ANEXO DE SEGURIDAD DE LA INFORMACIÓN

Este ISA (*Information Security Addendum* o Anexo de Seguridad de la Información) complementa y se incorpora por referencia al Contrato entre el grupo Emburse (del que forma parte CAPTIO TECH, S.L.) y el Cliente. A menos que se establezca lo contrario a continuación, los términos en mayúsculas que no figuren en este ASI tendrán el significado establecido en el Contrato.

ADMINISTRACIÓN

Equipo de seguridad de la información

Emburse cuenta con un equipo de seguridad de la información especial, compuesto por profesionales de ingeniería de seguridad, operaciones de seguridad, programas de seguridad, así como profesionales de gobernanza, riesgo y cumplimiento (GRC) de TI. La seguridad de la información de Emburse adopta un enfoque integrado y basado en el riesgo para la seguridad, haciendo uso de la automatización y de herramientas para la evaluación continua del riesgo y del cumplimiento respecto de nuevos avances. El programa de seguridad y privacidad de Emburse cuenta con las certificaciones ISO 27001 e ISO 27701. Cada año se realiza una evaluación de riesgos de seguridad en toda la empresa, con los riesgos asociados al responsable de riesgos correspondiente para su corrección o aceptación. Estos se mantienen dentro de nuestra evaluación anual de riesgos. La totalidad de los riesgos identificados se tratan según proceda. Otras certificaciones dependientes del servicio incluyen SOC1 tipo II, SOC2 tipo II, PCI-DSS y Tx-RAMP.

Políticas, planes y normas

Emburse cuenta con políticas documentadas para cumplir con las recomendaciones de las normas ISO 27001 e ISO 27701. Las Políticas de seguridad de la información de Emburse se revisan al menos una vez al año, o cuando se produce un cambio significativo, para garantizar su continua idoneidad, adecuación y eficacia.

Junto con sus proveedores de alojamiento de centros de datos, Emburse cubre las áreas críticas de seguridad y privacidad: seguridad física, infraestructura de red, operaciones de seguridad y manejo de datos.

- La seguridad física incluye bloquear y registrar todo el acceso físico a nuestros centros de datos.
- La infraestructura de red proporciona las garantías de disponibilidad, sostenidas por nuestros SLA (*Service Level Agreements*, o Acuerdos de nivel de servicio).
- La seguridad operativa implica la creación de procesos y políticas de empresa que sigan las mejores prácticas de seguridad para limitar el acceso a información confidencial y mantener una seguridad estricta.
- La gestión de datos proporciona orientación sobre la gestión de datos de clientes y empleados.

Políticas de seguridad de la información de Emburse

- ISPOL01: Seguridad de la información
- ISPOL02: Uso aceptable
- ISPOL03: Gestión de datos
- ISPOL04: Contraseñas
- ISPOL05: Mensajería y colaboración
- ISPOL06: Criptografía y cifrado
- ISPOL07: Terceros
- ISPOL08: Seguridad de red
- ISPOL09: Seguridad física

- ISPOL10: Conservación de datos
- ISPOL11: Resiliencia cibernética
- ISPOL12: Gestión de acceso
- ISPOL13: Gestión de activos
- ISPOL14: Eliminación de equipos
- ISPOL15: Desarrollo seguro de aplicaciones
- ISPOL16: Endurecimiento de infraestructura
- ISPOL17: Control de cambios

Planes, normas y directrices de seguridad

- ISPR01: Plan de respuesta ante incidentes de seguridad
- Plan de continuidad de la actividad de Emburse
- ISDRP01: Plan de recuperación ante desastres de seguridad de la información
- ISTND01: Norma de cifrado y criptografía
- ISGDL01: Guía de concienciación sobre seguridad
- Pautas para contraseñas

CONTROL DE ACCESO

Normas

Emburse mantiene sólidas políticas de control de acceso que se aplican al acceso de los empleados a todos los entornos de producción. Los procesos de control incluyen, entre otros elementos:

