MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GOTOASSIST REMOTE SUPPORT v5

(ANTERIORMENTE, RESCUEASSIST)

CONTROLES OPERATIVOS DE SEGURIDAD Y PRIVACIDAD

Fecha de publicación: febrero de 2022

1 Productos y servicios

Este documento analiza las medidas técnicas y organizativas (TOM) de la infraestructura y los canales de comunicación de GoToAssist Remote Support v5 (anteriormente, RescueAssist).

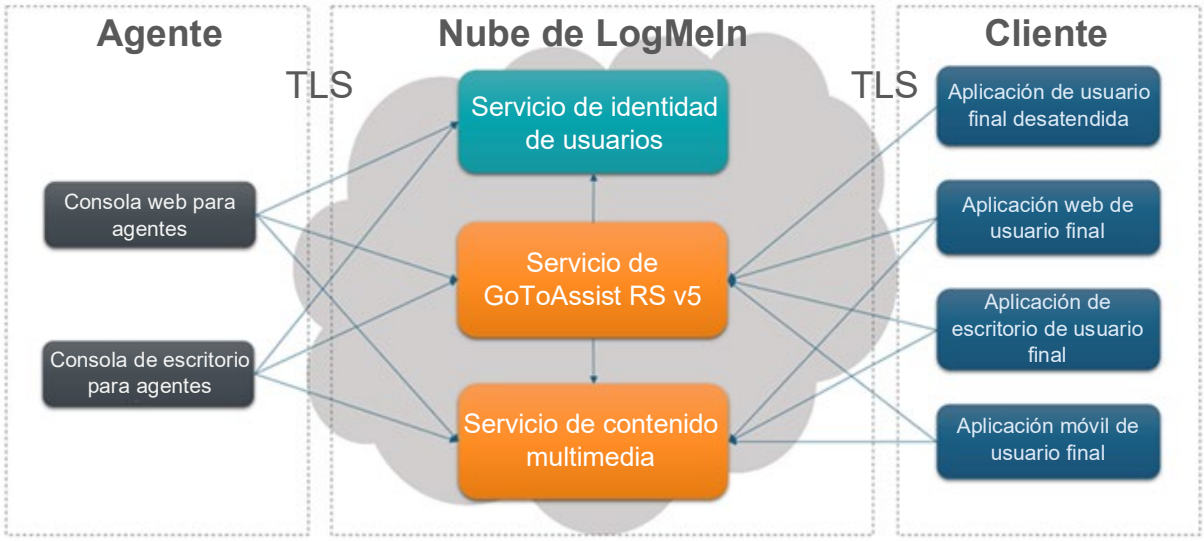
GoToAssist Remote Support v5 permite a los profesionales de TI y de asistencia ofrecer asistencia remota a ordenadores, servidores y dispositivos móviles con funciones de visualización remota, control remoto y uso compartido de la cámara desde una consola para agentes de escritorio o basada en la web. GoToAssist Remote Support v5 emplea medidas de seguridad de datos resistentes para defenderse de ataques tanto pasivos como activos.

2 Arquitectura del producto

GoToAssist Remote Support v5 utiliza un modelo de proveedor de servicios de aplicaciones (ASP) diseñado para proporcionar operaciones seguras a la vez que se integra con la red y la infraestructura de seguridad existentes en la empresa. Su arquitectura está diseñada para ofrecer un rendimiento, una fiabilidad y una escalabilidad óptimos. La arquitectura incorpora conmutadores y enrutadores redundantes para garantizar que no haya un único punto de fallo. Se utilizan servidores en clúster de alta capacidad y sistemas de copia de seguridad para garantizar el funcionamiento continuo de los procesos de las aplicaciones aunque haya cargas pesadas o errores del sistema. Los agentes de servicio equilibran la carga de las sesiones de cliente/servidor entre servidores de comunicación ubicados en distintos puntos geográficos. La arquitectura de comunicaciones de GoToAssist Remote Support v5 se describe en la sección 2.1 a continuación.

2.1. Arquitectura de las comunicaciones

La arquitectura de comunicaciones de GoToAssist Remote Support v5 se resume en la siguiente figura.



La autenticación de agentes utiliza el servicio de identidad de usuarios de GoTo. Las comunicaciones entre los participantes en una sesión de GoToAssist Remote Support v5 se realizan a través de una pila de red superpuesta, situada de forma lógica encima de la pila de TCP/IP y UDP convencional. Esta red la proporcionan el Servicio de GoToAssist Remote Support v5 y el Servicio de contenido multimedia, alojados en Amazon AWS.

