DECLARACIÓN de medidas de seguridad de datos técnicos y organizacionales

Historial de revisiones

Versión	Fecha	Editor	Cambios	Aprobado por
8.3	23 de enero de 2023	Naveen Pillai	Se incluyó el Certificado de aspectos cibernéticos básicos en la sección Recursos	Alan Cawse
8.4	15 de marzo de 2023	Neeraj Shar...	Se agregó la sección Comuníquese con Geotab y se aprobaron los cambios a la sección de Lat-Lon en el Apéndice 3.	Alan Cawse
8.5	10 de mayo de 2023	Neeraj Shar...	Se actualizaron las secciones de Lat-Lon en el Apéndice 3 para reflejar los cambios sugeridos por el departamento Legal.	Alan Cawse
8.6	14 de julio de 2023	Hari Krishn...	Se actualizó el estándar de cifrado a AES-128 en la sección Transmisión de datos en el Apéndice 3: Medidas de seguridad del sistema de Lat-Lon confirmadas por el vicepresidente asociado de Ingeniería de Datos	Alan Cawse
8.7	4 de junio de 2024	Vani Bhatia	Se actualizó la información de contacto de seguridad del diagrama de arquitectura para Lat-Lon, en el Apéndice 1: Se actualizó la sección Seguridad de dispositivos GO y MyGeotab, se eliminó la sección del Apéndice 2 “Medidas de seguridad de iGestion y uReaderGPS”	Alan Cawse

Este documento se redactó originalmente en inglés y expresa mejor las intenciones de las partes en inglés. Por lo tanto, en caso de discrepancia entre esta traducción y la versión en inglés, la versión en inglés prevalecerá en la medida de la inconsistencia. Se puede acceder a la versión en inglés a través del siguiente enlace:

https://docs.google.com/document/d/1b8F7XB86Z0h8xyD4GF3wH3vzwtdzMhKb-SmhYkz8lGs/edit#

Exención de responsabilidad importante

Esta declaración está sujeta a cambios y actualizaciones regulares. Por sí sola, esta Declaración no crea obligaciones vinculantes ni responsabilidad hacia Geotab ni hacia los distribuidores, usuarios finales ni ninguna otra parte de Geotab. Para obtener más información sobre la finalidad de este documento, consulte la Introducción. Este documento se creó con el fin de que se distribuya en formato con una versión en funcionamiento accesible a través de Google Docs. La versión en funcionamiento siempre está disponible en https://www.geotab.com/es/seguridad/.

Introducción

Esta Declaración de medidas de seguridad de datos técnicos y organizacionales de Geotab (indicada como "TOMS") proporciona una visión general de las medidas de seguridad de datos técnicos y organizacionales que Geotab Inc. ("Geotab" o "nosotros") implementó como su enfoque estándar. Por sí misma, esta declaración no otorgará derechos ni facultades a ninguna persona. Si Geotab y sus clientes incorporan esta declaración como referencia en un contrato, los derechos y las obligaciones de las partes se deben determinar según dicho contrato. Las medidas de seguridad para productos específicos de Geotab se describen en las secciones del Apéndice.

Uso permitido

Este documento solo se puede usar para fines internos de clientes relacionados con los productos y servicios específicos de Geotab. Este documento se actualiza frecuentemente. Esta declaración no se puede copiar ni duplicar sin el permiso expreso por escrito de Geotab.

Preguntas o comentarios

Envíe sus preguntas, comentarios o cualquier otra información a través del formulario que se encuentra en la parte inferior de la página web: https://www.geotab.com/es/seguridad/.

Medidas y controles comunes de seguridad

Las medidas y los controles de seguridad descritos en esta sección siguen el enfoque estándar de Geotab de manera horizontal para todos los productos y servicios de Geotab, a menos que se indique específicamente en las secciones del Apéndice.

Políticas de empleados de Geotab

Geotab implementa medidas y políticas para garantizar que todo el personal de Geotab esté capacitado y plenamente consciente de todas las políticas relacionadas con la seguridad y la privacidad; y que solo las personas específicas tengan acceso a áreas específicas dentro de la red y de los sistemas. Para lograr esto, se hace lo siguiente:

- A los empleados de Geotab se les otorgan credenciales muy limitadas y solo se les asignan credenciales adicionales cuando es necesario y después de revisión e instrucción,
- Todas las contraseñas de empleados de Geotab deben incluir al menos 12 caracteres, un número, una mayúscula, un carácter no alfanumérico y no deben incluir palabras ni nombres de usuario de uso común,
- Solo los empleados autorizados de Geotab pueden acceder a las áreas seguras dentro del sistema de MyGeotab,
- Cualquier credencial de usuario sin uso o inactiva se desactivará automáticamente después de 90 días,
- Todos los empleados de Geotab se someten a revisiones de antecedentes totalmente aprobadas y autorizadas por el Gobierno,
- Todos los empleados de Geotab realizan programas regulares de instrucción en materia de seguridad,
- Todos los derechos de acceso siguen el principio de mínimo privilegio,
- Todas las solicitudes de acceso se deben someter a un proceso de autenticación multifactorial para garantizar que las credenciales no estén en peligro,
- Todas las solicitudes de acceso son cronometradas, controladas y registradas, y
- Se sigue un proceso formal de desactivación para cualquier persona inmediatamente después de su despido con el fin de garantizar que todos los accesos, derechos, permisos y datos no estén disponibles para dicha persona.