- Requisitos estrictos de complejidad de contraseñas
- Uso del principio de mínimo privilegio y segregación de obligaciones
- Identificación y autenticación de usuario únicas
- Procesos de aprovisionamiento y desaprovisionamiento de cuentas
- Acceso remoto seguro y cifrado
- Autenticación multifactor

Autenticación

Las soluciones de Emburse proporcionan integraciones con SSO (*Single Sign On* o Inicio de Sesión Único). Se recomienda a los clientes que utilicen SSO configurado con autenticación multifactor. Esto se puede configurar en las opciones administrativas de inicio de sesión de Emburse y en la configuración de su proveedor de SSO. Esta configuración de implementación de primer nivel permite configurar una autenticación sólida para Emburse y posibilita un aprovisionamiento, un funcionamiento y una supervisión de Emburse en coherencia junto con otras aplicaciones de empresa.

MANEJO Y PRIVACIDAD DE LOS DATOS

Clasificación de datos

Emburse ha implementado una clasificación de la información para gestionar los datos de la forma más segura posible. En función de su sensibilidad, la información se clasifica y etiqueta en las tres categorías siguientes.

Altamente confidencial: Información destinada a personas específicas, con un alto riesgo de pérdida financiera o daño a la reputación de la empresa si se produce una divulgación o un acceso no autorizados.

Confidencial: Información destinada a una distribución limitada, con riesgo de pérdida financiera o daño a la reputación de la empresa si se produce una divulgación o acceso no autorizados.

Pública: Información disponible públicamente y/o destinada a la difusión pública.

Tratamiento de datos

Consulte nuestro Acuerdo de protección de datos para ver cómo tratará los datos Emburse en nombre de nuestros clientes.

Información de identificación personal (IIP)

Todos los datos de IIP almacenados en aplicaciones Emburse se conservan y utilizan únicamente con el fin de proporcionar a los usuarios el servicio del sistema previsto. La información no se reutiliza con otros fines ni se vende. La información se trata de conformidad con los planes de almacenamiento de datos autorizados, mientras que el almacenamiento de los datos fuera del centro se gestiona en tal calidad según corresponda. El acceso a los datos de IIP se limita a los empleados que "necesiten conocerlos" solo para fines autorizados. El almacenamiento de los activos de IIP se limita al tiempo necesario para los fines de los flujos de trabajo previstos. Los activos se limitan a los elementos de datos necesarios. El acceso físico a la IIP está restringido por el entorno de centro de datos seguro del proveedor de alojamiento y las protecciones adecuadas de red y hardware/software. No se deben descargar, imprimir ni almacenar de otro modo activos de IIP en dispositivos que no sean activos aprobados del Centro de datos. Las cuentas de usuario deshabilitadas no pueden acceder a los datos de IIP. Se aplica un umbral de bloqueo de cuenta que ayuda a bloquear el acceso no autorizado a los datos de IIP. El acceso a los datos de IIP está restringido a los usuarios que corresponda, en función de las reglas de autorización y de los roles en el sistema. Emburse no recopila ni almacena direcciones IP y, por lo tanto, las direcciones IP no deben incluirse en la lista. En concreto, el departamento de marketing de Emburse no recopila direcciones IP y el producto no recoge ni almacena direcciones IP. El producto referencia solo una parte de la dirección IP de un usuario (la sub-red de clase C) con un hash irreversible, por lo que Emburse no puede regenerar la dirección IP del usuario.

Los servicios de Emburse no recopilan Información personal sensible (IPS) según se define en el artículo 9 del RGPD, ni Información médica protegida (IMP) según se define en la HIPAA (*Health Insurance Portability and Accountability Act*). Es responsabilidad de nuestros clientes proporcionar únicamente los datos que se vayan a utilizar en los servicios prestados. Emburse es el encargado del tratamiento de datos y actuará en el tratamiento de tales datos con arreglo a los acuerdos y a la comunicación que reciba del responsable del tratamiento de datos.

