ANEXO DE SEGURIDAD ONEASY

Versión internacional empresarial mejorada

Última actualización: 25 de junio de 2026
Fecha de entrada en vigor: 25 de junio de 2026

---

1. FINALIDAD Y ALCANCE

Este Anexo de Seguridad ("Anexo") complementa el Contrato de Servicios SaaS de Oneasy y describe las medidas técnicas y organizativas adoptadas por GloryScience International Limited, mediante Oneasy SaaS Platform ("Oneasy"), para proteger los Datos del Cliente, datos del Tenant, datos operativos de la plataforma y la seguridad de los sistemas relacionados.

"GloryScience" significa GloryScience International Limited. "Oneasy" o "Servicios Oneasy" significa Oneasy SaaS Platform operada por GloryScience, sus funciones, componentes, APIs, recursos de acceso mediante Agent/VPN y servicios de soporte. Salvo cuando describa un producto o tecnología, los derechos, obligaciones, limitaciones y avisos de este Anexo corresponden a GloryScience. Oneasy no es un operador de telecomunicaciones, ISP, operador de la red del Cliente, proveedor de comunicaciones a usuarios finales ni controlador final de la red de producción del Cliente.

Este Anexo se aplica a la plataforma inteligente de OAM en la nube, APIs, consola administrativa, componentes de acceso remoto, Agent/VPN y soporte proporcionados como SaaS.

En caso de conflicto, este Anexo prevalece respecto de controles de seguridad, incidentes, acceso, medidas técnicas y organizativas, Agent/VPN, acceso remoto, vulnerabilidades, conservación de registros, seguridad de IA y responsabilidades de seguridad del Cliente. Si el asunto también implica Tratamiento de Datos Personales, transferencia internacional, Subencargados, derechos de los Titulares, notificación de violaciones u obligaciones legales de protección de datos, prevalecerá el DPA. Los demás asuntos seguirán sujetos al Contrato Principal.

---

2. GOBERNANZA DE SEGURIDAD

GloryScience mantendrá mecanismos de seguridad de la información comercialmente razonables, incluidos:

1. un responsable o equipo de seguridad;
2. políticas internas, control de acceso y respuesta a incidentes;
3. confidencialidad para empleados, contratistas y personas autorizadas que accedan a Datos del Cliente;
4. evaluaciones periódicas de riesgos y mejora continua según el negocio, las amenazas, la tecnología y las necesidades razonables; y
5. referencia, cuando sea razonable, a principios como ISO 27001, SOC 2 y CSA CCM.

Las referencias a normas son únicamente referencias de control, salvo certificación formal. Toda certificación, auditoría o evaluación futura se acreditará mediante el certificado o informe efectivo, su alcance y período de validez.

---

3. HOSPEDAJE DE DATOS Y SEGREGACIÓN DE TENANTS

1. De forma predeterminada, el hospedaje, Tratamiento y almacenamiento principales de Oneasy se ubican en la región de Singapur de Alibaba Cloud International. GloryScience podrá utilizar otras regiones para nodos secundarios, recuperación ante desastres, borde, registros o acceso de soporte, según disponibilidad, seguridad, soporte, rendimiento, Subencargados o configuración del Cliente.
2. Los Servicios Oneasy utilizan segregación lógica entre espacios, cuentas, permisos y datos de distintos Clientes.
3. GloryScience adoptará medidas razonables contra el acceso no autorizado entre Tenants.
4. El Cliente administra los usuarios, funciones, permisos y auditoría interna de su Tenant.
5. Una región específica, localización de datos, restricción transfronteriza, entorno dedicado, clave exclusiva o segregación adicional requieren una Order Form, SOW, DPA, SLA o acuerdo específico y podrán generar costos adicionales.

---

4. CONTROL DE ACCESO

GloryScience aplicará controles comercialmente razonables, incluidos RBAC, privilegio mínimo, aprobación y revocación de acceso del personal, restricción del acceso a producción, registro de operaciones privilegiadas, soporte de MFA cuando sea técnicamente viable, autenticación reforzada para cuentas internas privilegiadas o de alto riesgo, revisiones periódicas o después de cambios y protección de credenciales, API Keys, tokens y credenciales de VPN/Agent.

El Cliente deberá:

1. administrar adecuadamente las cuentas de administrador y los permisos de los Usuarios Autorizados;
2. eliminar sin demora a usuarios desvinculados, transferidos o que ya no necesiten acceso;
3. proteger contraseñas, API Keys, tokens y credenciales de VPN/Agent;
4. habilitar MFA o autenticación fuerte para administradores y usuarios privilegiados cuando sea compatible; y
5. asumir los riesgos derivados del compromiso de sus cuentas, cuentas compartidas, contraseñas débiles, filtración de credenciales o configuración inadecuada de permisos.

