de Datos Personales

20.1 Condiciones aplicables. Las Partes acuerdan que está previsto que BT y el Proveedor puedan recibir o tratar Datos Personales en nombre del Cliente como Encargado de Tratamiento de Datos en relación con el Servicio

o como resultado de la prestación de este Servicio. Todos los Datos del Cliente están sujetos a la cláusula "Datos" establecida en el Contrato.

20.2 La naturaleza y la finalidad del Tratamiento de los Datos Personales del Cliente por parte de BT;

(a) El Servicio BT Managed Cloud Security (Zscaler) permite al cliente establecer reglas para bloquear URL y filtrar contenido web en sus sistemas de TI. El software en sí lo proporciona el Proveedor y se aloja en la infraestructura de nube pública de dicho Proveedor, sin que BT pueda acceder a la información subyacente. El Cliente puede elegir que sus registros de transacciones se almacenen en el EEE y Suiza utilizando los siguientes centros de datos centrales: (1) Interxion Deutschland GmbH en Fráncfort, Alemania; (2) Equinix (Países Bajos) B.V. en Ámsterdam, Países Bajos; y (3) Equinix (Suiza) GmbH en Zúrich, Suiza. La siguiente URL ofrece una descripción completa de los subencargados utilizados por el proveedor: https://www.zscaler.com/legal/subprocessors.

(b) Con la ventana superpuesta del Servicio BT Managed Security, BT tendrá acceso a través del portal en línea a un registro de las direcciones IP y MAC del Cliente, junto con los intentos de URL o visitas a sitios web por parte de dichas direcciones, con el fin de proporcionar informes al Cliente. BT no tiene acceso a más datos que los de este portal.

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

- sitio web o dirección IP;
- nombre;
- dirección;
- número de teléfono;
- dirección de correo electrónico;
- puesto de trabajo;
- nombre de la empresa;
- registros de contacto;
- registros de uso (registros de llamadas, de Internet o del router);
- registros de transacciones, y
- gestión de identidades - perfiles de usuario.

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

- los empleados del Cliente;
- los clientes del Cliente o terceros; y
- cualquier Titular de los datos (controlado por el Cliente).

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: (Representante autorizado)	Firmado: (Representante autorizado)
(Nombre)	Paul Rhodes
Representante legal	Representante legal

Apéndice 1 al Servicio BT Managed Cloud Security (Zscaler)

Política de Uso Aceptable de Zscaler

Esta Política de Uso Aceptable ("PUA") describe los usos aceptables de los servicios y productos Zscaler ("Productos"). Esta PUA prohíbe usos y actividades que involucren los Productos que sean ilegales, infrinjan los derechos de otros, o interfieran o disminuyan el uso y disfrute de los Productos por otros. Por ejemplo, estos usos y actividades prohibidos incluyen el uso de los Productos para:

Restricciones de conducta e información

- Emprender o llevar a cabo cualquier propósito ilegal. Esto incluye, pero no se limita a, publicar, almacenar, transmitir o difundir información, datos o material que sea calumnioso, obsceno, ilegal, amenazador o difamatorio, o que infrinja los derechos de propiedad intelectual de cualquier persona o entidad, o que de alguna manera constituya o fomente una conducta que constituiría un delito penal, o que viole cualquier ley, orden o reglamento local, estatal, federal o no estadounidense;
- Cargar, enviar, publicar, transmitir, reproducir, crear trabajos derivados o distribuir de cualquier forma información, software u otro material obtenido a través de los Productos o de cualquier otro modo que esté protegido por derechos de autor u otros derechos de propiedad, sin obtener el permiso necesario del propietario;
- Transmitir mensajes masivos o comerciales no solicitados, comúnmente conocidos como "spam".
- Enviar un número muy elevado de copias del mismo mensaje o de mensajes sustancialmente similares, mensajes vacíos o sin contenido sustancial, o enviar mensajes o archivos muy grandes que perturben un servidor, cuenta, blog, grupo de noticias, chat o servicio similar;
- Participar en la recopilación de un gran número de direcciones de correo electrónico, nombres de pantalla u otros identificadores de otras personas (sin su consentimiento previo), una práctica a veces conocida como spidering o harvesting, o participar en el uso de software (incluido el "spyware") diseñado para facilitar esta actividad;
- Falsificar, alterar o eliminar las cabeceras de los mensajes;
- Hacerse pasar por otra persona o entidad, falsificar la dirección del remitente, falsificar la firma digital o manual de otra persona o realizar cualquier otra actividad fraudulenta similar (por ejemplo, "phishing");