CIFRADO

Normas generales

- Portátiles de empleados: cifrado AES-256 de disco completo
- Datos del cliente: AES-256 totalmente cifrado
- TLS: el valor predeterminado es TLS 1.2 o superior

Emburse aplica nuestras normas generales de cifrado utilizando nuestras herramientas de cifrado de proveedores de servicios en la nube (AWS, Azure, GCP).

Bases de datos de clientes

Emburse utiliza el modelo multiusuario. Con Emburse, cada usuario se identifica mediante un identificador de cliente único dentro de todos los sistemas. Cada cliente recibe el mismo código de la aplicación, pero con opciones de configuración específicas para cada cliente que adaptan la aplicación a sus propias necesidades.

Cada usuario recibe servicio mediante una única instancia común, con metadatos configurables específicos para ellos, y que se aplica en tiempo de ejecución para proporcionar a cada cliente una experiencia de usuario única.

Los clientes acceden a una granja de carga equilibrada de múltiples instancias con metadatos configurables y aislamiento de datos, donde los datos de cada cliente se mantienen completamente separados de todos los demás clientes. Emburse emplea la metodología de Sistema independiente de base de datos compartida (es decir, todos los datos del cliente se almacenan en una base de datos compartida y el sistema y los datos se separan mediante filtros de consultas SQL).

Emburse ha estructurado nuestras aplicaciones para contribuir a los requisitos operativos de capacidad de mantenimiento, escalabilidad y seguridad mediante el uso de múltiples niveles. Los niveles se particionan físicamente entre sí en segmentos de red separados, que los aíslan y proporcionan una mayor seguridad. Estos niveles son 1) capa web, 2) capa de aplicación y 3) capa de base de datos.

Las comunicaciones entre los segmentos están cifradas y solo se permiten a través de canales limitados. Emburse realiza pruebas de penetración con regularidad para garantizar que el aislamiento esté intacto

Gestión de claves

Emburse proporciona cifrado AES completo de 256 bits en reposo. Las claves se almacenan de forma segura y van rotando al caducar. Los empleados responsables de gestionar las claves firman acuerdos de custodia de claves que describen las responsabilidades de la gestión de claves.

SEGURIDAD DE RED

Segmentación

Emburse ha estructurado nuestras aplicaciones para contribuir a los requisitos operativos de capacidad de mantenimiento, escalabilidad y seguridad mediante el uso de múltiples niveles. Los niveles se particionan físicamente entre sí en segmentos de red separados, que los aíslan y proporcionan una mayor seguridad. Estos niveles son 1) capa web, 2) capa de aplicación y 3) capa de base de datos. Las comunicaciones entre los segmentos están cifradas y solo se permiten a través de canales limitados. Emburse realiza pruebas de penetración con regularidad para garantizar que el aislamiento esté intacto.

Cortafuegos

Emburse emplea cortafuegos con estado en el perímetro y cortafuegos basados en host en el interior. Emburse y nuestros entornos de alojamiento proporcionan seguridad lógica y física para el servicio y sus sistemas relacionados, incluidos cortafuegos, equilibradores de carga, routers, conmutadores de red y sistemas operativos.

Nuestros proveedores de servicios en la nube (AWS y Azure) ofrecen a Emburse la flexibilidad de colocar instancias y almacenar datos en múltiples regiones geográficas, así como en múltiples zonas de disponibilidad dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de fallo independiente, lo que significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana típica y están ubicadas en terrenos llanos con bajo riesgo de inundación (la categorización específica de la zona de inundación varía según la región).

Además del sistema de alimentación ininterrumpida (SAI) discreto y las instalaciones de generación de copias de seguridad in situ, las zonas de disponibilidad se alimentan cada una a través de diferentes redes de servicios de suministro público independientes para reducir aún más los puntos de fallo individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a múltiples proveedores de tránsito de nivel 1.