---

5. CIFRADO Y PROTECCIÓN DE DATOS SENSIBLES

GloryScience adoptará, conforme a las prácticas del sector, el escenario y estándares comerciales razonables:

1. protocolos de transmisión cifrada, preferentemente TLS 1.2 o superior, o seguridad equivalente, cuando sea aplicable y técnicamente viable;
2. cifrado, segregación, control de acceso o salvaguarda equivalente para datos en reposo en producción, cuando corresponda;
3. hash, cifrado, almacenamiento seguro, restricciones o controles equivalentes para contraseñas, credenciales, claves y tokens;
4. esfuerzos razonables para no exponer secretos completos en registros, mensajes de error, depuración, configuraciones en texto simple, soporte o canales inseguros;
5. controles de acceso y auditoría para datos sensibles; y

6. gestión del ciclo de vida de claves, certificados, tokens y credenciales, incluida su generación, almacenamiento, acceso, rotación, revocación y eliminación.

GloryScience podrá actualizar las medidas según la tecnología, los riesgos, las normas, las dependencias o la arquitectura, sin reducir deliberadamente el nivel general de protección descrito.

El Cliente evitará enviar contraseñas en texto simple, claves privadas, información sensible sin anonimizar, interceptaciones ilegales o no autorizadas y datos de alto riesgo mediante campos no designados, soporte ordinario, mensajería instantánea o correo electrónico inseguro. Salvo acuerdo escrito, GloryScience no garantiza requisitos especializados de un sector, país, marco regulatorio, certificación de algoritmos o gestión exclusiva de claves determinados.

---

6. REGISTROS Y MONITOREO

GloryScience mantendrá mecanismos adecuados, conforme a prácticas razonables, necesidades operativas, cumplimiento y funciones efectivas de los Servicios, para monitorear la plataforma, detectar incidentes, solucionar problemas, analizar accesos anómalos, apoyar auditorías y mantener registros de cumplimiento.

Los registros podrán incluir autenticación, llamadas de API, operaciones críticas, errores y operación del sistema, incidentes, estado y acceso de Agent/VPN o acceso remoto, cambios de alto riesgo, tareas automatizadas o por lotes y operaciones remotas de OAM.

GloryScience adoptará medidas comercialmente razonables contra el acceso, manipulación, eliminación anormal o exportación inadecuada, como control de acceso, integridad, copias de seguridad, centralización y marcas de tiempo.

Los tipos, granularidad, conservación, acceso y exportación varían según la versión, implementación, configuración, datos, riesgos, ley y Servicios contratados, y se rigen por el Contrato Principal, el DPA, este Anexo, la Order Form, la configuración o la ley. Salvo obligación legal o acuerdo escrito, GloryScience no deberá conservar registros históricos indefinidamente, facilitar todos los registros sin procesar, cumplir estándares forenses ni dar acceso más allá de las necesidades razonables.

Cuando sea exigido o razonablemente necesario, GloryScience podrá apoyar solicitudes relacionadas con incidentes, regulación o auditoría, con anonimización, agregación, extracción o restricción para proteger la seguridad, confidencialidad, otros Clientes, integridad, secretos comerciales y la ley.

Si los registros, capturas, copias, salidas de CLI/API o diagnósticos de Agent/VPN contienen materiales propietarios de fabricantes, secretos del Cliente, información sensible de ciberseguridad o datos regulados, GloryScience podrá anonimizarlos, extraerlos, limitar su exportación, aislarlos o eliminarlos y restringir el acceso, intercambio, copia o descarga.

---

7. SEGURIDAD DE RED E INFRAESTRUCTURA

GloryScience adoptará medidas razonables, incluido control de acceso a la red; firewalls, grupos de seguridad o segregación equivalente; configuración segura de la nube; parches y correcciones; separación razonable entre producción y no producción; monitoreo de capacidad, disponibilidad y seguridad; protección contra acceso malicioso, tráfico anómalo, fuerza bruta, abuso de privilegios y de los Servicios; y restricción o monitoreo reforzado de interfaces administrativas, APIs, consola, acceso remoto y componentes de alto riesgo.

Parte de la infraestructura podrá depender de proveedores de nube, red, seguridad, monitoreo, comunicaciones u otros terceros. GloryScience seleccionará proveedores con capacidad apropiada e impondrá responsabilidades mediante contratos, gestión de proveedores u otros mecanismos razonables.

---

8. SEGURIDAD DE AGENT, VPN Y ACCESO REMOTO

Debido a que Oneasy puede conectarse al entorno del Cliente mediante Agent, VPN, Connector, API, túnel, script remoto, herramienta de OAM u otro medio, las partes reconocen la elevada sensibilidad, incluido el posible acceso a equipos, interfaces de OLT/ONU, configuraciones y entornos operativos.

El acceso remoto seguirá, de forma predeterminada, la autorización del Cliente, limitación de la finalidad, privilegio mínimo, exposición mínima de la red, revocabilidad, capacidad de auditoría y control seguro.