Todos los empleados principales de ingeniería de soluciones e ingeniería de soporte de Geotab están ubicados actualmente en Ontario, Canadá. Geotab también tiene empleados de ingeniería ubicados en otras partes del mundo, incluidos Columbia Británica, Canadá; Nevada y Nueva York, EE. UU.; Múnich, Alemania; Londres, Reino Unido; y Madrid, España.

Segregación de deberes

Geotab implementa controles internos para reducir los riesgos asociados con los empleados de Geotab que disfruten de privilegios excesivos dentro de la red o del sistema. Siempre que sea posible, los privilegios se dividen entre distintos usuarios con el fin de garantizar que ningún empleado de Geotab pueda controlar completamente un proceso desde el comienzo hasta su fin. Cuando una división no sea posible, se revisa el acceso y el uso de forma periódica. Asimismo, todas las solicitudes de acceso al servidor requieren de aprobación y el acceso solo se otorga durante un período limitado. Los registros de acceso se conservan para todos los servidores y sistemas.

Centros de datos, proveedores de servicios tecnológicos

Geotab almacena datos en servicios de nube pública operados actualmente por Google (Compute Engine), ubicados en los Estados Unidos, Canadá, Europa y Asia. Estos proveedores de nube no permiten visitas presenciales de terceros y solo permiten que el personal autorizado tenga acceso a sus propias instalaciones de servidores físicos.

Geotab puede potenciar distintas regiones y añadir centros de datos según sea necesario, ya sea por razones de rendimiento, equilibrio de carga o seguridad. No obstante, siempre cumplirán con nuestros requisitos estrictos de

seguridad y redundancia.

Geotab también emplea servicios de mapeo y proveedores de tecnología inalámbrica y de información (que incluye, entre otros, proveedores de seguridad de la red y control de intrusión) para operar la plataforma de tecnología de Geotab. Las medidas tecnológicas, organizacionales y contractuales impiden que los proveedores de servicios accedan o vean la información personal de los clientes.

Seguridad de la nube pública

Geotab aprovecha los servicios de nube pública de vanguardia para ayudar a cumplir con sus compromisos de servicio en todo el mundo. Por lo tanto, Geotab se asoció con Google, que dispone de tecnología GCP (Google Cloud Platform) (Compute Engine y BigQuery) y múltiples centros de datos.

Geotab emplea Google Compute Engine con el fin de brindar recursos computacionales para alojar aplicaciones y datos. Estos servicios están contemplados en las políticas estrictas y líderes mundiales de seguridad de Google, lo que ayuda a Geotab a conservar la seguridad de los datos de nuestros clientes. Entre las características principales de sus programas de seguridad se incluyen las siguientes:

- Un equipo dedicado de seguridad de la información compuesto por los mejores expertos en la seguridad de la información, aplicaciones y redes,
- Todos los centros de datos de Google cuentan con un modelo de seguridad por capas que incluye dispositivos de seguridad como, tarjetas de acceso electrónicas personalizadas, alarmas, detección de intrusiones con rayo láser y biometría,
- Controles únicos de acceso a datos para facilitar la protección de seguridad de la información del cliente,
- La detección de intrusiones de Google implica el control del tamaño y de la recuperación de la superficie de ataque de Google mediante medidas preventivas, el uso de controles inteligentes de detección en los puntos de accesos de datos, y el empleo de tecnologías que solucionen automáticamente ciertas situaciones de peligro y
- La plataforma en la nube y la infraestructura de Google están certificadas según un número creciente de controles y estándares de cumplimiento normativo; además, se someten a varias auditorías independientes de terceros para verificar la seguridad, privacidad y protección de los datos.

Para conocer más información sobre la seguridad de la plataforma en la nube de Google, haga clic aquí.

El reporte SSAE Tipo II SOC 2 de Google se puede conseguir mediante una solicitud y según un acuerdo de no divulgación de Geotab. Puede encontrar información adicional sobre el cumplimiento en el respectivo sitio web de Google aquí.

Control de acceso de áreas de procesamiento

Los centros de datos de socios de la nube pública de Geotab no son accesibles para personas externas y sin autorización, lo que incluye al personal de Geotab. Estos centros de datos emplean accesos de seguridad y controles preventivos modernos para prevenir el acceso no autorizado a los equipos de procesamiento de datos (es decir, servidores de aplicaciones y bases de datos, así como hardware relacionado).

Para conocer más información sobre la seguridad del Centro de datos de Google, haga clic aquí.

Control de acceso a sistemas de procesamiento de datos

Geotab implementa medidas apropiadas para prevenir que personas no autorizadas usen sus sistemas de procesamiento de datos. Esto se consigue con lo siguiente:

- Identificación del terminal o del usuario del terminal en los sistemas de Geotab,
- Tiempo de espera automático del terminal de usuario inactivo, identificación, contraseña y factores adicionales necesarios para volver a abrir,
- Apagado automático de la ID del usuario si se ingresan varias contraseñas erróneas y archivo de registro de eventos (monitoreo de intentos de intrusión),
- Emisión y protección de códigos de identificación,
- Dedicación de terminales individuales o de usuarios de terminales, e identificación de características exclusivas de funciones específicas y
- Registro, monitoreo y seguimiento de todos los accesos a contenido de datos.

Geotab conserva una lista de personas que tienen acceso a los datos de clientes. Geotab otorga derechos de acceso solo a una cantidad limitada de personas.