Emburse ha diseñado la arquitectura de nuestros entornos en la nube para aprovechar múltiples regiones y zonas de disponibilidad. Distribuir aplicaciones en múltiples zonas de disponibilidad proporciona la capacidad de seguir siendo resilientes ante fallos, incluidos desastres naturales y fallos del sistema.

Segregación de datos

Las instancias de los clientes de Emburse se separan de forma lógica-y se evitan y registran los intentos de acceso a los datos que se salgan de los límites de dominio permitidos. Se han implementado medidas significativas para garantizar que las cargas ejecutables, el código o los actores no autorizados no puedan acceder a datos no autorizados, por ejemplo, que un cliente acceda a archivos de otro cliente. Las políticas de control de acceso de Emburse se basan en los principios de "mínimo privilegio" y "segregación de obligaciones". La segregación se aplica a través de políticas de control de acceso basado en roles (CABR) y controles técnicos. Emburse mantiene cuatro entornos:

1. Producción
2. UAT
3. QA interno (activación)
4. Los ingenieros de desarrollo no tienen permitido el acceso a ningún entorno de producción, incluido el UAT.

ENDURECIMIENTO DE PLATAFORMA

Emburse utiliza la infraestructura como código para obtener un endurecimiento de la plataforma en coherencia con las normas de seguridad del sector. Solo están habilitadas las funcionalidades necesarias. El registro y la supervisión están activados.

Análisis de vulnerabilidades y pruebas de penetración

Emburse ejecuta un análisis de vulnerabilidades al menos una vez al mes y después de cualquier cambio significativo en la red (p. ej., nuevas instalaciones de componentes del sistema, cambios en la topología de la red, modificaciones de reglas de cortafuegos, actualizaciones de productos). Las pruebas de penetración anuales son realizadas por un tercero aprobado e independiente.

Realizamos pruebas de penetración en la infraestructura y las aplicaciones de red al menos una vez al año y después de cualquier actualización o modificación significativa de la infraestructura o la aplicación (p. ej., actualización del sistema operativo, sub-red añadida al entorno, servidor web añadido al entorno).
La segmentación de red se realiza dos veces al año para entornos PCI.

El resumen ejecutivo de los resultados de la prueba de penetración está disponible a solicitud, sujeto a acuerdo de confidencialidad.

Además, Emburse cuenta con un programa privado de Bug Bounty. Emburse y la seguridad de la plataforma se someten a pruebas de forma continua.

Cortafuegos de aplicaciones web

Emburse ha implementado y gestiona un Cortafuegos de aplicaciones web (Web Application Firewall, WAF), además de los cortafuegos de red. Este control de seguridad adicional evita muchos patrones de ataque conocidos.

Protección de terminales: Malware y antivirus

Emburse ha implementado protecciones de terminales mediante el uso del software antimalware y de detección de intrusiones (SDI) en todos los sistemas de Emburse. La detección de malware se ejecuta continuamente y se realizan análisis exhaustivos con carácter regular. Emburse ha implementado CrowdStrike para la protección de estaciones de trabajo y de servidores de Windows y ha contratado el servicio de respuesta ante incidentes por actividad anómala. Las redes y los correos electrónicos se supervisan para detectar el movimiento ilícito de archivos y la circulación de datos confidenciales. El antivirus y el malware se instalan en todas las estaciones de trabajo y todos los servidores.

APLICACIÓN DE PARCHES Y GESTIÓN DE VULNERABILIDADES

Parches

Seguimos un modelo de desarrollo ágil con actualizaciones del sistema implementadas cada dos semanas. Estas actualizaciones quincenales se instalan sin tiempo de inactividad y con un impacto mínimo para los usuarios finales. Además, estas actualizaciones incluyen parches y correcciones de errores, así como nuevas funciones de producto y ajustes del rendimiento del sistema.