8.1 Establecimiento y Autorización

1. El acceso se establecerá mediante aceptación del Contrato Principal y este Anexo, configuración de los Servicios, Order Form, plan de implementación, consola, acción del administrador, confirmación dentro del producto u otro método acordado.
2. Al aceptar documentos, incorporar dispositivos, configurar credenciales, habilitar Agent, VPN, Connector, API, SNMP, TR-069, TR-369, CLI, Syslog, ACS o NMS, enviar MIB, OID, resultados de SNMP walk, salidas de CLI/API, copias, registros, capturas, scripts, plantillas o materiales técnicos, o solicitar soporte, el Cliente autoriza a GloryScience, en la medida necesaria o razonablemente relacionada con la prestación, operación, mantenimiento, protección, soporte, diagnóstico, adaptación, prueba, mejora y optimización de los Servicios, a acceder, leer, recopilar, analizar, almacenar en caché, tratar, mostrar, invocar, transmitir o ayudar a operar dispositivos, sistemas, interfaces, cuentas, credenciales, datos y entornos de OAM.
3. El Cliente confirmará la propiedad, derecho operativo o de administración, autorización contractual e interna, licencia de terceros o fabricantes, exención de confidencialidad, autorización regulatoria y aviso o consentimiento del usuario final respecto de OLT, ONU, CPE, ACS, NMS, redes, interfaces, cuentas, credenciales, datos, registros, configuraciones, topologías y materiales técnicos.
4. Salvo acuerdo escrito, GloryScience no accederá proactivamente a redes, sistemas, dispositivos o datos no autorizados y podrá confiar razonablemente en las declaraciones, autorizaciones y registros del Cliente.
5. El Cliente podrá suspender, restringir o revocar el acceso mediante la consola, cambios de configuración, políticas de red, revocación de credenciales, cierre de la VPN, aviso escrito u otro medio razonable. La revocación no afecta la licitud del Tratamiento anterior ni la conservación necesaria para seguridad, auditoría, copias, controversias, ley u operación razonable.

8.2 Alcance y Límites de Red

1. Salvo acuerdo escrito, el acceso se limita a las interfaces de gestión de OLT/ONU, protocolos, puertos, cuentas, subredes, registros, telemetría, configuración y datos operativos necesarios.
2. No se utilizará para redes corporativas, finanzas, RR. HH., contenido del tráfico de usuarios finales, sistemas internos no relacionados ni entornos ajenos a los Servicios.
3. El Cliente limitará el alcance mediante segregación, firewall, grupo de seguridad, ACL, lista de permitidos, enrutamiento, jump server, cuenta dedicada u otras medidas.
4. Cuando sea viable, Agent o Connector deberá preferir una conexión saliente cifrada iniciada por el Cliente, una VPN aprobada u otro método que reduzca la superficie expuesta.

5. Los puertos públicos, subredes débilmente aisladas, cuentas compartidas, privilegios excesivos o accesos más allá de la finalidad quedarán bajo el riesgo del Cliente y podrán requerir confirmación escrita.

8.3 Gestión de Credenciales y Claves

El Cliente creará, configurará, protegerá, rotará y revocará sus cuentas, SNMP community, API Keys, tokens, credenciales de VPN, cuentas de dispositivos, claves privadas, certificados y otros secretos. GloryScience protegerá comercialmente las credenciales que administre o almacene mediante los Servicios y evitará exponer secretos completos en texto simple.

El Cliente rotará sus cuentas conforme a su propia política y tras cambios de personal o autorización, terminación, sospecha de filtración o incidente. Salvo acuerdo escrito, no proporcionará cuentas administrativas compartidas, cuentas genéricas no auditables, privilegios superiores a la finalidad ni credenciales de producción no relacionadas.

El Cliente no disfrazará, como credencial, configuración, nota, script o diagnóstico, MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documentos internos o interfaces privadas de origen desconocido, sin derecho de divulgación, sujetos a confidencialidad de terceros o prohibidos para la nube. Los materiales legítimamente proporcionados o autorizados quedan sujetos a la Sección 8.4.

8.4 Seguridad de Materiales Técnicos y de Fabricantes

"Materiales Técnicos de Terceros" comprende todo material de dispositivos, redes, protocolos, interfaces o fabricantes proporcionado, mostrado, divulgado, autorizado para lectura o generación, incluidos MIB, tablas OID, resultados de SNMP walk, documentación o salidas de CLI/API, manuales de comandos, interfaces privadas, OMCI, extensiones privadas basadas en TR-069, TR-369 o TR-181, parámetros no públicos, modelos privados, documentos ACS/NMS, firmware, plantillas de configuración, scripts, capturas, registros, soporte de fabricantes, pruebas, listas de compatibilidad y materiales sujetos a propiedad intelectual, secreto comercial, contrato o confidencialidad.

Las normas sectoriales, especificaciones de protocolos, RFC y los informes o modelos TR-069, TR-369 y TR-181 del Broadband Forum publicados no se convierten en materiales confidenciales por el soporte, referencia, implementación, análisis o adaptación de Oneasy. Su uso seguirá sujeto a derechos de autor, licencias y reglas aplicables.

Las extensiones privadas, parámetros e implementaciones no públicos, documentos internos, MIB/OID privados, CLI/API privadas, salidas de equipos, configuraciones locales, registros, capturas, SNMP walk y diagnósticos podrán constituir Datos del Cliente, datos de red, materiales técnicos, secretos comerciales o materiales restringidos.

Al enviar, configurar, autorizar la lectura, permitir la generación o solicitar el Tratamiento de esos materiales mediante Agent, VPN, Connector, API, ticket, registros, capturas, copias, CLI, diagnóstico, script o plantilla, el Cliente autoriza su Tratamiento dentro del límite necesario o razonablemente relacionado con los Servicios.