Los participantes de la sesión de GoToAssist Remote Support v5 (Consola web para agentes, Consola de escritorio para agentes y terminales del cliente) se comunican con el Servicio de GoToAssist Remote Support v5 y el Servicio de contenido multimedia mediante conexiones TCP salientes en los puertos 443 o UDP 15000, según la disponibilidad. Dado que GoToAssist Remote Support v5 es un servicio basado en la web, los participantes pueden estar situados en prácticamente cualquier lugar de Internet: una oficina remota, una casa, un centro de negocios o la red de otra empresa.

2.2. Consola de escritorio para agentes

Los agentes pueden utilizar la Consola web para agentes o la Consola de escritorio para agentes instalable con la que conectarse al Servicio de GoToAssist Remote Support v5. La consola de escritorio utiliza el conjunto de herramientas multiplataforma Qt para ejecutarse en MacOS y Windows y aprovecha el navegador web de código abierto Chromium para utilizar los componentes de la consola web.

3 Controles técnicos de GoToAssist Remote Support v5

GoTo utiliza controles técnicos de seguridad estándar en el sector, adecuados a la naturaleza y el alcance de los Servicios (tal y como se define el término en las Términos del servicio) y diseñados para proteger la infraestructura del Servicio y los datos que residen en ella. Puede consultar los Términos del servicio en https://www.goto.com/company/legal/terms-and-conditions.

3.1. Autenticación

Los agentes y administradores de cuenta de GoToAssist Remote Support v5 se identifican por su dirección de correo electrónico y se autentican mediante una contraseña. Durante la autenticación autorizada, la contraseña nunca se transfiere en estado no cifrado.

Los procedimientos de autenticación se rigen por las siguientes políticas:

- **Contraseñas seguras:** una contraseña segura debe tener una longitud mínima de 8 caracteres con suficientes requisitos de complejidad (es decir, debe contener tanto letras como números). La seguridad de las contraseñas se comprueba cuando se establecen o cambian.
- **Autenticación de dos factores:** como medida de seguridad adicional, la autenticación de dos factores está disponible de forma opcional en todas las cuentas empresariales de GoToAssist Remote Support v5. Si está activada, la autenticación de dos factores requiere que cada usuario autorice el acceso mediante dos métodos distintos.
- **Bloqueo de la cuenta:** tras cinco intentos fallidos consecutivos de inicio de sesión, la cuenta de usuario pasa a un estado de bloqueo temporal obligatorio. Esto implica

que el titular de la cuenta de usuario no podrá conectarse durante cinco minutos. Una vez transcurrido el periodo de bloqueo, el titular de la cuenta de usuario podrá intentar acceder de nuevo a ella.

3.2. Control de acceso lógico

Existen procedimientos de control de acceso lógicos, diseñados para prevenir o mitigar la amenaza del acceso no autorizado a las aplicaciones y la pérdida de datos en entornos corporativos y de producción. A los empleados se les concede un acceso básico (o con "privilegios mínimos") a los sistemas, las aplicaciones, las redes y los dispositivos GoTo especificados según sea necesario. Además, los privilegios de los usuarios se segregan según el rol funcional y del entorno.

Los usuarios que pueden acceder a los componentes del producto GoToAssist Remote Support v5 son el personal técnico autorizado de GoTo (por ejemplo, Departamento Operaciones Técnicas e Ingeniería DevOps), los administradores del cliente y los usuarios finales del producto. Los servidores de producción locales solo están disponibles desde los hosts de salto o a través de la red privada virtual (VPN) del Departamento de Operaciones. Los componentes de producción en la nube están disponibles a través de la autenticación SSU (Self Service Unix).

3.3. Control de acceso basado en permisos

3.3.1. Sesión realizada

Una parte esencial de la seguridad de GoToAssist Remote Support v5 es su modelo de control de acceso basado en permisos, diseñado para proteger el acceso al ordenador y a los datos del cliente. Durante las sesiones de asistencia en directo a las que asiste el cliente, se le pide permiso antes de iniciar cualquier uso compartido de pantalla, control remoto o transferencia de archivos.

Una vez autorizados el control remoto y la pantalla compartida durante una sesión atendida, el Cliente puede ver lo que hace el agente en todo momento. Además, el servicio está diseñado para que el cliente pueda retomar fácilmente el control o finalizar la sesión cuando quiera.

3.3.2. Sesión desatendida

La asistencia desatendida requiere que la aplicación de Cliente desatendida esté instalada en el dispositivo del Cliente. Puede configurarse de dos maneras, instalación durante la sesión (durante una sesión presencial) o mediante un instalador fuera de sesión, y ambas requieren la aprobación del cliente.