Las vulnerabilidades críticas se parchean en 14 días. Las vulnerabilidades altas se parchean en un plazo de 30 días. Las vulnerabilidades medias se parchean en un plazo de 90 días.

Vulnerabilidades

Emburse utiliza escáneres para supervisar el entorno de producción en busca de vulnerabilidades y configuraciones erróneas. Los análisis de vulnerabilidades se realizan de manera regular. Las vulnerabilidades de seguridad descubiertas recientemente se evalúan, mitigan y corrigen en función de su impacto. El equipo de seguridad y operaciones se reúne semanalmente para revisar las nuevas vulnerabilidades y exposiciones comunes (VEC) en todos los sistemas del entorno.

Emburse participa en un programa de Bug Bounty. Los resultados revelados por los investigadores de seguridad se evalúan, mitigan y corrigen en función del impacto.

Los miembros del equipo de seguridad de la información de Emburse supervisan regularmente fuentes de amenazas, plataformas o bases de datos con vulnerabilidades y demás fuentes de información de seguridad para obtener información actualizada sobre amenazas, vulnerabilidades y programas intrusos emergentes.

GESTIÓN DE CAMBIOS Y RIESGOS

Política y proceso de gestión de cambios

Los procesos de gestión de cambios en Emburse se aplican a los cambios que se realicen en la plataforma y la infraestructura. El proceso requiere, entre otros aspectos:

- Que los desarrolladores estén identificados y autorizados
- Que los cambios en el código fuente se revisen y aprueben
- Que los cambios de código fuente pasen las pruebas
- La segregación de tareas en la implementación
- Entornos de desarrollo, preparación y producción separados lógicamente
- Que se registren todos los cambios
- Que los cambios de emergencia requieran aprobación

Revisiones de seguridad

Emburse lleva a cabo reuniones periódicas de revisión con las partes implicadas en materia de seguridad, de forma regular, para debatir y realizar un seguimiento de los riesgos potenciales o activos relacionados con el negocio.

Riesgo de terceros: Gestión de proveedores y socios

Emburse realiza un análisis de riesgos en proveedores de servicios externos. La alta dirección de Emburse reconoce que son necesarias relaciones con terceros seguras y fiables para dar soporte a los productos y servicios de la empresa. Estas políticas y procedimientos se aplican a terceros, independientemente del país en el que se encuentren o desde el que se presten los servicios.

La alta dirección reconoce, además, que las relaciones con terceros presentan riesgos potenciales que deben gestionarse adecuadamente, comenzando con un sólido proceso de diligencia debida al principio y continuando con revisiones anuales o más frecuentes de todas las relaciones con terceros. El alcance del riesgo varía en cada relación con terceros; entre los riesgos más comunes relacionados con terceros se encuentra la falta de supervisión de terceros por parte de la alta dirección, lo que podría dar lugar a que la empresa experimente riesgos operativos, riesgos de privacidad y riesgos para la reputación.

La alta dirección reconoce que es responsable en última instancia de identificar y controlar los riesgos derivados de dichas relaciones, en la misma medida que si se trataran dentro de la empresa. La revisión de seguridad y la modelización de amenazas pueden incluir, entre otros aspectos:

- Revisiones del flujo de datos o diagramas técnicos
- Evaluaciones de riesgos relacionados con la gestión de datos y medidas adoptadas para proteger los datos
- Otras integraciones de terceros
- Notificaciones de cumplimiento
- Controles y requisitos de acceso
- Resultados de las pruebas de penetración
- Modelos de alojamiento
- Pruebas de Sandbox o pruebas de seguridad realizadas por el equipo de seguridad de la información de Emburse

Subencargados del tratamiento

Emburse utiliza subencargados del tratamiento para dar soporte a nuestra actividad; consulte el ATD (sección 3) y la Carta de subencargado del tratamiento para obtener más información.