El Cliente garantizará derechos suficientes de obtención, divulgación, envío, configuración, lectura, uso y Tratamiento, y no proporcionará materiales que no pueda divulgar, copiar, sublicenciar, tratar en la nube o internacionalmente, ni materiales cuya divulgación, copia, sublicencia, Tratamiento en plataforma o uso comercial esté prohibido por un tercero.

GloryScience podrá crear y mejorar bibliotecas de protocolos y MIB/OID, mapeos, plantillas de comandos, reglas de adaptación, compatibilidad y diagnóstico, automatizaciones, pruebas, algoritmos, modelos y funciones generales basados en materiales autorizados o públicos, salidas, pruebas y experiencia operativa. Sin autorización del titular, no distribuirá a otros Clientes archivos MIB no públicos originales, tablas OID

privadas, documentación de CLI/API, firmware, documentos internos ni materiales confidenciales identificables enviados por el Cliente.

GloryScience no es auditora de la cadena de autorizaciones entre fabricantes, integradores, canales, clientes finales o terceros y, salvo obligación legal o acuerdo escrito, no verificará proactivamente el origen de los derechos, contratos, confidencialidad o licencias. Podrá rechazar, aislar, eliminar, restringir el acceso o la exportación, interrumpir el Tratamiento o suspender Agent/VPN, acceso remoto, API, registros, soporte o funciones por un riesgo razonable de seguridad, confidencialidad, propiedad intelectual, licencia, secreto de las comunicaciones, protección de datos o cumplimiento, sin que ello constituya incumplimiento.

8.5 Operaciones, Aprobación y Cambios de Alto Riesgo

1. Oneasy podrá proporcionar recomendaciones de configuración y diagnóstico, tareas automatizadas o por lotes, ejecución de scripts, flujos de tickets, análisis asistido por IA y otros recursos auxiliares de OAM.
2. Para operaciones que puedan afectar la red de producción, configuraciones de OLT/ONU, VLAN, QoS, ACL, autenticación, puertos, plantillas de servicio, altas o bajas por lotes, retiro de equipos, firmware, scripts o continuidad, el Cliente realizará una aprobación, evaluación de impacto, ventana de mantenimiento, copia de seguridad, plan de reversión y guardia adecuados.
3. Salvo acuerdo escrito, las recomendaciones, automatización o acceso remoto no garantizan los resultados de la red de producción, calidad para el usuario final, continuidad, éxito de configuración o reversión.
4. El Cliente conserva el juicio, aprobación y control finales.

8.6 Registros y Pista de Auditoría

GloryScience registrará, cuando sea técnicamente viable, el estado de conexión de Agent/VPN, horarios, origen, destino, operaciones críticas, tareas de alto riesgo y anomalías. La conservación se rige por la Sección 6, configuración, Order Form, DPA o ley. El Cliente podrá consultar, exportar o solicitar resúmenes razonables cuando sean compatibles. GloryScience podrá anonimizar, agregar, extraer, aislar, eliminar, restringir la exportación o denegar contenido sin procesar para proteger la plataforma, otros Clientes, secretos, terceros o la ley.

8.7 Suspensión de Emergencia y Control de Seguridad

Si identifica razonablemente acceso no autorizado, filtración de credenciales, operación maliciosa, tráfico anómalo, movimiento lateral, intrusión en la red del Cliente, uso ilícito, riesgo regulatorio, ataque de terceros o riesgo para Oneasy, Clientes, la nube o terceros, GloryScience podrá suspender, restringir, bloquear, revocar o rechazar Agent/VPN, acceso remoto, API, automatización u operaciones de alto riesgo en la medida necesaria y notificará al Cliente cuando sea razonablemente posible.

8.8 Responsabilidad del Cliente y Limitación

El Cliente deberá evaluar y aprobar el acceso; configurar segregación, firewall y controles; aplicar privilegio mínimo; impedir usos no autorizados; instalar actualizaciones o mitigaciones recomendadas; proteger redes, OLT/ONU, dispositivos y segmentos administrativos; mantener aprobación, monitoreo, guardias y permisos; asegurar origen lícito, autorización y confidencialidad de datos y materiales técnicos; y suspender o terminar oportunamente el acceso cuando sea necesario.

Salvo dolo o negligencia grave directamente imputable a GloryScience, esta no responderá por pérdidas derivadas de fallas de seguridad, permisos, segregación, actualización o revocación del Cliente; intrusión o movimiento lateral de terceros; operación interna no autorizada; defectos de dispositivos o firmware; MIB/OID o interfaces privadas; materiales técnicos no autorizados; errores del Cliente; o aumento del riesgo por falta de medidas razonables.

La aceptación de los documentos, configuración del acceso, envío de credenciales o materiales y autorización para leer o generar SNMP walk, CLI/API, copias, registros, capturas o diagnósticos constituye autorización e instrucción. GloryScience podrá confiar en esos registros sin obtener autorización separada para cada Tratamiento ni auditar la cadena de derechos del Cliente.

---

9. GESTIÓN DE VULNERABILIDADES

GloryScience mantendrá un proceso comercialmente razonable de identificación, evaluación y priorización, parches, ajustes, mitigación o aceptación del riesgo, tratamiento prioritario de alto riesgo, avisos necesarios y seguimiento de componentes de terceros, nube, código abierto y proveedores.

