MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA EL RESCUE LIVE GUIDE

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) para Rescue Live Guide.

Rescue Live Guide es una herramienta de asistencia basada en web que utilizan los profesionales de atención al cliente para proporcionar orientación visual remota en el navegador, sin necesidad de añadir un script al sitio web al que se presta asistencia ni de descargar ningún software. Con los permisos del usuario final, Rescue Live Guide permite a un profesional de atención al cliente explorar sitios web de forma segura junto con el usuario final y proporcionar herramientas de orientación al agente.

2 Arquitectura del producto

GoTo Rescue Live Guide es una solución de interacción visual basada en software como servicio (SaaS) que conecta al usuario final y al agente en un navegador seguro basado en la nube.

Las aplicaciones tanto para el agente como para el usuario final son web y se ejecutan en el navegador compatible elegido por los usuarios. Los back-ends que sirven a estas aplicaciones se alojan en la nube de Amazon Web Services (AWS) de GoTo, lo que proporciona a los pares los medios para conectarse entre sí en una sesión de navegación conjunta.

La sesión se crea cuando un usuario final inicia una sesión de navegación compartida. Se genera un PIN de sesión que se muestra al usuario final al inicio de la sesión. El usuario final puede permitir que el agente se una a la sesión tras compartir el PIN de la sesión. Una vez que se establece una sesión de navegación conjunta entre el usuario final y el agente, el sitio web compatible se carga en un navegador aislado en la nube de GoTo.

La navegación real por la web y las comunicaciones con el sitio web compatible tienen lugar en el navegador en la nube. La imagen se transmite a las aplicaciones web de ambos usuarios, y las acciones del usuario se envían de vuelta para que se completen en el navegador en la nube.

Las instancias del navegador en la nube están completamente aisladas. Aparte de los datos de los informes, la grabación (si está activada) y la información de la sesión, los datos se purgan al finalizar una sesión de navegación conjunta.

Puede obtener más información sobre las medidas de seguridad de la solución en el siguiente capítulo (“Controles técnicos de seguridad”) de este documento.

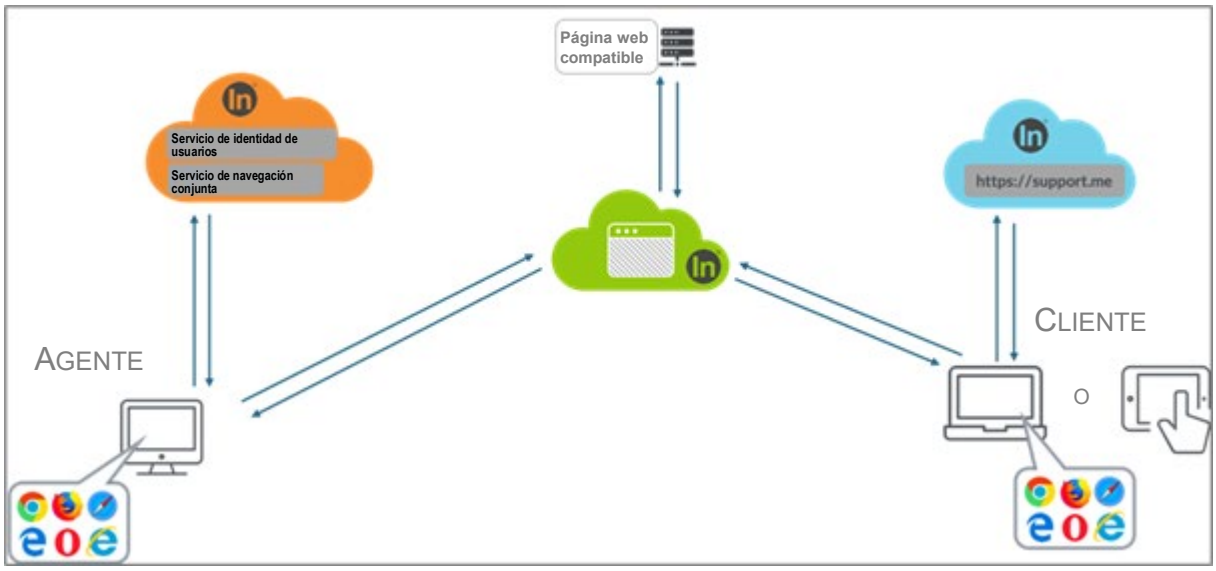

Figura 1: Infraestructura de Rescue Live Guide

3 Controles técnicos de seguridad

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. Control de acceso lógico

Existen controles 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 agentes de Rescue Live Guide están vinculados a cuentas de empresa y deben autenticarse con su nombre de usuario y una contraseña segura. Como medida de seguridad adicional opcional, el administrador de la cuenta puede establecer la autenticación de doble factor obligatoria para todos los agentes en su cuenta. Solo se puede acceder a la consola del agente tras autenticarse correctamente.

La disponibilidad de servicios adicionales (por ejemplo, informes, grabaciones o administración de cuentas) para los agentes/administradores autenticados puede controlarse y limitarse con roles asignados.

3.2. Protección de usuarios finales

Al crear este servicio se tuvo en cuenta la privacidad de los usuarios finales de Rescue Live Guide: el PIN de sesión es propiedad del usuario final, y un agente de asistencia solo puede unirse a una sesión si el usuario final ha compartido con él su PIN de sesión. Además, el PIN de sesión es específico de cada empresa, ya que a una sesión iniciada en un sitio web

determinado solo pueden unirse los agentes que formen parte de la cuenta asignada a ese sitio web.