Control de acceso al uso de áreas específicas de sistemas de procesamiento de datos

Geotab se compromete a que las personas con derecho a usar su sistema de procesamiento de datos solo puedan tener acceso a los datos dentro del alcance y en la medida en que estén cubiertos por su respectivo permiso de acceso (autorización), y a que dichos datos personales no se puedan leer, copiar, modificar ni eliminar sin autorización. Esto se consigue con lo siguiente:

- Políticas e instrucción regulares de empleados con respecto a los derechos de acceso de cada empleado a los datos personales,
- Asignación de terminales individuales o de usuario de terminales, e identificación de características exclusivas de funciones específicas,
- Capacidad de monitoreo con respecto a personas que eliminen, añadan o modifiquen los datos personales,
- Medidas disciplinarias moderadas y efectivas en contra de las personas que accedan a los datos personales sin autorización,
- Divulgación de datos solo a personas autorizadas,
- Control de archivos, destrucción controlada y documentada de datos y
- Políticas que controlan la retención de copias de seguridad.

Control de transmisión de datos

Geotab implementa medidas adecuadas para prevenir la lectura, copia, alteración o eliminación de los datos, los servicios de nube y de dispositivos por parte de terceros no autorizados durante la transmisión de los mismos o durante el transporte de soportes de datos. Esto se consigue con lo siguiente:

- El uso adecuado de cortafuegos y tecnologías de cifrado para proteger las vías de acceso y los canales por los cuales viajan los datos y
- La supervisión de la integridad y la exactitud de la transferencia de datos (verificación de extremo a extremo).

Consulte los controles de transmisión de datos de los productos específicos en los Apéndices.

Monitoreo del acceso

Geotab implementa medidas adecuadas para monitorear las restricciones de acceso a los administradores de sistemas de Geotab y para garantizar que actúen de acuerdo con las instrucciones recibidas. Esto se consigue con lo siguiente:

- El nombramiento individual de los administradores del sistema,
- La adopción de medidas adecuadas para llevar una relación de los registros de acceso de los administradores del sistema a la infraestructura y mantenerlos seguros, precisos y sin modificar durante, al menos, seis meses,
- Auditorías periódicas de la actividad de los administradores del sistema para evaluar el cumplimiento de las tareas asignadas, las instrucciones recibidas por el importador y las leyes aplicables y
- La conservación de una lista actualizada con los detalles de identificación de los administradores del sistema (por ejemplo, nombre, apellido, función o área organizativa) y las tareas asignadas.

Monitoreo de sistemas

Todos los servidores Geotab se monitorean las 24 horas del día, los 365 días del año mediante sistemas de monitoreo completamente redundantes y personal interno de ingeniería. Cada servidor se crea utilizando una compilación estándar aprobada de un sistema operativo Windows Server o Linux Server, el cual se reforzó para garantizar que todos los servicios redundantes o no utilizados estén desactivados y que los puertos innecesarios estén cerrados.

Todas las actualizaciones y parches de software se prueban en un entorno contenido y, a continuación, se instalan mensualmente en cada servidor para garantizar que los servidores de Geotab ejecuten los parches, programas y aplicaciones más recientes y seguros.

Todos los servidores se gestionan y se mantienen mediante agentes personalizados de creación interna y líderes de la industria, que proporcionan monitoreo y protección de seguridad continuos, lo que incluye detección/prevención de intrusiones en el host (HIDS, por sus siglas en inglés), antimalware (actualizado automáticamente), análisis de vulnerabilidades continuo (tanto interno como externo), herramientas de gestión de eventos de información de seguridad (SIEM, por sus siglas en inglés), y monitoreo de registros y eventos personalizados.

Pruebas de penetración/análisis de vulnerabilidad

Geotab se somete a pruebas anuales de penetración externa en todas sus redes, aplicaciones y dispositivos de generación de corriente GO de Geotab, por medio de socios de seguridad de confianza, para garantizar que los sistemas permanezcan seguros y contenidos.

Geotab lleva a cabo pruebas sistemáticas de vulnerabilidad en todos nuestros servidores de producción (análisis continuo) y en nuestras imágenes de servidor anteriores a la publicación para garantizar que se mantengan nuestros procesos y que no se creen posibles riesgos de seguridad o privacidad. Cualquier vulnerabilidad detectada durante el proceso se mitiga y se vuelve a probar antes de que la imagen se lance a producción.

Geotab cuenta con un activo programa privado de recompensas por encontrar errores en sus aplicaciones MyGeotab y MyAdmin, que proporciona un entorno aislado con sus aplicaciones más recientes, a varios investigadores de seguridad externos, para permitirles revisar, analizar e intentar infringir la seguridad de las

aplicaciones. Todas las vulnerabilidades detectadas se verifican, priorizan y abordan de forma inmediata en un plazo adecuado.

No se pueden realizar análisis de puertos, pruebas de vulnerabilidad ni pruebas de penetración de terceros en ninguno de los servicios, servidores ni activos de Geotab sin la aprobación expresa por escrito de Geotab y sus socios de alojamiento.

Auditorías

Geotab se somete a auditorías internas periódicas de sus políticas y procedimientos de seguridad. Durante la auditoría, todos los empleados de Geotab reciben instrucción sobre seguridad y sensibilidad; se revisan las políticas de seguridad internas, los procesos de actualización de seguridad y los procesos de monitoreo de servidores.

Las políticas de seguridad de la información se revisan anualmente. La instrucción y las pruebas de concientización de los empleados se llevan a cabo regularmente durante todo el año.

Incidentes de seguridad

En caso de una infracción de seguridad, el departamento de ingeniería de Geotab puede interrumpir el acceso a algunos o a todos los servicios de Geotab para mitigar cualquier posible daño debido a la intrusión. Una vez contenida o neutralizada la amenaza, personal de alto nivel de Geotab llevará a cabo una investigación exhaustiva e inmediata para determinar específicamente los nombres o la ubicación de los atacantes, los métodos de infracción, el tipo de datos expuestos (si los hubiera) y los clientes que podrían verse afectados.