Salvo disposición en una Order Form, SLA o acuerdo específico, los objetivos para vulnerabilidades confirmadas que afecten los Servicios son:

1. **Crítica:** corrección, mitigación o aislamiento previsto dentro de 7 días calendario desde la confirmación;
2. **Alta:** dentro de 30 días calendario;
3. **Media:** dentro de 90 días calendario o inclusión en una versión planificada; y
4. **Baja:** según el riesgo, impacto, planificación y razonabilidad comercial.

Estos plazos son objetivos de gestión, no un SLA, crédito de servicio, promesa absoluta ni indemnización incondicional. La duración real podrá depender de la complejidad, proveedores, nube, fabricantes, entorno del Cliente, pruebas, ventanas, continuidad o estrategia de seguridad.

Los objetivos se aplican a vulnerabilidades confirmadas de la plataforma, componentes, configuración o código bajo control de GloryScience. Los riesgos en redes y dispositivos del Cliente, OLT/ONU, CPE, firmware, interfaces privadas, terceros, nube propia o configuración del Cliente son responsabilidad del Cliente o tercero, salvo acuerdo escrito.

El Cliente no realizará, sin autorización escrita, pruebas de penetración, análisis de vulnerabilidades, carga, red team, ingeniería social, denegación de servicio u otra evaluación de la plataforma, API, producción o infraestructura. Las pruebas autorizadas requieren acuerdo previo sobre alcance, horario, método, contactos, datos, informes, corrección y limitaciones.

---

10. COPIAS DE SEGURIDAD Y RECUPERACIÓN

GloryScience mantendrá una estrategia razonable, que podrá incluir copias de bases de datos, configuraciones, registros o metadatos críticos y copias para recuperación ante desastres.

RTO, RPO, tiempo o integridad de recuperación, continuidad o procedimientos solo serán compromisos vinculantes cuando se establezcan en un SLA, Order Form o acuerdo separado. El Cliente exportará y conservará datos, configuraciones e informes importantes, especialmente antes de la terminación, reembolso, migración, tareas por lotes, automatización, OAM remoto o cambios significativos.

---

11. RESPUESTA A INCIDENTES DE SEGURIDAD

GloryScience mantendrá un proceso razonable de identificación, evaluación inicial, contención, mitigación, análisis de impacto, notificación, corrección y revisión.

Al confirmar un incidente con impacto significativo en los Datos del Cliente, datos del Tenant, Datos Personales, seguridad de los Servicios o entorno de acceso remoto, notificará sin demora indebida conforme a la ley y, cuando sea razonablemente viable y exista información preliminar confirmada, normalmente dentro de las setenta y dos (72) horas siguientes a la confirmación.

Podrá complementar la notificación por etapas cuando el caso sea complejo, siga bajo investigación, involucre nubes o redes de terceros, existan restricciones forenses, la divulgación aumente el riesgo o la ley así lo exija. En la medida de la información disponible, indicará la naturaleza, datos, sistemas o accesos afectados, impactos, medidas tomadas o planificadas, acciones recomendadas y comunicación posterior.

El Cliente cooperará oportunamente con registros, configuraciones, información de redes y dispositivos, contactos, alertas de sus herramientas y registros de acceso. GloryScience realizará esfuerzos comercialmente razonables ante retrasos o limitaciones causados por infraestructura, nube, red, fabricantes, entorno del Cliente o fuerza mayor.

La notificación de GloryScience al Cliente no sustituye el aviso del Cliente a autoridades, usuarios finales, abonados, empleados o terceros, salvo obligación legal o acuerdo escrito. El Cliente evaluará y cumplirá sus propias obligaciones regulatorias y legales.

---

12. SEGURIDAD DEL PERSONAL

GloryScience aplicará confidencialidad, aprobación y revocación de permisos, capacitación de concientización, restricción y supervisión de accesos privilegiados y controles reforzados o auditoría según el riesgo de la función.

Podrá utilizar empleados, afiliados, contratistas o proveedores, imponiendo obligaciones apropiadas. Para el acceso fuera de Hong Kong, aplicará los controles de acceso, confidencialidad, transferencia internacional, registros y acceso mínimo exigidos por el DPA, la Política de Privacidad, el Contrato Principal y la ley.

---

13. SUBENCARGADOS Y PROVEEDORES TERCEROS

GloryScience podrá utilizar proveedores de infraestructura en la nube, procesamiento de pagos, registros y monitoreo, tickets y soporte, correo electrónico y comunicaciones, herramientas de seguridad, IA cuando corresponda, dominio, CDN, autenticación, alertas, análisis u otros servicios auxiliares. Adoptará medidas comercialmente razonables para imponer protección de datos, confidencialidad y seguridad compatibles.

El aviso y la objeción a Subencargados se rigen por el DPA, la Política de Privacidad o el Contrato Principal. Para continuidad, incidentes, interrupción de un proveedor, cumplimiento o ajuste de infraestructura, GloryScience podrá sustituir o suspender proveedores y notificará a los Clientes afectados cuando sea razonablemente viable.

---

14. SEGURIDAD DE IA Y USO DE DATOS

Algunas funciones podrán utilizar IA, machine learning, grandes modelos de lenguaje, RAG, análisis automatizado, análisis auxiliar de RCA u otros recursos.