GoTo no almacena el contenido del usuario final que se genera durante la sesión de asistencia. Como se ha mencionado anteriormente, las instancias del navegador en la nube están completamente aisladas y, aparte de los datos de informes, la grabación (si está activada) y la información de la sesión, los datos se eliminan una vez concluida la sesión de navegación conjunta.

El usuario final también tiene a su disposición un botón *Detener* durante toda la sesión de asistencia para hacer clic en él y finalizarla en cualquier momento.

3.3. Defensa perimetral y detección de intrusiones

La arquitectura de red local de GoTo se segmenta en zonas de red pública, privada y de gestión Integrated Lights-Out (iLO). La zona pública contiene servidores orientados a Internet, y el tráfico que entra en esta red debe pasar por un cortafuegos. Solo se permite el tráfico de red necesario; se deniega el resto del tráfico de red y no se permite el acceso desde la zona pública a las zonas de red privada o de gestión iLO.

La zona de red privada alberga sistemas administrativos y de supervisión a nivel de aplicación, y la zona de red de gestión iLO sirve para la administración y supervisión del hardware y la red. El acceso a estas redes se limita a los empleados autorizados mediante la autenticación de dos factores.

Además, GoTo emplea medidas de protección perimetral, incluido un servicio de prevención de denegación de servicio distribuido (DDoS) de terceros en la nube, para evitar que el tráfico de red no autorizado entre en la infraestructura de nuestros productos.

3.4. 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.

3.5. Seguridad física

Seguridad física del centro de datos

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 el envío de una solicitud a través del sistema de tickets correspondiente y la aprobación por parte del responsable correspondiente, así como la revisión y aprobación por parte 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.

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

Los centros de datos de producción utilizan conexiones de red redundantes de alta velocidad. Existen grupos de servidores web y puerta de enlace en centros de datos geográficamente distantes. Los equilibradores de carga distribuyen el tráfico de la red y mantienen la disponibilidad de estos servidores en caso de fallos del servidor o del centro de datos.

En general, 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.

3.7. Protección contra malware

En todos los servidores de Rescue Live Guide se instala software de protección contra malware con registro de auditoría. Las alertas que indican una posible actividad maliciosa se envían a un equipo de respuesta adecuado.

3.8. 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.

3.8.1. Cifrado en tránsito

El tráfico de red que entra y sale de los centros de datos de GoTo, incluido el Contenido del cliente, se cifra en tránsito. A fin de evitar ataques de escucha, modificación o repetición, se utilizan protocolos de seguridad de la capa de transporte estándar del IETF para proteger todas las comunicaciones entre los terminales y nuestros servicios. Nuestros servicios admiten los siguientes protocolos de cifrado o versiones posteriores (según proceda): TLS 1.2, RSA de 2048 bits, cifrado fuerte AES-256 con algoritmo SHA-2 de 384 bits.

3.8.2. Cifrado en reposo

Las configuraciones de Rescue Live Guide, los datos de la sesión y los archivos de grabación se cifran en reposo con un cifrado AES de 256 bits.

3.9. Gestión de vulnerabilidades

El análisis de vulnerabilidades de los sistemas internos y externos o de la red se realiza una vez al mes. También se realizan pruebas dinámicas y estáticas de vulnerabilidad de las aplicaciones periódicamente, así como actividades de pruebas de penetración para entornos específicos. Estos resultados de análisis y pruebas se comunican a las herramientas de supervisión de la red y, cuando procede y según la criticidad de cualquier vulnerabilidad identificada, se adoptan medidas de corrección.

Las vulnerabilidades también se comunican y gestionan mediante informes mensuales y trimestrales, que se facilitan a los equipos de desarrollo y gestión.

3.10. 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 para proteger la postura de seguridad y privacidad de Rescue Live Guide.

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.
- Informe de atestación para el servicio de Rescue del Instituto Americano de Contables Públicos Certificados (AICPA) de Control de Organizaciones de Servicios (SOC) 2 Tipo 2.
- 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 Rescue Live Guide. 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, según el 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, el análisis dinámico 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. Rescue Live Guide cumple 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.

La opción de residencia de datos de Rescue Live Guide le permite elegir dónde desea guardar los datos de los usuarios finales: en la Unión Europea (Fráncfort, Dublín) o en los Estados Unidos. GoTo garantiza que al elegir la residencia de datos en la Unión Europea solo se establecerá conexión con centros de datos de la Unión Europea, y que los datos del cliente permanecerán exclusivamente dentro de la región seleccionada.

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 podrán solicitar la devolución o eliminación de su Contenido 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 se eliminará durante los treinta (30) días posteriores a la solicitud del Cliente.

El Contenido del cliente de Rescue Live Guide 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 Rescue Live Guide 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 Rescue Live Guide (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 Rescue Live Guide.
- 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 que prestan servicios basados en la seguridad de la información, incluida la evaluación de las instalaciones de alojamiento de terceros. El Departamento Jurídico y de Adquisiciones puede 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 y utiliza las plantillas de contratación aprobadas por GoTo o negocia dichos términos de terceros si lo considera necesario.

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.