Si Geotab determina que hubo personas no autorizadas que accedieron a los datos del cliente, Geotab informará inmediatamente a los clientes afectados (en un plazo de 24 horas), según lo requiera la legislación aplicable, y trabajará con ellos para garantizar que los datos estén protegidos, se muevan, se eliminen o se modifiquen.

El Programa de respuesta a incidentes de Geotab (GRIP, por sus siglas en inglés) se desarrolló de acuerdo con la publicación especial 800-61, revisión 2 de la Computer Security Incident Handling Guide (Guía para el manejo de incidentes de seguridad informática) del NIST, y está diseñado para seguir las prácticas recomendadas de la industria. Geotab se compromete a mejorar y actualizar continuamente nuestras capacidades de respuesta a incidentes mediante la incorporación de las lecciones aprendidas de respuestas anteriores que hayan ocurrido tanto internamente como en la comunidad de seguridad en general.

Cualquier información o conocimiento de cualquier debilidad de seguridad, infracción de seguridad, intento de infracción de seguridad o cualquier otra información que se sospeche que pueda estar relacionada con Geotab y sus servicios se puede reenviar a `security@geotab.com`.

Divulgación responsable

Geotab se toma muy en serio la seguridad y la transparencia y apreciamos los esfuerzos en curso de personas o entidades que estudian la seguridad o las vulnerabilidades de seguridad (conocidas como “investigadores de seguridad”). Para servir mejor a los investigadores de seguridad, Geotab desarrolló un programa para facilitar el reporte de vulnerabilidades y reconocer el esfuerzo de esos investigadores por hacer de Internet un lugar más seguro. Esta política proporciona las directrices de Geotab para que se nos informe de cualquier vulnerabilidad.

Para obtener más información sobre el Programa de divulgación de vulnerabilidades de Geotab, visite la página de

Política de divulgación responsable en nuestro sitio web.

Continuidad del negocio

Los miembros de la dirección sénior de Geotab supervisan la planificación de la continuidad del negocio para garantizar que se puedan prestar los servicios críticos a los clientes de manera continua.

Geotab lleva a cabo un análisis periódico del impacto empresarial para comprender el panorama de amenazas/riesgos y priorizar la planificación. Esto incluye ataques cibernéticos, sabotaje, apagones/cortes de electricidad, terrorismo y fallas aleatorias de los sistemas de misión crítica.

Geotab implementa planes, medidas y acuerdos adecuados para garantizar la continuidad del negocio, entre los que se incluyen los siguientes:

- Servicios de centros de datos en diversas ubicaciones,
- Potencia completamente redundante con generadores de respaldo (centros de datos),
- Proveedores de redes de varias fuentes (centros de datos),
- Equipo de red y hardware redundantes de servidores,
- Disponibilidad de opciones de almacenamiento de copias de seguridad fuera del sitio para los clientes (previa solicitud),
- Uso de la tecnología de nube para el negocio de Geotab (disponible en cualquier lugar),
- Sistema interno de monitoreo redundante (monitorea todos los servidores de producción, alertas de seguridad y otros problemas críticos),
- Soporte técnico de ingeniería en espera, disponible las 24 horas, todos los días del año, para todos los servicios críticos (ingenieros y desarrolladores) y
- Planes de recuperación ante desastres para fallas del servidor: permite el cambio a hardware redundante.

Geotab lleva a cabo pruebas mensuales limitadas de los planes de recuperación ante desastres. Para obtener más información sobre el Plan de recuperación ante desastres de Geotab, consulte la POLÍTICA del Plan de recuperación ante desastres (GRIDIRON) (en inglés).

Suscripciones y membresías a grupos de interés especial

Geotab tiene el compromiso de mantenerse al día y al tanto de todas las vulnerabilidades y riesgos conocidos relacionados con la información y la seguridad cibernética. Como parte de estos esfuerzos continuos, Geotab mantiene relaciones directas o indirectas con muchas organizaciones, que incluyen, entre otras, las siguientes:

- US-CERT (vulnerabilidades y alertas),
- Duo (seguridad relacionada con IAM),
- SecurityMetrics (análisis de redes PCI-DSS),
- SAE Electrical Systems Security Committee (vulnerabilidades de seguridad/ataques cibernéticos de vehículos),
- NMFTA (seguridad cibernética para camiones HD),
- Auto-ISAC (Análisis y uso compartido de información de seguridad de automóviles) y
- DOT-Volpe (seguridad cibernética para camiones HD).

Comuníquese con Geotab

Geotab se toma muy en serio la seguridad y el servicio de asistencia al cliente, y nos comprometemos a proporcionarle la mejor experiencia posible. Consulte la siguiente tabla para comunicarse con los contactos adecuados, según su consulta:

Tipo de consulta	Información de contacto
Incidentes de seguridad graves (disponibilidad ininterrumpida)	incident@geotab.com
Envío de vulnerabilidades de seguridad	Política de divulgación responsable (en inglés)
Soporte de seguridad general	Utilice el formulario en la parte inferior de la página web: https://www.geotab.com/es/seguridad/
Servicios generales de turno de Geotab	Servicios On-Call de Geotab
Consultas generales	Comuníquese con nosotros
Foros de soporte	Geotab Community

Para solicitar una copia en formato PDF, utilice el formulario en la parte inferior de la página web: https://www.geotab.com/es/seguridad/. Todas las copias se marcarán con una fecha de caducidad específica. Se invita a todos los lectores a revisar de vez en cuando este documento en funcionamiento.