Sin autorización escrita, GloryScience no utilizará Datos del Cliente identificables para entrenar modelos generales de IA. Aplicará medidas razonables para restringir el acceso a funciones de IA, evitar transferencias

innecesarias a terceros, clasificar las salidas como auxiliares o informativas, exigir revisión humana antes de ejecutar recomendaciones o automatizaciones en producción y, de forma comercialmente razonable, registrar entradas, salidas, llamadas, aprobaciones o ejecuciones críticas para auditoría y solución de problemas.

Si el Cliente configura su propia API Key de LLM, modelo, nube, plugin o IA externa, evaluará los términos, Tratamiento de datos, transferencias, confidencialidad, seguridad y costos. Fuera de los asuntos de Oneasy controlados por GloryScience, esta no controla al proveedor elegido ni responde por el entrenamiento, conservación, calidad, cumplimiento, disponibilidad o incidentes de ese tercero.

El Cliente no aplicará contenido, RCA, configuración, scripts o automatización generados por IA a producción sin revisión humana. Responderá por errores, interrupciones, fallas, reclamaciones o pérdidas derivadas de esa ejecución, salvo dolo o negligencia grave directamente imputable a GloryScience y responsabilidad que no pueda excluirse por ley.

Cuando GloryScience seleccione IA, modelos, API de nube, RAG, bases vectoriales o servicios similares que traten datos identificables, gestionará la transferencia y al proveedor conforme al DPA, la Política de Privacidad, el mecanismo de Subencargados y la ley y, salvo disposición aplicable, exigirá de forma comercialmente razonable que el proveedor no use datos identificables para entrenar modelos generales.

---

15. RESPONSABILIDADES DE SEGURIDAD DEL CLIENTE

El Cliente deberá:

1. gestionar Usuarios Autorizados y permisos;
2. habilitar MFA o autenticación fuerte cuando sea compatible;
3. proteger contraseñas, API Keys, tokens, VPN, SNMP community, cuentas, claves y certificados;
4. configurar segregación, firewall, ACL, listas de permitidos, rutas y control de acceso;
5. proteger OLT, ONU, servidores, firewalls, switches, routers, ACS/NMS y segmentos administrativos;
6. mantener copias de datos y configuraciones críticas;
7. revisar cambios, recomendaciones de IA, automatizaciones, tareas por lotes, scripts y OAM remoto;
8. garantizar autoridad legal sobre redes y equipos;
9. garantizar el origen, autorización y confidencialidad de MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documentos de fabricantes, interfaces privadas, scripts, capturas, registros, plantillas y materiales técnicos;
10. no enviar interceptaciones ilegales, comunicaciones no autorizadas, datos contrarios al secreto de las comunicaciones ni datos sensibles inadecuados;
11. revocar o cambiar credenciales tras la terminación, cambios de personal, filtraciones, cambios de permisos o incidentes; y
12. designar un contacto de seguridad y cooperar oportunamente en incidentes, anomalías remotas u operaciones de alto riesgo.

El Cliente evaluará y asumirá los efectos de los cambios, automatización, tareas por lotes y OAM remoto y cumplirá sus obligaciones locales de telecomunicaciones, ciberseguridad, protección de datos, secreto e infraestructura crítica.

---

16. DOCUMENTACIÓN DE SEGURIDAD Y APOYO DE AUDITORÍA

Previa solicitud razonable, GloryScience podrá facilitar materiales divulgables o confidenciales, como una descripción general o white paper, un resumen de TOMs y Subencargados, flujos de datos, procesos de incidentes y vulnerabilidades, resúmenes de pruebas o evaluaciones, certificaciones disponibles, cuestionarios empresariales y apoyo acordado.

Salvo acuerdo escrito, no aceptará auditorías presenciales irrestrictas; pruebas en producción; análisis, carga, red team o validaciones no autorizadas; acceso a sistemas internos, código fuente, modelos, prompts, consola de infraestructura, datos de otros Clientes o secretos; solicitudes que afecten la seguridad, estabilidad, continuidad o a terceros; ni solicitudes excesivas, repetitivas o sin necesidad real. El apoyo adicional, evaluaciones especiales, cumplimiento personalizado, cooperación regulatoria, visitas, cuestionarios extensos o informes en formato del Cliente requerirán un acuerdo y podrán generar costos.

---

17. SUPRESIÓN Y ELIMINACIÓN SEGURA

Tras el cierre de la cuenta, terminación, período de exportación o solicitud válida, GloryScience tratará los Datos del Cliente conforme al Contrato Principal, la Política de Privacidad, el DPA y la ley. En general:

1. el Cliente podrá exportar datos del Tenant dentro de treinta (30) días, salvo disposición diferente;

2. GloryScience iniciará y completará un proceso comercialmente razonable de supresión o anonimización en producción dentro de noventa (90) días tras la terminación;

3. se exceptúan copias, registros de seguridad, auditoría e incidentes, registros financieros, conservación legal, controversias y datos cuya conservación esté permitida o exigida;

4. los datos en copias históricas se eliminarán o se volverán irrecuperables conforme a la rotación, sobrescritura o expiración, sin obligación de eliminar aisladamente la copia de un Cliente;

5. los datos conservados se tratarán solo para cumplimiento, seguridad, controversias, recuperación, auditoría, finanzas o ley; y

6. GloryScience podrá suprimir, anonimizar, sobrescribir, aislar, restringir el acceso o utilizar otro método comercialmente razonable.