Instalación durante la sesión: una vez que el Cliente y el agente han entrado en una sesión realizada, el agente puede solicitar un permiso adicional para instalar la aplicación de Cliente desatendida. Se solicita la aprobación del Cliente, que debe dar su consentimiento explícito.

Instalador fuera de sesión: Tras iniciar sesión de forma segura en el sitio web de GoToAssist Remote Support v5 o en la aplicación de escritorio, el agente puede descargar un instalador, que permite la instalación de la aplicación de Cliente desatendido en cualquier PC Windows o Mac para el que el agente tenga acceso de administrador.

3.3.3. Seguridad durante la sesión

GoToAssist Remote Support v5 no se ha diseñado para anular los controles de seguridad locales del ordenador del Cliente.

Si el Cliente vuelve a la máquina mientras se está llevando a cabo una sesión desatendida, puede finalizar la sesión y revocar permanentemente los privilegios de asistencia desatendida del agente en cualquier momento.

3.4. Control de acceso basado en funciones

GoToAssist Remote Support V5 proporciona acceso a diversos recursos y servicios mediante un sistema de control de acceso basado en funciones, que ejecutan los componentes de entrega del servicio. Se definen las siguientes funciones:

- **Administrador de cuenta:** usuario de GoToAssist Remote Support v5 con plenos privilegios de administrador para realizar funciones administrativas relativas a los agentes. Los administradores de cuentas pueden crear, modificar y eliminar cuentas de agentes y modificar los datos de suscripción.
- **Agente:** usuario de GoToAssist Remote Support v5. El agente puede iniciar sesiones de GoToAssist Remote Support v5 para proporcionar asistencia técnica a los Clientes a través de la visualización y el control remotos o la cámara compartida.
- **Cliente:** persona no autenticada que solicita asistencia al Agente. El Cliente puede cerrar las sesiones y debe conceder permisos para que el agente acceda a su dispositivo.

3.5. Defensa perimetral y detección de intrusiones

GoTo utiliza herramientas, técnicas y servicios de protección perimetral estándar del sector, diseñados para evitar que el tráfico de red no autorizado entre en la infraestructura de sus productos. La red GoTo cuenta con cortafuegos externos y segmentación de red interna. Los recursos en la nube también utilizan cortafuegos basados en host.

3.6. Segregación de datos

GoTo aprovecha una arquitectura multiusuario, separada de forma lógica a nivel de base de datos, basada en la cuenta GoTo de un usuario o de una organización. Solo las partes autenticadas tienen acceso a las cuentas pertinentes.

3.7. Seguridad física

GoTo contrata a los centros de datos la seguridad física y los controles ambientales de las salas que albergan los servidores de producción. Estos controles incluyen:

- videovigilancia y grabación
- Autenticación multifactor para zonas muy sensibles
- control de la temperatura de calefacción, ventilación y aire acondicionado
- extinción de incendios y detectores de humo
- Sistema de alimentación ininterrumpida (SAI)
- suelos elevados o gestión integral de cables
- supervisión continua y alertas
- Protecciones contra las catástrofes naturales y las provocadas por el hombre más comunes, según lo exijan la geografía y la ubicación del centro de datos en cuestión

- mantenimiento programado y validación de todos los controles críticos de seguridad y medioambientales

GoTo limita el acceso físico a los centros de datos de producción únicamente a las personas autorizadas. El acceso a una sala de servidores local o a una instalación de alojamiento de terceros requiere la presentación de una solicitud a través del sistema de tickets correspondiente y la aprobación del responsable aplicable, así como la revisión y aprobación del Departamento de Operaciones Técnicas. La dirección de GoTo revisa los registros de acceso físico a los centros de datos y las salas de servidores al menos una vez cada trimestre. Además, el acceso físico a los centros de datos se elimina al cesar al personal previamente autorizado.

3.8. Copia de seguridad de datos, recuperación ante desastres, disponibilidad

La arquitectura de GoTo está diseñada para realizar la replicación casi en tiempo real en ubicaciones geográficamente diversas. Las copias de seguridad de las bases de datos se realizan mediante una estrategia de copia de seguridad incremental continua. En caso de desastre o de fallo total del emplazamiento en alguna de las varias ubicaciones activas, las ubicaciones restantes están diseñadas para equilibrar la carga de la aplicación. La recuperación en caso de desastre relacionada con estos sistemas se prueba periódicamente.