El equipo de soporte de Geotab está disponible para ayudarlo con cualquier pregunta o problema que pueda tener. Nos esforzamos por brindar un apoyo oportuno y efectivo, y siempre buscamos formas de mejorar nuestra experiencia de servicio de asistencia al cliente.

Si tiene algún comentario o alguna sugerencia sobre cómo podemos mejorar nuestra seguridad o el servicio de asistencia al cliente, háganoslo saber. Siempre estamos abiertos a escuchar a nuestros clientes y estamos comprometidos a ofrecerles el mejor servicio posible.

Recursos

La siguiente es una lista de recursos que incluimos como documentación complementaria para revisar:

- POLÍTICA de nivel de servicio de MyGeotab (web)
- POLÍTICA del Plan de recuperación ante desastres (GRIDIRON)
- Política del PROGRAMA de divulgación de vulnerabilidades de Geotab [PÚBLICA]
- Sitio de seguridad de Google Compute Engine

- Sitio de seguridad de Geotab
- Certificado de certificación ISO 27001 de Geotab
- Autorización FedRAMP de nivel de impacto moderado de Geotab
- Validación FIPS 140-2 de Geotab para el módulo criptográfico en dispositivos GO
- Certificado de garantía de aspectos cibernéticos básicos de Geotab

Para consultas generales, visite la página Comuníquese con nosotros en nuestro sitio web. Para ver foros de soporte, visite Geotab Community a fin de encontrar respuestas y conectarse con expertos de Geotab.

Apéndice 1: Seguridad de dispositivos GO y MyGeotab

Seguridad de datos de dispositivos GO de Geotab

Geotab implementa medidas adecuadas para prevenir la lectura, copia, alteración o eliminación de datos por parte de terceros no autorizados durante la transmisión o el transporte de cualquier dato desde y hacia el dispositivo Geotab GO. Para lograr esto, se hace lo siguiente:

- Autenticación segura de todas las comunicaciones antes de iniciar cualquier transmisión. Cifrado de extremo a extremo entre el dispositivo y el servidor seguro del portal de acceso de Geotab de todos los datos, ya sea directamente desde el mismo dispositivo, de dispositivos de terceros adjuntos o del servidor del portal de acceso, mediante un algoritmo de cifrado AES-256 de norma común,
- Los procesos de autenticación y cifrado emplean claves de cifrado individuales, aleatorias y sucesivas que cambian constantemente,
- Todo el firmware del dispositivo GO de Geotab se firma usando el algoritmo RSA 2048 y autentica antes de que se actualice en el dispositivo. Esta medida protege al dispositivo ante firmware malicioso o no autorizado,
- Ningún GPS basado en Geotab ni datos del motor transmitidos incluyen nombres de conductores ni ningún otro dato confidencial y
- Todos los envíos de datos entre el servidor del portal de acceso y la base de datos de MyGeotab se realizan por medio de una conexión TLS segura y cifrada.

¡ IMPORTANTE: Los datos de dispositivos de terceros enviados mediante el dispositivo GO conectado se enviarán y almacenarán en los servidores Geotab.

Medidas de seguridad del sistema MyGeotab

Transmisión de datos

Geotab implementa medidas adecuadas para evitar la lectura, copia, alteración o eliminación de cualquier por parte de terceros no autorizados durante la transmisión o el transporte de cualquier dato hacia y desde MyGeotab. Para lograr esto, se hace lo siguiente:

- Todos los clientes alojados se conectan a MyGeotab mediante un moderno navegador web, a través de HTTPS (cifrado TLS para todas las comunicaciones hacia y desde los servidores alojados),
- Todos los puertos de entrada TCP y UDP, y servicios (excepto los puertos y servicios específicos requeridos por la aplicación MyGeotab) se desactivan dentro de la red Geotab.
- Todos los dispositivos dirigidos al público están protegidos por cortafuegos de norma de la industria, que se supervisan las 24 horas del día.
- Todos los servidores conectados a internet están separados de los sistemas internos de Geotab por dos cortafuegos y
- Los ingenieros de soporte de Geotab se conectan a través de IAP de GCP y el acceso se controla a través del directorio interno de Geotab.

Acceso al sistema

Geotab implementa medidas adecuadas para evitar el acceso no autorizado al sistema MyGeotab. Para lograr esto, se hace lo siguiente:

- MyGeotab usa la autenticación HTTPS (TLS) (mediante el uso de un nombre de usuario y una contraseña únicos) para autenticar a usuarios en el sistema,
- MyGeotab no permite el uso de contraseñas comunes (obtenidas de una lista activa de muchas de las contraseñas más comunes utilizadas),
- La contraseña real que un usuario utilice no se puede recuperar, ya que se somete a un hash de 256 bits con una sal aleatoria de 128 bits; además, la contraseña real nunca se almacena ni se guarda en el disco,
- Toda actividad a la que se somete un usuario dentro de MyGeotab queda registrada y cualquier usuario aprobado dentro del registro avanzado de auditoría de MyGeotab puede verla,
- Los datos del registro avanzado de auditoría no se pueden modificar ni eliminar,
- El sistema MyGeotab permite una gestión de derechos muy flexible, lo que habilita un acceso limitado a varias áreas del sistema para usuarios específicos,
- Los datos del cliente están completamente separados de otros datos del cliente, es decir, la información (datos GPS, información del usuario, reglas de excepción, entre otros) que se almacena en una base de datos de clientes no se puede acceder ni está disponible para otras bases de datos, incluso si las dos bases de datos están en el mismo servidor físico y
- Solo los empleados autorizados de Geotab se pueden conectar e iniciar sesión en todas las bases de datos alojadas para propósitos de solución de problemas, las cuales se encuentran auditadas y registradas en el registro avanzado de auditoría.