Restricciones técnicas

- Acceder al ordenador o sistema informático, red, software o datos de otra persona sin su conocimiento y consentimiento; vulnerar la seguridad de otro usuario o sistema; o intentar burlar la autenticación de usuario o la seguridad de cualquier host, red o cuenta. Esto incluye, pero no se limita a, acceder a datos no destinados a usted, iniciar sesión o hacer uso de un servidor o cuenta a los que no esté expresamente autorizado a acceder, o sondear la seguridad de otros hosts, redes o cuentas sin permiso expreso para hacerlo;
- Utilizar o distribuir herramientas o dispositivos diseñados o utilizados para comprometer la seguridad o cuyo uso no esté autorizado por otros motivos, como programas para adivinar contraseñas, descodificadores, recopiladores de contraseñas, registradores de pulsaciones de teclas, analizadores, herramientas de cracking, rastreadores de paquetes, dispositivos para eludir el cifrado o programas troyanos. El escaneo de puertos no autorizado está estrictamente prohibido;
- Copiar, distribuir o sublicenciar cualquier software propietario proporcionado en conexión con los Productos por Zscaler;
- Distribuir programas que realizan cambios no autorizados en el software (cracks);
- Alterar, modificar o manipular los Productos o permitir que lo haga cualquier otra persona no autorizada por Zscaler;

Restricciones de red y uso

- Restringir, inhibir o interferir de cualquier otro modo en la capacidad de cualquier otra entidad para utilizar o disfrutar de los Productos, incluyendo la publicación o transmisión de cualquier información o software que contenga un gusano, virus u otra característica dañina, o la generación de niveles de tráfico suficientes para impedir la capacidad de otros para utilizar, enviar o recuperar información;
- Restringir, inhibir, interferir o de otro modo interrumpir o causar una degradación del rendimiento de los Productos o de cualquier host, servidor, red troncal, nodo o servicio de Zscaler (o proveedor de Zscaler), o de otro modo causar una degradación del rendimiento de cualquier instalación de Zscaler (o proveedor de Zscaler) utilizada para suministrar los Productos;
- Interferir con la red informática o el servicio de telecomunicaciones a cualquier usuario, host o red, incluyendo, sin limitación, ataques de denegación de servicio, inundación de una red, sobrecarga de un servicio, apropiación indebida y abuso de privilegios de operador, e intentos de "colapsar" un host.

ZSCALER SE RESERVA EL DERECHO DE NOTIFICAR A SUS CLIENTES CUALQUIER INFORMACIÓN QUE AFECTE A LA SEGURIDAD DE LOS PRODUCTOS.

Si tiene alguna pregunta sobre esta PUA, póngase en contacto con Zscaler de la siguiente manera:

Zscaler, Inc.
ATTN: Departamento Jurídico
110 Rose Orchard Way
San José, CA 95134, EE.UU.

Correo electrónico: contracts@zscaler.com

Apéndice 2 del Servicio BT Managed Cloud Security (Zscaler)

Cambios Simples y Complejos

Nota: Dado que cualquier cambio no calificado como "Simple" en la siguiente tabla será un Cambio Complejo, los Cambios Complejos enumerados a continuación son ejemplos no exhaustivos.

Simple (también conocidas como SSR - Simple Service Requests)