3.9. Cifrado

GoTo mantiene una norma de cifrado que se ajusta a las recomendaciones de grupos industriales, publicaciones gubernamentales y otros grupos de normas acreditadas. La norma de cifrado se revisa periódicamente, y las tecnologías y los cifrados seleccionados se actualizan en función del riesgo evaluado y de la aceptación en el mercado de nuevas normas.
Los puntos clave del cifrado en GoToAssist Remote Support v5 incluyen:

- Los datos de sesión de GoToAssist Remote Support v5 están protegidos con cifrado TLS 1.2 (si es compatible) AES de 256 bits en tránsito.
- Las claves de sesión son generadas en el servidor por el agente y permanecen allí para poder conectar al cliente con él. El servicio está diseñado para garantizar que estas claves nunca se muestren ni faciliten al público.
- La comunicación cifrada entre el cliente y el agente en GoToAssist Remote Support v5 se produce a través de una solución de servicio multimedia personalizada.
- Los terminales de la infraestructura de GoToAssist Remote Support v5 utilizan conexiones de seguridad de la capa de transporte (TLS).

3.9.1. Cifrado en tránsito

Para proteger aún más el Contenido del cliente (tal y como se define en los Términos del servicio) mientras está en tránsito, GoTo utiliza protocolos actuales TLS y conjuntos de cifrado asociados.

Las comunicación entre terminal del Cliente y el back-end se cifran mediante OpenSSL. Los controles de seguridad de las comunicaciones basados en un cifrado fuerte se implementan en la capa TCP a través de soluciones estándar TLS.

Se utilizan medidas de autenticación fuerte para reducir la probabilidad de que posibles atacantes se hagan pasar por servidores de infraestructura o se introduzcan en medio de las comunicaciones de las sesiones de asistencia.

A fin de evitar ataques de escucha, modificación o repetición, se utilizan protocolos TLS estándar del IETF para proteger todas las comunicaciones entre los terminales y nuestros servicios. Los datos utilizados al compartir pantalla compartida, los datos de control del teclado o el ratón, los archivos transferidos, los datos de diagnóstico remoto y la información del chat de texto se cifran en tránsito con TLS 1.2 (cifrado fuerte RSA de 2048 bits, AES-256 con algoritmo SHA-2 de 384 bits).

A fin de garantizar una compatibilidad y un equilibrio de seguridad adecuados, el servicio de GoToAssist Remote Support v5 también admite conexiones entrantes a través de la mayoría de los conjuntos de cifrado TLS compatibles en TLS 1.2.

GoTo también recomienda que los agentes configuren sus navegadores para usar un cifrado fuerte de forma predeterminada siempre que sea posible, a fin de mejorar las protecciones técnicas en el equipo del agente, y que instalen siempre los parches de seguridad del sistema operativo y del navegador más recientes.

Cuando se establecen conexiones con el sitio web de GoToAssist Remote Support v5 y entre los componentes de GoToAssist Remote Support v5, los servidores de GoTo se autentican ante los clientes mediante certificados de clave pública GlobalSign. Solo se puede acceder a las API de servidor a servidor dentro de la red privada de GoTo protegida por cortafuegos.

3.9.2. Seguridad de la capa TCP

Los protocolos TLS estándar del Grupo de Trabajo de Ingeniería de Internet (IETF) se utilizan para proteger la comunicación entre terminales.

Con fines de protección, GoTo recomienda a los clientes que configuren sus navegadores para usar un cifrado fuerte de forma predeterminada siempre que sea posible y que mantengan actualizados los parches de seguridad del sistema operativo y del navegador.

3.9.3. Protección de terminales del cliente

Las aplicaciones de escritorio y las aplicaciones desatendidas de usuario final deben ser compatibles con una amplia variedad de entornos de escritorio. GoToAssist Remote Support v5 lo consigue mediante una descarga ejecutable que emplea medidas de cifrado fuerte.

Las aplicaciones de escritorio y las aplicaciones desatendidas de usuario final se descargan en los PC del cliente como un instalador firmado digitalmente. Esto ayuda a proteger al Cliente de la instalación accidental de un troyano u otro malware que se haga pasar por el software GoToAssist Remote Support v5.

El software de terminal se compone de varios ejecutables con firma digital y bibliotecas vinculadas dinámicamente. GoTo Sigue procedimientos de gestión de la configuración y control de calidad apropiados durante el desarrollo y la implementación para mejorar la seguridad del software.

3.10. Gestión de vulnerabilidades

Garantizar la seguridad y la protección de los contenidos y sistemas de los clientes de GoTo es una prioridad absoluta. GoTo aplica diversas medidas de seguridad a lo largo de la vida útil de todos sus productos. Los aspectos de seguridad se tienen en cuenta durante el desarrollo y las operaciones de GoToAssist Remote Support v5.