Control de entrada

Geotab implementa las medidas adecuadas para garantizar que se pueda comprobar y determinar si se han ingresado o eliminado datos personales en el sistema MyGeotab y quién lo ha hecho. Esto se consigue con lo siguiente:

- Una política de autorización para el ingreso de datos en la memoria, así como también para la lectura, alteración y eliminación de datos almacenados,
- Autenticación del personal autorizado,
- Medidas de protección para el ingreso de datos en la memoria, así como también para la lectura, alteración y eliminación de datos almacenados,
- Uso de códigos de usuario (contraseñas),
- Cierre de sesión automático de las ID de usuario que no se hayan utilizado durante un período considerable y
- Prueba establecida dentro de la organización de Geotab de la autorización de entrada.

Separación del procesamiento para diferentes propósitos

Geotab implementa medidas adecuadas a fin de garantizar que los datos recopilados para diferentes fines se puedan procesar por separado. Para lograr esto, se hace lo siguiente:

- El acceso a los datos se separa mediante la seguridad de la aplicación para los usuarios adecuados,
- Los módulos del sistema MyGeotab separan los datos que se utilizan para cada propósito, es decir, por

funcionalidad y función,

- A nivel de base de datos, los datos se almacenan en diferentes tablas normalizadas, separadas por módulos o por la función con la que son compatibles y
- Las interfaces, los procesos por lotes y los reportes están diseñados solo para fines y funciones específicos, por lo que los datos recopilados para fines específicos se procesan por separado.

Inquietudes generales

Es importante mantener la seguridad de cualquier identificación o contraseña de usuario, y no divulgarlas a ninguna otra persona ni reutilizar contraseñas en otros sitios que puedan verse afectados. Geotab no es responsable de contraseñas perdidas ni robadas. Geotab recomienda estándares mínimos de contraseña para la longitud y complejidad.

Si el cliente cree que se produjo una infracción de seguridad, debe notificar inmediatamente al equipo de Incidentes de seguridad graves (disponibilidad ininterrumpida) mediante el correo incident@geotab.com. Los clientes no deben crear usuarios en su sistema para las personas en las que no confían plenamente y deben revocar las cuentas de usuario para las personas que ya no requieren acceso al sistema.

No existe ninguna instalación ni requisito, bajo ninguna circunstancia, para que Geotab se conecte directamente a la red de los usuarios finales. Todos los datos de MyGeotab están totalmente contenidos y se gestionan dentro de la infraestructura de MyGeotab. El usuario final puede, por medio del Kit de Desarrollo de Software (SDK) de MyGeotab, descargar datos a su red, si fuera necesario. Esa conexión y cualquier dato transferido fuera de la red de Geotab se realizan por medio de HTTPS.

Ningún dato de MyGeotab se almacena, copia o transfiere a través de dispositivos de almacenamiento extraíbles, a menos que exista un requisito específico del usuario final, con su aprobación por escrito. Cualquier dato de este tipo bajo el control de Geotab se controla estrictamente y se destruye como es debido cuando ya no se necesita.

Residencia de datos del cliente

Los datos de usuario relacionados con la telemática y la telemática del cliente se almacenan en los siguientes medios:

- El dispositivo GO en el vehículo (el cliente puede etiquetar el dispositivo GO),
- La PC del cliente (el cliente puede etiquetar su propia PC),
- El servidor que administra Geotab (los datos del cliente se separarán por medios lógicos y virtuales),
- Los datos de clientes europeos se almacenan en los centros de datos europeos de Geotab y
- Todos los demás datos de clientes se almacenan en los centros de datos de Geotab, ya sea en Canadá, Estados Unidos o Asia, de acuerdo con la ubicación del cliente y los parámetros de optimización.

Los datos de usuario relacionados con la telemática y la telemática del cliente se pueden eliminar de forma segura a pedido del cliente.

Siempre que, por cualquier razón, el cliente de Geotab envíe solicitudes formales para eliminar sus datos, Geotab puede eliminar la información de los clientes de forma segura y permanente.

Disponibilidad de datos y copias de seguridad

Geotab implementa medidas adecuadas para garantizar que los datos personales estén protegidos contra la

destrucción o la pérdida accidental. Para lograr esto, se hace lo siguiente:

- Se realizan copias de seguridad de todos los datos alojados en la plataforma MyGeotab diariamente, los 365 días del año,
- Todas las copias de seguridad se confirman, se verifican y se replican en diversas ubicaciones físicas independientes para su almacenamiento (que pueden estar o no dentro del mismo centro de datos).
- Todos los datos de los que se realiza una copia de seguridad están protegidos y el acceso se limita a empleados específicos y autorizados de Geotab,
- Toda la infraestructura de copia de seguridad tiene una redundancia adecuada en caso de fallas de hardware y
- Todos los datos de los que se ha realizado una copia de seguridad se almacenan completamente cifrados mediante tecnologías de cifrado de nivel empresarial.

Conservación, corrección y eliminación de datos

Conservación de datos

Geotab conservará los datos durante un mínimo de dos años antes de la fecha de purga. Si desea conservar sus datos durante más de dos años, le recomendamos que recupere los datos deseados utilizando una de las herramientas de API que proporciona Geotab.

Opciones de corrección y eliminación de datos

Los clientes pueden eliminar y corregir los datos almacenados en los sistemas de Geotab. A petición de los interesados, Geotab puede ayudar con la exportación, eliminación y corrección de datos en virtud de un acuerdo de consultoría independiente, a las tarifas por hora vigentes en ese momento. Revise nuestra Política de nivel de servicio de MyGeotab para obtener más información sobre las copias de seguridad.