---

18. CONTINUIDAD DEL NEGOCIO

GloryScience mantendrá planes comercialmente razonables de continuidad y recuperación ante desastres. Sin un SLA, Order Form o acuerdo específico, los planes, RTO, RPO, objetivos, procedimientos o copias no constituyen compromisos vinculantes. Los Clientes empresariales, regulados o críticos podrán acordar disponibilidad, respuesta, RTO, RPO, créditos, simulacros o informes mediante un Enterprise SLA, Anexo u Order Form.

---

19. LIMITACIONES

Este Anexo no promete seguridad absoluta, operación ininterrumpida, ausencia de pérdidas o incidentes, responsabilidad de GloryScience por la red, dispositivos, configuraciones, credenciales, permisos, terceros o usuarios finales del Cliente, certificaciones no declaradas, ausencia de fallas en OLT/ONU, compatibilidad, resultados de IA/RCA o automatización, ni asunción de las obligaciones legales intransferibles del Cliente como ISP, operador de telecomunicaciones, redes o infraestructura crítica.

Se aplican las limitaciones de la Sección 9 del Contrato de Servicios SaaS, excepto la responsabilidad cuya limitación esté prohibida por ley.

---

20. LEY APLICABLE Y RESOLUCIÓN DE CONTROVERSIAS

Se aplican la ley y el mecanismo de resolución de controversias de la Sección 12 del Contrato de Servicios SaaS de Oneasy.

---

21. ORDEN DE PRELACIÓN

Este Anexo prevalece en los asuntos de seguridad indicados en la Sección 1; el DPA prevalece cuando también haya Tratamiento de Datos Personales, transferencias, Subencargados, derechos de Titulares, notificación de violaciones u obligaciones de protección de datos.

Salvo disposición expresa en un instrumento autorizado, el orden es:

1. Order Form, Subscription Order, SOW o Enterprise SLA;
2. Data Processing Agreement o DPA;
3. Security Addendum;
4. Contrato de Servicios SaaS de Oneasy;
5. Términos de Pago y Reembolso;
6. Política de Privacidad;
7. Política de Cookies; y
8. Términos de Uso del Sitio.

Para pagos, reembolsos, facturación, renovación, contracargos o mora, prevalecen los términos de pago; para el acceso al sitio, los Términos de Uso; para cookies, la Política de Cookies; para Datos Personales, el DPA; y para controles de seguridad, este Anexo, sin perjuicio de la prioridad del DPA en asuntos de protección de datos.

ANEXO A - MATRIZ DE CONTROLES DE SEGURIDAD

1. **Gobernanza:** responsable o equipo, políticas, respuesta y análisis de riesgos. ISO 27001, SOC 2 y CSA CCM son referencias, salvo certificación.
2. **Control de acceso:** RBAC, privilegio mínimo, aprobaciones, revisiones y restricción de producción. El Cliente administra las funciones y usuarios del Tenant.

3. **Autenticación:** contraseñas, MFA cuando esté disponible y controles reforzados para privilegios. El Cliente debe habilitar MFA cuando sea compatible.
4. **Cifrado en tránsito:** TLS 1.2 o superior, o equivalente, cuando sea viable, sujeto a limitaciones de dispositivos, integraciones o protocolos heredados.
5. **Protección en reposo:** cifrado, segregación, acceso o equivalente según el componente.
6. **Secretos:** protección de credenciales, ciclo de claves y tokens y enmascaramiento razonable. El Cliente controla sus credenciales de dispositivos, VPN y API, salvo acuerdo.
7. **Materiales técnicos de terceros:** el envío, configuración, lectura autorizada o generación permitida constituye autorización; GloryScience podrá rechazar, aislar, eliminar o limitar materiales de alto riesgo. El Cliente no enviará MIB/OID, SNMP walk, CLI/API, OMCI, firmware ni materiales de fabricantes sin autorización.
8. **Registros:** autenticación, seguridad de API, acciones administrativas, Agent/VPN e incidentes. La conservación se rige por la Sección 6, configuración, Order Form, DPA, política y ley.
9. **Red:** firewall, grupos de seguridad, acceso restringido, protección de interfaces y monitoreo de abusos. No sustituye la seguridad de la red del Cliente.
10. **Infraestructura:** configuración de nube, separación de entornos y monitoreo, sujetos a dependencias de terceros.
11. **Vulnerabilidades:** objetivos basados en riesgos, parches, mitigación y avisos, sin constituir un SLA independiente.
12. **Incidentes:** detección, contención, notificación, corrección y actualizaciones; objetivo de aviso inicial en 72 horas para un incidente significativo confirmado cuando sea viable.
13. **Copias de seguridad:** estrategia comercialmente razonable; RTO y RPO vinculantes solo si se acuerdan.
14. **Personal:** confidencialidad, permisos, capacitación y supervisión; contratistas sujetos a obligaciones adecuadas.
15. **Subencargados:** selección, contratos y gestión; aviso y objeción conforme al DPA, la Política de Privacidad o el Contrato Principal.
16. **Acceso remoto:** límites de Agent/VPN, autorización, registros, revocación y suspensión de emergencia; véase el Anexo C.
17. **IA:** sin entrenamiento con datos identificables sin autorización, salidas consultivas y revisión humana; los riesgos de LLM/API Key proporcionados por el Cliente permanecen a su cargo.
18. **Auditoría:** resúmenes, TOMs, cuestionarios e informes disponibles; sin auditorías irrestrictas, pentest ni acceso al código o infraestructura.