También se realizan pruebas dinámicas y estáticas de vulnerabilidad de las aplicaciones periódicamente, así como actividades de pruebas de evaluación de la seguridad para entornos específicos. Las vulnerabilidades pertinentes también se comunican y gestionan mediante informes mensuales y trimestrales, que se facilitan a los equipos de desarrollo y gestión.

3.10.1. Equipo de seguridad

El equipo de seguridad de GoTo supervisa continuamente el desarrollo y las operaciones de producto junto con los ingenieros, a fin de mantener la seguridad de GoToAssist Remote Support v5 y prevenir o reducir la probabilidad de riesgos.

3.10.2. Auditorías internas y externas

El proceso de auditoría interna de GoTo incluye evaluaciones periódicas de la seguridad a nivel tanto de infraestructura como de software. Nuestras auditorías internas se complementan con varias evaluaciones externas independientes para garantizar el cumplimiento con las normas del sector.

3.11. Registro y alerta

GoTo recopila el tráfico anómalo o sospechoso identificado en los registros de seguridad de los sistemas de producción aplicables.

4 Controles organizativos

GoTo mantiene un amplio conjunto de controles organizativos y administrativos, diseñados para proteger la postura de seguridad y privacidad del producto GoToAssist Remote Support v5.

4.1. Políticas y procedimientos de seguridad

GoTo mantiene un amplio conjunto de políticas y procedimientos de seguridad alineados con los objetivos empresariales, los programas de cumplimiento y la gobernanza corporativa general. Estas políticas y procedimientos se revisan periódicamente y se actualizan según sea necesario para garantizar un cumplimiento continuo.

4.2. Cumplimiento de las normas

GoTo cumple con los requisitos legales, financieros, de privacidad de datos y normativos aplicables, y mantiene el cumplimiento de las siguientes certificaciones e informes de auditoría externa:

- Certificación de TRUSTe en materia de privacidad empresarial y prácticas de gobierno de datos para abordar los controles operativos de privacidad y protección de datos que están alineados con las principales leyes de privacidad y marcos de

privacidad reconocidos. Para obtener más información, visite nuestra entrada en el blog.

- Certificación del Sistema de Gestión de la Seguridad de la Información (SGSI) de la Organización Internacional de Estandarización: ISO/IEC 27001:2013.
- Informe de atestación del Instituto Americano de Contables Públicos Certificados (AICPA) de Control de Organizaciones de Servicios (SOC) 2 Tipo 2, incluido el Catálogo de computación en la nube (C5) de BSI.
- Informe de atestación del Instituto Americano de Contables Públicos Certificados (AICPA) de Control de Organizaciones de Servicios (SOC) 3 Tipo II.
- Cumplimiento de la Norma de seguridad para la industria de las tarjetas de pago (PCI DSS) para los entornos de comercio electrónico y de pago de GoTo.
- Evaluación de los controles internos exigidos en una auditoría anual de los estados financieros del Consejo de Supervisión de Contabilidad de Empresas Públicas (PCAOB).

4.3. Operaciones de seguridad y gestión de incidentes

El Centro de Operaciones de Seguridad (SOC) de GoTo cuenta con personal del equipo de operaciones de seguridad y se encarga de detectar y responder a los eventos de seguridad. El SOC utiliza sensores de seguridad y sistemas de análisis para identificar posibles problemas y ha desarrollado un plan de respuesta a incidentes que rige las respuestas correspondientes.

El plan de respuesta a incidentes se ajusta a los procesos críticos de comunicación de GoTo, la Política de gestión de incidentes de seguridad de la información y los procedimientos operativos estándar asociados. Está diseñado para gestionar, identificar y resolver eventos de seguridad sospechosos o identificados en todos sus sistemas y Servicios, incluido GoToAssist Remote Support v5. De acuerdo con el plan de respuesta a incidentes, el personal técnico identificará posibles eventos y vulnerabilidades relacionados con la seguridad de la información y escalará cualquier evento sospechoso o confirmado a la dirección, cuando proceda. Los empleados pueden informar de los incidentes de seguridad por correo electrónico, teléfono o ticket en función del proceso documentado en el sitio de la intranet de GoTo. Los sucesos identificados o sospechosos se documentan y escalan a través de tickets de sucesos estandarizados y se clasifican en función de su criticidad.