Enfoque de purga de datos

Geotab implementó un lista de purga por defecto en las bases de datos que elimina datos con una antigüedad superior a dos años.

Mejora y agrupación de datos

Geotab compila, almacena y utiliza datos agregados y la información de uso del sistema a fin de monitorear y mejorar los productos existentes, y para la creación de nuevos productos de acuerdo con la Política de datos y análisis de Geotab (en inglés). Los datos agregados que se usan de esta manera ya no están asociados con un dispositivo y, como tal, no corresponden a Datos del vehículo individual.

Geotab no intentará desagregar los datos ni volver a asociarlos con un dispositivo sin su consentimiento, a menos que esté obligado por ley a hacerlo o que se requiera para fines de seguridad o solución de problemas. Los siguientes son ejemplos del trabajo que Geotab realiza en los datos:

- Búsqueda de cualquier notificación del dispositivo de que nuestro producto no esté funcionando como debería,
- Búsqueda de un uso excesivo de datos que indique un defecto de diseño o una instalación incorrecta,
- Agrupación de la información sobre el tipo de motor disponible para cada marca, modelo y año de los

vehículos,

- Búsqueda de la cantidad de desconexiones de los dispositivos desglosadas por proveedor de telefonía celular, código postal/región,
- Búsqueda de la cantidad total de ocurrencias de frenado brusco en una carretera (para encontrar intersecciones peligrosas),
- Cálculo del consumo promedio de combustible para cada marca, modelo y año,
- Búsqueda de la velocidad promedio de todos los vehículos en una carretera en particular (velocidad del flujo de tráfico),
- Búsqueda de ubicaciones en las que haya posibles baches en la carretera y
- Como parte de la mejora de los productos de Geotab y de la experiencia del usuario, solo para los clientes de Norteamérica, Geotab puede consultar bases de datos que mantiene R.L. Polk & Co. (IHS) en busca de información que los usuarios hayan puesto previamente a disposición con respecto a su flota y operaciones. Dichas consultas se basarán en información de una muestra representativa de VIN (pero no en otra información del cliente) proporcionada a IHS de forma segura, confidencial y restringida.

Diagrama de arquitectura

Para ver un diagrama de arquitectura de alto nivel, haga clic aquí.

Apéndice 2: Medidas de seguridad del sistema de Lat-Lon

Resumen ejecutivo

Lat-Lon, LLC, sociedad de responsabilidad limitada de Colorado (“Lat-Lon”), es una filial de Geotab. Lat-Lon fabrica dispositivos de monitoreo y seguimiento de activos que funcionan con energía solar, comúnmente conocidos como “STU”. Los STU son dispositivos autónomos y de carga automática que tienen opciones de sensores con cable e inalámbricos. Los clientes no solo pueden realizar un seguimiento de sus activos, sino también monitorear diferentes aspectos del activo, como la detección de impacto, la temperatura, cuando se cierra/abre la puerta o trampilla, y la presión, por nombrar algunos. Las ofertas de productos Lat-Lon también incluyen un dispositivo certificado para ubicaciones peligrosas (Clase I, Div. 2).

La ubicación y los datos de sensores transmitidos por STU están disponibles a través del portal web de Lat-Lon. En este portal web, los clientes pueden configurar alertas por correo electrónico o mensaje de texto en tiempo real, cambiar configuraciones de dispositivo, crear usuarios adicionales, establecer geocercas y configurar reportes automáticos programados.

Para obtener más información, consulte el sitio web de Lat-Lon.

Medidas de seguridad del sistema de productos Lat-Lon

Transmisión de datos

Lat-Lon implementa medidas adecuadas para evitar la lectura, copia, alteración o eliminación de cualquier dato por parte de terceros no autorizados durante la transmisión o el transporte de cualquier dato hacia y desde Lat-Lon. Esto

se consigue con lo siguiente:

- Transmisión de sensor a dispositivo: los datos se cifran con AES-128 en bandas de radiofrecuencia (RF) sin licencia.
- Transmisión de dispositivo a servidor: los datos almacenados en hardware se cifran mediante procesos patentados mientras están en reposo a nivel de hardware y también cuando se transmiten a servidores internos.
- Transmisión de servidor a servidor: los datos se cifran en tránsito mediante el protocolo TLS 1.2.
- Transmisión de usuario a servidor: los datos se cifran en tránsito mediante el protocolo HTTPS.

Control de acceso al sistema

Lat-Lon implementa medidas adecuadas para evitar el acceso no autorizado al sistema de Lat-Lon. Para lograr esto, se hace lo siguiente:

- El acceso al portal web se autentica mediante una contraseña segura.
- Se pone sal y hash a las contraseñas usando la clase rfc2898DeriveBytes,
- Los usuarios deben cambiar su contraseña cada 12 meses,
- La aplicación Lat-Lon administra el acceso del cliente. Hay dos roles: administrador y usuario.
- Los datos del cliente se segregan según un proyecto de GCP. Por ejemplo, los entornos de producción, prueba y desarrollo están separados a nivel físico y lógico,
- El uso de la aplicación se monitorea mediante el Sistema de monitoreo de Lat-Lon.
- Se registran todos los intentos de inicio de sesión y cambios de contraseña y
- El monitoreo y las alertas del sistema se ejecutan mediante nuestro sistema operativo de pila Prometheus and Grafana (TIG), y las métricas de aplicación personalizadas se monitorean de forma ininterrumpida.