Formación sobre concienciación en materia de seguridad y privacidad

Todos los empleados de Emburse deben completar la formación de concienciación sobre seguridad en el momento de la contratación y cada año a partir de entonces. La formación incluye privacidad y gobernanza de datos, protección de datos, confidencialidad, ingeniería social, políticas de contraseñas y responsabilidades generales de seguridad dentro y fuera de Emburse. Como parte de la formación de concienciación sobre seguridad, los empleados deben confirmar que la han completado y aceptar su parte en el mantenimiento de la seguridad y privacidad de Emburse en general.

Los desarrolladores reciben formación anualmente para mantener al día el conocimiento del Top 10 OWASP para el desarrollo de código seguro. Por último, Emburse realiza pruebas de phishing con regularidad. Aquellos que hagan clic en un correo electrónico simulado de phishing deben realizar una formación correctiva.

RESILIENCIA: RESPUESTA A INCIDENTES, BCP Y DR

Respuesta ante incidentes

La Política de respuesta ante incidentes de Emburse abarca cuatro fases principales: 1) preparación, 2) detección y análisis, 3) contención, erradicación y recuperación y 4) actividad posterior al incidente. Cuando se sospecha de un incidente, se dedican los recursos adecuados a la validación y corrección. Dependiendo de quién haya informado del problema y de cómo se maneje, la responsabilidad de la solución recaerá en los equipos de soporte o de operaciones de Emburse.

El jefe del SIRT (Equipo de Respuesta ante Incidentes de Seguridad, ERIS) actúa como coordinador en respuesta a todos los incidentes o puntos débiles importantes relacionados con la seguridad. Un incidente o punto débil de seguridad importante se considera un impacto en la confidencialidad (p. ej., exfiltración de claves de cifrado), la

integridad (p. ej., fuga de datos o exfiltración imprevista) o la disponibilidad (p. ej., degradación grave del rendimiento). El jefe del SIRT es responsable de asignar el personal para que trabaje en tareas específicas del proceso de manejo de incidentes y coordinar la respuesta general ante incidentes.

Todo el personal involucrado en la respuesta y corrección de incidentes es responsable de proporcionar cualquier información necesaria a los miembros del SIRT. Cualquier directiva que emita un miembro del equipo de respuesta ante incidentes de seguridad podría reemplazar los detalles específicos de esta política.

BCP/DR

Emburse realiza anualmente un análisis de riesgos empresariales para evaluar y determinar los procesos y sistemas de empresa que resultan críticos para todas las funciones de empresa. Esto incluye un inventario de sistemas críticos, midiendo el posible impacto operativo general de la perturbación crítica del sistema y asignando una métrica RTO (Objetivos de Tiempo de Recuperación) y RPO (Objetivos de Punto de Recuperación) adecuada a partir de esa criticidad. Todas las copias de seguridad están cifradas.

La detección de una perturbación o de un desastre que pudiere afectar las operaciones de Emburse o los servicios de aplicaciones es responsabilidad del SIRT. Las responsabilidades específicas del SIRT y los grupos asociados se describen en nuestro Plan de continuidad de actividad con certificación ISO.

El SIRT se actualiza automáticamente a través de servicios de supervisión que proporcionan notificaciones por correo electrónico y teléfono. Cuando se produce una perturbación o un desastre, el miembro de guardia del SIRT realiza inmediatamente una evaluación de los servicios afectados. Si es necesario, inician el Plan de recuperación ante desastres y lo notifican a los demás miembros del *Disaster Recovery Team* (Equipo de Recuperación ante desastres, ERD).

Simulación teórica

Emburse lleva a cabo un ejercicio anual de simulación teórica con un grupo multifuncional de empleados de todos los departamentos de la organización. Este evento anual está estructurado con el fin de probar la preparación del equipo para responder a un evento de producción. Los ejercicios requieren que los participantes prueben, registren y simulen actividades de respuesta en caso de que la simulación teórica fuera una emergencia real. Se lleva a cabo una revisión posterior a la acción y se materializan las lecciones aprendidas para garantizar la mejora continua.