4.4. Seguridad de las aplicaciones

El programa de seguridad de aplicaciones de GoTo se basa en el ciclo de vida de desarrollo de seguridad (SDL) de Microsoft para asegurar el código de los productos. Los elementos centrales de este programa son las revisiones manuales del código, el modelado de amenazas, el análisis estático del código y el refuerzo del sistema.

4.5. Seguridad del personal

Los antecedentes de los nuevos empleados se comprobarán antes de la fecha de contratación en la medida que lo permita la legislación aplicable y según corresponda al puesto. Los resultados se mantienen en el expediente laboral del empleado. Los criterios de comprobación de antecedentes variarán en función de las leyes, la responsabilidad laboral y el nivel de liderazgo del posible empleado, y están sujetos a las prácticas comunes y aceptables del país en cuestión.

4.6. Programas de sensibilización y formación en materia de seguridad

Se informa a los nuevos empleados de las políticas de seguridad y del Código de conducta y ética empresarial de GoTo durante la orientación. Esta formación anual obligatoria sobre seguridad y privacidad se imparte al personal correspondiente y la gestiona el Departamento de Desarrollo de Talentos con el apoyo del equipo de seguridad.

Los empleados y trabajadores temporales de GoTo reciben información sobre las directrices, procedimientos, políticas y normas de seguridad y privacidad periódicamente a través de diversos medios, entre los que se incluyen kits de incorporación para nuevos empleados, campañas de concienciación, seminarios web con el CISO, un programa de campeones de seguridad y exhibiciones de carteles u otros materiales, que se rotan al menos dos veces al año e ilustran los métodos para proteger los datos, los dispositivos y las instalaciones.

5 Prácticas de privacidad

GoTo se toma muy en serio la privacidad de los Clientes, los suscriptores de los Servicios GoTo y los usuarios finales, y se compromete a divulgar las prácticas de gestión y manejo de datos de forma abierta y transparente.

5.1. RGPD

El Reglamento General de Protección de Datos (RGPD) es una ley de la Unión Europea (UE) que rige la protección y privacidad de los datos de los residentes en la Unión Europea. El objetivo principal del RGPD es ceder el control de sus datos personales a los ciudadanos y residentes, y también simplificar el entorno reglamentario en la UE. GoToAssist Remote Support v5 cumple con las disposiciones aplicables del RGPD. Para obtener más información, visite https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo garantiza que cumple con la Ley de Privacidad del Consumidor de California (CCPA). Para obtener más información, visite https://www.goto.com/company/trust/privacy.

5.3. Protección de datos y política de privacidad

GoTo ofrece un Anexo de tratamiento de datos (DPA) global y completo, disponible en inglés y alemán, para cumplir con los requisitos del RGPD, la CCPA y otras normativas, y que rige el tratamiento de datos personales por parte de GoTo.

En concreto, el DPA abarca varios aspectos de la protección la privacidad de datos en relación con el RGPD, entre los que se incluyen: (a) detalles del tratamiento de datos, divulgaciones de subprocesadores, etc., tal y como exige el artículo 28; (b) las Cláusulas contractuales tipo de la UE, y (c) la inclusión de las medidas técnicas y organizativas de GoTo. Además, para preparar la entrada en vigor de la CCPA, hemos actualizado nuestro APD global para incluir: (a) definiciones revisadas vinculadas a la CCPA; (b) derechos de acceso y eliminación y (c) garantías de que GoTo no va a vender la “información personal” de los usuarios.

Para los visitantes de nuestras páginas web, GoTo revela los tipos de información que recoge y utiliza para proporcionar, mantener, mejorar y asegurar los Servicios en su Política de Privacidad, en la página web pública. La empresa puede actualizar la Política de

privacidad ocasionalmente para reflejar cambios en sus prácticas de información o en la legislación aplicable, pero avisará de ello en su página web antes de que dichos cambios entren en vigor.

5.4. Marcos de transferencia

GoTo cuenta con un programa global de protección de datos que tiene en cuenta la ley aplicable y respalda las transferencias internacionales legales conforme a los marcos siguientes:

5.4.1. Cláusulas Contractuales Tipo

Las Cláusulas contractuales tipo ("CCT") son cláusulas contractuales estándar, reconocidas y adoptadas por la Comisión Europea, cuyo objetivo principal es garantizar que los datos personales que salgan del Espacio Económico Europeo ("EEE") se transferirá conforme a la legislación de la UE en materia de protección de datos. GoTo ha invertido en un programa de privacidad de datos de primera clase para cumplir con los requisitos de las CCT al transferir datos personales. GoTo proporciona a los clientes las CCT, que establecen garantías específicas para la transferencia de datos personales en los servicios de GoTo como parte del DPA global. La ejecución de las CCT garantiza que los clientes de GoTo puedan transferir datos libremente del EEE al resto del mundo.