Control de entrada/validación de entrada

Lat-Lon implementa las medidas adecuadas para garantizar que se pueda comprobar y determinar si se han ingresado o eliminado datos personales en el sistema de Lat-Lon y quién lo ha hecho. Para lograr esto, se hace lo siguiente:

- Todos los datos de entrada por medio de la interfaz web se corrigen a través de las funciones estándar C# para la corrección de datos y
- Se valida el cliente de entrada y el lado del servidor.

Separación/segregación del procesamiento para diferentes propósitos

Lat-Lon implementa medidas adecuadas a fin de garantizar que los datos recopilados para diferentes fines se puedan procesar por separado. Para lograr esto, se hace lo siguiente:

- El desarrollo, el control de calidad (QA) y la producción están completamente separados y restringidos mediante el control de acceso basado en roles.

Inquietudes generales

Lat-Lon no tiene control sobre los clientes que comparten su contraseña con otros, por lo que es importante

mantener la seguridad de cualquier identificación o contraseña de usuario, y no divulgarlas a ninguna otra persona ni reutilizar contraseñas en otros sitios que puedan verse afectados.

Lat-Lon requiere que las contraseñas cumplan con los requisitos mínimos de longitud y complejidad. Los usuarios deben cambiar su contraseña cada 12 meses. Si el cliente cree que se produjo una infracción de seguridad, debe notificar inmediatamente al equipo de Incidentes de seguridad graves (disponibilidad ininterrumpida) mediante el correo incident@geotab.com. Los clientes no deben crear usuarios en su sistema para las personas en las que no confían plenamente y deben revocar las cuentas de usuario para las personas que ya no requieren acceso al sistema.

No existe ninguna instalación ni requisito, bajo ninguna circunstancia, para que Lat-Lon se conecte directamente a la red de los usuarios finales. El usuario final tiene la capacidad, por medio de la Guía del usuario de registrador binario de Lat-Lon para la API y el Kit de Desarrollo de Software (SDK) de MyGeotab para descargar datos a su propia red, si fuera necesario. Esa conexión y cualquier dato transferido fuera de la red de Geotab se realizan por medio de HTTPS.

Los datos nunca se almacenan, copian ni transfieren a través de dispositivos de almacenamiento extraíbles, a menos que exista un requisito específico del usuario final, con su aprobación por escrito. Cualquier dato de este tipo bajo el control de Geotab o Lat-Lon se controla estrictamente y se destruye como es debido cuando ya no se necesita.

Residencia de datos del cliente

Ubicación y medios de almacenamiento de datos del cliente

Los datos de STU del cliente y los datos de usuario relacionados de Lat-Lon se almacenan en los siguientes medios:

- Los STU en el activo.
- La computadora del cliente (el cliente puede etiquetar su propia computadora).
- El servidor Lat-Lon (los datos del cliente se separarán por medios lógicos y virtuales).
- Todos los datos del cliente se almacenan en los servidores Lat-Lon en la ubicación del este de EE. UU.

Enfoque de eliminación de datos del cliente

Los datos de STU del cliente y los datos de usuario relacionados se pueden eliminar de forma segura a pedido del cliente.

Siempre que, por cualquier razón, los clientes de Lat-Lon envíen solicitudes formales para eliminar sus datos de cliente, Lat-Lon puede borrar los datos de forma segura y permanente.

Disponibilidad de datos y copias de seguridad

Lat-Lon implementa medidas adecuadas para garantizar que los datos personales estén protegidos contra la destrucción o la pérdida accidentales. Para lograr esto, se hace lo siguiente:

- Se realizan copias de seguridad de todos los datos alojados en la plataforma de Lat-Lon diariamente, los 365 días del año.
- Todas las copias de seguridad se confirman, se verifican y se mueven a una ubicación física independiente

para su almacenamiento (que puede estar o no dentro del mismo centro de datos),

- Todos los datos de los que se realiza una copia de seguridad están protegidos y el acceso se limita a empleados específicos y autorizados.
- Toda la infraestructura de copia de seguridad tiene una redundancia adecuada en caso de fallas de hardware y
- Todos los datos de los que se ha realizado una copia de seguridad se almacenan completamente cifrados mediante tecnologías de cifrado de nivel empresarial.

Conservación, corrección y eliminación de datos

Conservación de datos

Si Lat-Lon realiza una purga, conservará un mínimo de 365 días de datos previos a la fecha de la purga y hará todo lo posible por notificar con antelación a los propietarios de la base de datos de Lat-Lon. Si se van a purgar los datos y un cliente desea conservar sus datos durante más de un (1) año, se le recomienda que recupere los datos deseados utilizando una de las herramientas de API que proporciona Lat-Lon.

Opciones de corrección y eliminación de datos

Los clientes pueden eliminar y corregir manualmente los datos almacenados en los sistemas de Lat-Lon a través del portal web de Lat-Lon. A petición de los interesados, Lat-Lon puede ayudar con la exportación, eliminación y corrección de datos en virtud de un acuerdo de consultoría independiente, a las tarifas por hora vigentes en ese momento.

Enfoque de purga de datos

Lat-Lon hará todo lo posible para iniciar solo una purga cuando sea necesario a fin de preservar la integridad, confiabilidad y disponibilidad del portal web de Lat-Lon. Todas las unidades sacadas de servicio se limpian con herramientas estándares de la industria para la destrucción de datos o, en el caso de una unidad que falla, se destruyen para garantizar que no se puedan recuperar jamás los datos.

Diagrama de arquitectura

Para ver un diagrama de arquitectura de alto nivel, haga clic aquí.