Política de resiliencia

La Política de resiliencia de Emburse rige y vela por el cumplimiento de los procesos, incluidos, entre otros elementos:

- Programación y supervisión de copias de seguridad
- Restauración del sistema
- Cifrado en tránsito y en reposo
- Responsabilidades de ingeniería

El contenido y los datos de los clientes de Emburse tienen una elevada disponibilidad y se realizan copias de seguridad a diario. Todo dato en reposo y en tránsito está cifrado. Está activado un registro que realiza un seguimiento del estado de la copia de seguridad. Emburse realiza copias de seguridad de una cuenta en la nube segmentada e independiente y no está disponible (fuera de línea) para el resto de los sistemas de producción e ingenieros.

Supervisión y alertas

Emburse realiza una supervisión ininterrumpida de la infraestructura y los entornos de Emburse. Están implementadas y supervisadas la monitorización automatizada y las alertas de rendimiento (p. ej., tiempo de actividad, CPU, memoria, discos) y seguridad.

La supervisión de uso indebido se realiza en toda la infraestructura de producción para detectar y alertar de actividades sospechosas o cambios en la infraestructura crítica.

RTO/RPO

Emburse se esfuerza por mantener los servicios en funcionamiento; sin embargo, todas las empresas de SaaS sufren perturbaciones ocasionales. Los OTR y los OPR están vinculados a procesos específicos, no a la disponibilidad general de toda la plataforma. Estas métricas se evalúan anualmente durante el análisis de riesgos de empresa de Emburse. Emburse mantiene copias de seguridad casi en tiempo real, por lo que el OPR general se mide en minutos.

CUMPLIMIENTO

Emburse

Emburse y sus filiales respetan múltiples marcos de seguridad y cumplimiento, incluidos SOC1, SOC 2, ISO 27001 y PCI-DSS. (Nota: las certificaciones de cumplimiento específicas difieren según los servicios de Emburse)

SOC 1: muchas de las filiales de Emburse han sido auditadas por un tercero y han alcanzado el cumplimiento certificado de SOC 1. El informe está disponible sujeto a acuerdo de confidencialidad para que lo revisen los clientes o clientes potenciales. SOC 2: muchas de las filiales de Emburse han sido auditadas por un tercero y han alcanzado el cumplimiento certificado de SOC 2. El informe está disponible sujeto a acuerdo de confidencialidad para que lo revisen los clientes o clientes potenciales.

ISO 27001: muchas de las filiales de Emburse han sido auditadas por un tercero y han alcanzado el cumplimiento de seguridad certificado ISO 27001. El certificado de registro está disponible sujeto a acuerdo de confidencialidad para que lo revisen los clientes o clientes potenciales.

ISO 27701: muchas de las filiales de Emburse han sido auditadas por un tercero y han alcanzado el cumplimiento de la norma de privacidad ISO 27701. El certificado de registro está disponible sujeto a acuerdo de confidencialidad para que lo revisen los clientes o clientes potenciales.

PCI-DSS: muchas de las filiales de Emburse han sido auditadas por un tercero y han alcanzado el cumplimiento de PCI-DSS. El certificado de registro está disponible sujeto a acuerdo de confidencialidad para que lo revisen los clientes o clientes potenciales.

El RGPD y la Sentencia Schrems II, la Política de privacidad de Emburse y la información de privacidad de datos del RGPD se pueden encontrar aquí: https://www.emburse.com/privacy-policy

Marco de privacidad de datos, Emburse cumple con el Marco de privacidad de datos de EE.UU.-UE-Reino Unido-Suiza.

Amazon Web Services

El cumplimiento de AWS se puede encontrar aquí: https://www.atlas.aws/

Microsoft Azure

El cumplimiento de Azure se puede encontrar aquí: https://learn.microsoft.com/en-us/azure/compliance/