Medidas complementarias

Aparte de las medidas especificadas en estas TOM, GoTo ha creado las siguientes preguntas frecuentes para esbozar las medidas complementarias que respaldarán las transferencias legales conforme al capítulo 5 del RGPD y regir los análisis "caso por caso" recomendados por el Tribunal de Justicia Europeo junto con las CCT.

5.4.2. Certificaciones CBPR y PRP de APEC

GoTo también ha obtenido las certificaciones Reglas de Privacidad Transfronteriza (CBPR) y Reconocimiento de Privacidad para Procesadores (PRP) de la Cooperación Económica Asia-Pacífico (APEC). Los marcos de CBPR y PRP de APEC son los primeros marcos de regulación de datos aprobados para la transferencia de datos personales entre países miembros de APEC y se obtuvieron y validaron de forma independiente a través de TrustArc, un proveedor externo líder en el cumplimiento de la protección de datos de APEC.

5.5. Devolución y eliminación del Contenido del cliente

En cualquier momento, los Clientes de GoToAssist Remote Support v5 podrán solicitar la devolución o eliminación de sus Contenidos a través de interfaces estandarizadas. Si estas interfaces no están disponibles o GoTo no puede completar la solicitud, GoTo hará todo lo posible para ayudar al Cliente a recuperar o eliminar su Contenido, sujeto a la viabilidad técnica. El Contenido del cliente en GoToAssist Remote Support v5 se eliminará durante los treinta (30) días posteriores a la solicitud del Cliente. El Contenido del cliente de GoToAssist Remote Support v5 se eliminará automáticamente en un plazo de noventa (90) días tras la expiración o finalización de su último periodo de suscripción. Previa solicitud por escrito, GoTo certificará la eliminación del Contenido.

5.6. Datos sensibles

Aunque GoTo intenta proteger el Contenido del cliente, las limitaciones normativas y contractuales nos obligan a restringir el uso de GoToAssist Remote Support v5 a determinados tipos de información. A menos que el Cliente cuente con el permiso por escrito de GoTo, los siguientes datos no deben cargarse ni generarse en GoToAssist Remote Support V5 (por el Cliente o los usuarios finales):

- números de identificación emitidos por el gobierno e imágenes de documentos de identificación
- Información relacionada con la salud de una persona, incluida, entre otras, la Información Protegida sobre la Salud (IPS), tal y como se identifica en la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios de 1996 (HIPAA) de EE. UU. y en las leyes y normativas asociadas.
- información relacionada con cuentas financieras e instrumentos de pago, incluidos, entre otros, los datos de tarjetas de crédito La única excepción general a esta disposición se extiende a los formularios y páginas de pago explícitamente identificados que GoTo utiliza para cobrar el pago de GoToAssist Remote Support v5.
- Cualquier información especialmente protegida por las leyes y normativas aplicables, en concreto información sobre la raza, etnia, creencias religiosas o políticas, pertenencia a organizaciones, etc. de la persona.

5.7. Seguimiento y análisis

GoTo mejora continuamente sus sitios web y productos mediante herramientas de análisis web de terceros, que ayudan a GoTo a comprender cómo utilizan los visitantes sus sitios web, herramientas de escritorio y aplicaciones móviles, así como las preferencias y los problemas de los usuarios. Para obtener más información, consulte la Política de privacidad.

6 Terceros

6.1. Uso de terceros

Como parte de la evaluación interna y de los procesos relacionados con proveedores y terceros, las evaluaciones de proveedores pueden realizarlas varios equipos en función de su relevancia y aplicabilidad. El equipo de seguridad evalúa a los proveedores pertinentes que prestan servicios basados en la seguridad de la información, incluida la evaluación de las instalaciones de alojamiento de terceros. Los equipos del Departamento Jurídico y de Adquisiciones de GoTo pueden evaluar los contratos, las declaraciones de trabajo y los acuerdos de servicio según sea necesario, de acuerdo con los procesos internos. La documentación o los informes de cumplimiento se pueden obtener y evaluar al menos una vez al año, según se considere oportuno, para garantizar que el entorno de control funciona adecuadamente y que se abordan los controles de consideración del usuario correspondientes. Además, los terceros que alojen datos sensibles y confidenciales (o a los que GoTo conceda acceso a ellos) deben firmar un contrato por escrito en el que se indiquen los requisitos para el acceso a la información o su almacenamiento y manipulación, según proceda.