ANEXO B - LISTA DE VERIFICACIÓN DE SEGURIDAD DEL CLIENTE

Esta lista describe responsabilidades y recomendaciones y no impone a GloryScience la auditoría o monitoreo del entorno del Cliente, salvo acuerdo escrito.

El Cliente deberá, como mínimo:

1. habilitar MFA para administradores y usuarios privilegiados cuando sea compatible;
2. utilizar contraseñas fuertes y rotarlas;

3. controlar API Keys, tokens, SNMP community, cuentas, claves, certificados y VPN/Agent;

4. eliminar usuarios sin necesidad de acceso;

5. limitar la red accesible mediante VPN/Agent;

6. segregar los segmentos de gestión de OLT/ONU;

7. utilizar firewalls, ACL, listas de permitidos, cuentas dedicadas o jump server;

8. revisar recomendaciones de IA, automatizaciones, lotes y operaciones de alto riesgo;

9. realizar copias y preparar la reversión antes de cambios significativos;

10. revisar registros de operación y acceso remoto;

11. instalar actualizaciones de Agent/VPN o mitigaciones recomendadas;

12. revocar o rotar credenciales después de cambios, terminación o sospecha;

13. designar un contacto y cooperar en investigaciones;

14. garantizar autorización legal para equipos, redes y datos;

15. no enviar MIB, OID, SNMP walk, CLI/API, OMCI, firmware, documentos internos, interfaces privadas, scripts, capturas, registros, plantillas ni materiales de terceros sin derechos; y

16. no enviar interceptaciones ilegales, comunicaciones no autorizadas ni datos de alta sensibilidad inadecuados.

ANEXO C - CUADRO DE CONTROL DE ACCESO REMOTO

Autorización

Posición predeterminada: el acceso exige autorización mediante contrato, configuración, SOW, consola u otro método acordado.
Responsabilidad del Cliente: confirmar la autoridad legal y operativa.

Método de Conexión

Posición predeterminada: Agent, VPN, Connector, API o túnel compatible y acordado.
Responsabilidad del Cliente: aprobar la implementación y mantener controles de red.

Alcance de Red

Posición predeterminada: interfaces, protocolos, puertos, cuentas y subredes necesarias de OLT/ONU.
Responsabilidad del Cliente: restringir la red, puertos, rutas, ACL y firewall.

Alcance Prohibido

Posición predeterminada: sin acceso a redes corporativas, RR. HH., finanzas, sistemas no relacionados o contenido del tráfico, salvo acuerdo expreso.
Responsabilidad del Cliente: no exponer sistemas ajenos a los Servicios.

Credenciales

Posición predeterminada: protección razonable de las credenciales gestionadas en Oneasy.
Responsabilidad del Cliente: crear, rotar, revocar y limitar sus credenciales.

Materiales Técnicos

Posición predeterminada: los materiales autorizados podrán tratarse para los Servicios, adaptación, diagnóstico y mejora; GloryScience podrá rechazar, aislar, eliminar, limitar la exportación o interrumpir materiales no autorizados o de alto riesgo.
Responsabilidad del Cliente: confirmar los derechos sobre MIB/OID, SNMP walk, CLI/API, OMCI, firmware y materiales de fabricantes y no enviar materiales restringidos mediante Agent, VPN, API, soporte, registros o diagnósticos.

Privilegios

Posición predeterminada: privilegio mínimo y acceso limitado a la finalidad.
Responsabilidad del Cliente: evitar cuentas administrativas compartidas y privilegios innecesarios.

Operaciones de Alto Riesgo

Posición predeterminada: aprobación, ventana, copia de seguridad, reversión y pista cuando sea viable.
Responsabilidad del Cliente: evaluar el impacto y mantener el control operativo final.

Registros

Posición predeterminada: conexión, acceso y operaciones críticas registrados cuando sea viable.
Responsabilidad del Cliente: revisar e informar anomalías oportunamente.

Revocación

Posición predeterminada: el Cliente puede pausar, restringir o revocar mediante control técnico o aviso.
Responsabilidad del Cliente: implementar y confirmar la desactivación cuando sea necesario.

Suspensión de Emergencia

Posición predeterminada: GloryScience puede suspender o restringir por seguridad, ley, abuso o riesgo.
Responsabilidad del Cliente: cooperar con la investigación y corrección.

IA y Automatización

Posición predeterminada: las salidas son auxiliares, salvo acuerdo expreso.
Responsabilidad del Cliente: revisión humana antes de la ejecución en producción.

Cooperación en Incidentes

Posición predeterminada: GloryScience proporciona avisos y actualizaciones razonables sobre incidentes significativos confirmados.
Responsabilidad del Cliente: facilitar registros, contactos, información de dispositivos y apoyo local a la investigación.