Cambia	Mecanismo para solicitar cambios
Actualizar categoría de URL	Gestor de cambios de seguridad de BT
Cambio para resolver la/s incidencia/es	Gestor de cambios de seguridad de BT
Cambiar las reglas de filtrado de URL	Gestor de cambios de seguridad de BT
Normas de inspección SSL	Gestor de cambios de seguridad de BT
Añadir/modificar cuenta de administrador (ZIA)	Gestor de cambios de seguridad de BT
Restablecer la contraseña de la cuenta de administrador (ZIA)	Gestor de cambios de seguridad de BT
Eliminar la cuenta de administrador	Gestor de cambios de seguridad de BT
Inspección de excepciones de seguridad	Gestor de cambios de seguridad de BT
Cambiar la configuración de la protección antimalware	Gestor de cambios de seguridad de BT
Cambiar la configuración de la protección frente a amenazas avanzadas	Gestor de cambios de seguridad de BT
Control del tipo de archivo	Gestor de cambios de seguridad de BT
Control del navegador	Gestor de cambios de seguridad de BT
Configuración del Sandbox	Gestor de cambios de seguridad de BT
Añadir cuenta de Usuario (SÓLO ZIA)	Gestor de cambios de seguridad de BT
Modificar/eliminar cuenta de Usuario (SÓLO ZIA)	Gestor de cambios de seguridad de BT
Añadir/modificar/eliminar atributos SAML de grupo de Usuarios	Gestor de cambios de seguridad de BT
ZCC (Mobile Portal) - añadir/modificar perfil Linux - no Tunnel 2.0 config	Gestor de cambios de seguridad de BT
ZCC (Mobile Portal) - añadir/modificar perfil MacOS - no Tunnel 2.0 config	Gestor de cambios de seguridad de BT
ZCC (Mobile Portal) - añadir/modificar perfil Windows - no Tunnel 2.0 config	Gestor de cambios de seguridad de BT
ZCC (Mobile Portal) - añadir/modificar Tunnel 2.0 config	Gestor de cambios de seguridad de BT
ZCC (Portal Móvil) - añadir/modificar perfil Android	Gestor de cambios de seguridad de BT
ZCC (Portal Móvil) - añadir/modificar perfil IOS	Gestor de cambios de seguridad de BT
ZCC (Mobile Portal) - eliminar perfil	Gestor de cambios de seguridad de BT
Sublocalización - añadir/modificar/eliminar (SÓLO ZIA)	Gestor de cambios de seguridad de BT
Añadir segmento de aplicación	Gestor de cambios de seguridad de BT
Segmento de aplicación existente - añadir/eliminar aplicación o puertos	Gestor de cambios de seguridad de BT
Política de acceso - añadir/modificar/eliminar	Gestor de cambios de seguridad de BT

Política de tiempo de espera - añadir/modificar/eliminar	Gestor de cambios de seguridad de BT
Añadir/modificar cuenta de administrador (ZPA)	Gestor de cambios de seguridad de BT
Restablecer la contraseña de la cuenta de administrador (ZPA)	Gestor de cambios de seguridad de BT
Política de reenvío de clientes - añadir/modificar/eliminar	Gestor de cambios de seguridad de BT
Cambio para reconstruir conector/es de aplicación fallido/s	Gestor de cambios de seguridad de BT

Complejos no contractuales

Cambia	Mecanismo para solicitar cambios
Ampliar el servicio MCS a un nuevo emplazamiento	Mi cuenta
Asistencia para la integración de identidades	Mi cuenta
Ayuda a la definición de políticas (L)	Mi cuenta
Ayuda a la definición de políticas (M)	Mi cuenta
Ayuda a la definición de políticas (S)	Mi cuenta
Soporte para el descifrado SSL del cliente (L)	Mi cuenta
Compatibilidad con el descifrado SSL del cliente (M)	Mi cuenta
Compatibilidad con el descifrado SSL del cliente (S)	Mi cuenta
Reenvío de tráfico (L)	Mi cuenta
Reenvío de tráfico (M)	Mi cuenta
Reenvío de tráfico (S)	Mi cuenta

Contrato complejo que afecta a

Cambia	Mecanismo para solicitar cambios
Incorporación de la función SKU de Zscaler	Gestionado por el Equipo de Cuentas
Adición de Usuarios	Gestionado por el Equipo de Cuentas
Característica adicional de BT	Gestionado por el Equipo de Cuentas
Cese/Desactualización de Zscaler (inc. cálculo de gastos de rescisión)	Gestionado por el Equipo de Cuentas
Modificar la duración del contrato	Gestionado por el Equipo de Cuentas
Fundación - paso de SIP a Profesional	Gestionado por el Equipo de Cuentas
Traslado de Niveles de Servicio GSM: de Soporte a Soporte Plus o Premium y de Soporte Plus a Premium	Gestionado por el Equipo de Cuentas