6.2. Prácticas contractuales

Para garantizar la continuidad del negocio y que se apliquen las medidas adecuadas para proteger la confidencialidad y la integridad de los procesos empresariales y el tratamiento de datos de terceros, GoTo revisa los términos y condiciones de los terceros pertinentes, utiliza las plantillas de contratación aprobadas por GoTo o negocia dichos términos de terceros si lo considera necesario en colaboración con los Departamentos Jurídico, de Seguridad, de Adquisición y de Finanzas (en cada caso, según proceda).

7 Contactar con GoTo

Los clientes pueden ponerse en contacto con GoTo en https://support.goto.com para consultas generales o enviar un correo electrónico a privacy@goto.com para preguntas relacionadas con la privacidad.

8 Anexo: terminología

Agente: usuario de GoToAssist Remote Support v5 que crea sesiones de GoToAssist Remote Support v5 para proporcionar asistencia técnica a los Clientes mediante visualización y control remotos o cámara compartida.

Consola web para agentes: una aplicación web que se ejecuta en el PC, Mac, Tablet o dispositivos Chromebook del agente en cualquiera de los navegadores compatibles (Chrome, Firefox, Safari) y se conecta al Servicio de GoToAssist Remote Support v5. Permite al agente crear y llevar a cabo sesiones de GoToAssist Remote Support v5, así como diversas funciones de gestión de cuentas, gestión de servicios y elaboración de informes.

Consola de escritorio del agente: aplicación de escritorio que se ejecuta en ordenadores MacOS y Windows y se conecta al servicio GoToAssist Remote Support v5 y aprovecha la tecnología de la consola web del agente GoToAssist Remote Support v5, Qt y el motor web Chromium. Proporciona la misma funcionalidad que la Consola web para agentes, pero con un aspecto nativo.

Sesión presencial: una sesión de asistencia en la que el Cliente está presente durante la sesión y puede participar en ella.

Cliente: persona que recibe soporte técnico del agente a través de una sesión de GoToAssist Remote Support v5.

Aplicación de escritorio de usuario final: una aplicación de escritorio que se ejecuta en el ordenador del Cliente (Windows o Mac) y se conecta a una sesión de GoToAssist Remote Support v5 a través del Servicio de GoToAssist Remote Support v5. Proporciona la función de control remoto, así como otras funcionalidades avanzadas y la posibilidad de instalar una aplicación desatendida en el ordenador del Cliente.

Terminal del cliente: término colectivo que hace referencia a cualquier terminal del cliente (aplicación web, aplicación de escritorio, aplicación móvil o aplicación desatendida).

Aplicación móvil de usuario final: aplicación móvil (Android e iOS) que se ejecuta en el dispositivo móvil/tablet del cliente y puede conectarse a una sesión de GoToAssist Remote

Support v5 a través del Servicio de GoToAssist Remote Support v5. Ofrece funciones de visualización remota (Android e iOS) y control remoto (solo Android).

Aplicación web de usuario final: aplicación web que se ejecuta en cualquier navegador compatible del ordenador/dispositivo móvil del cliente y se conecta a una sesión de GoToAssist Remote Support v5 a través del Servicio de GoToAssist Remote Support v5. Puede proporcionar funciones de chat, visualización remota y uso compartido de la cámara, así como la posibilidad de elevar la sesión en cualquier momento a control remoto al descargar la Aplicación de escritorio de usuario final o instalar la Aplicación móvil de usuario final.

Servicio de medios: una flota de servidores de carga equilibrada distribuidos por todo el mundo que proporcionan una variedad de servicios de comunicación unidifusión y multi-difusión de alta disponibilidad basados en protocolos WebRTC.

Sesiones de GoToAssist Remote Support v5: chat asistido, vista remota, control remoto o uso compartido de la cámara y control remoto sin supervisión.

Servicio GoToAssist Remote Support v5: una flota de servidores de carga equilibrada distribuidos globalmente que proporcionan acceso seguro a la Consola web del agente y a los terminales del Cliente mediante conexión web-socket cifrada y llamadas API.

Aplicación desatendida del Cliente: aplicación de escritorio (Windows y Mac) instalable que se ejecuta en segundo plano en el ordenador del cliente. Puede descargar y ejecutar una aplicación de escritorio de usuario final para conectarse a una sesión desatendida autorizada.

Sesión desatendida: sesión de asistencia en la que el cliente no está presente. La sesión la inicia y establece el agente sin intervención del Cliente a través de una aplicación de Cliente desatendida autorizada.