ADJUNTO DE SEGURIDAD DE SAAS

Introducción: Hyland mantiene y gestiona un programa de seguridad integral por escrito que cubre el Servicio en la Nube de Hyland diseñado para proteger: (a) la seguridad e integridad de los Datos del Cliente; (b) contra amenazas y peligros que puedan impactar negativamente los Datos del Cliente, y (c) contra el acceso no autorizado a los Datos del Cliente, y dicho programa incluye lo siguiente:

I. Gestión de Riesgo.

a. Realizar una evaluación anual de riesgos diseñada para identificar amenazas y vulnerabilidades en las salvaguardas administrativas, físicas, legales, regulatorias y técnicas utilizadas para proteger el Servicio en la Nube de Hyland.

b. Mantener un proceso documentado de remediación de riesgos para asignar la titularidad de los riesgos identificados, establecer planes y plazos de remediación y proporcionar un monitoreo periódico del progreso.

II. Programa de Seguridad de la Información.

a. Mantener un programa documentado de seguridad de la información integral del Servicio en la Nube de Hyland. Este programa incluirá las políticas y procedimientos alineados con las prácticas estándar de la industria, que pueden incluir ISO 27001/27002 u otras normas equivalentes.

b. Dicho programa de seguridad de la información debe incluir, si aplica: (i) seguridad física y cibernética adecuada donde se procesarán y/o almacenarán los Datos del Cliente; y (ii) precauciones razonables tomadas con respecto al empleo del personal de Hyland.

c. Estas políticas serán revisadas y actualizadas anualmente por la gerencia de Hyland.

III. Organización de la Seguridad de la Información. Asignar responsabilidades de seguridad a los individuos o grupos de Hyland adecuados para facilitar la protección del Servicio en la Nube de Hyland y los activos asociados.

IV. Seguridad de Recursos Humanos.

a. Los empleados de Hyland deben someterse a una evaluación integral durante el proceso de contratación. Se realiza verificación de antecedentes y validación de sus referencias para determinar si las calificaciones de los candidatos son apropiadas para el puesto propuesto. Sujetas a las restricciones impuestas por la ley aplicable y con base en la jurisdicción, estas verificaciones incluyen verificaciones de antecedentes penales, validaciones de empleo y validación de estudios.

b. Asegurar que todos los empleados de Hyland estén sujetos a compromisos de confidencialidad y no divulgación previamente a proporcionar acceso al Servicio en la Nube de Hyland o a los Datos del Cliente.

c. Garantizar que los empleados de Hyland reciban capacitación sobre conciencia de seguridad diseñada para brindarles conocimientos de seguridad de la información para proporcionar la seguridad, disponibilidad y confidencialidad de los Datos del Cliente.

d. Tras una terminación del vínculo de un empleado o cambio de rol de un empleado de Hyland, Hyland se asegurará de revocar su acceso de empleado al Servicio en la Nube de Hyland de forma oportuna y que se regresen todos los activos de Hyland tanto de información como físicos.

V. Gestión de activos.

a. Mantener políticas y procedimientos de gestión de información y activos. Esto incluye la titularidad de activos, un inventario de activos, lineamientos de clasificación y estándares de manejo que pertenecen a los activos de Hyland.

b. Mantener los procedimientos de manejo de medios de Hyland para garantizar que los medios de Hyland que contienen Datos del Cliente estén cifrados y almacenados en un lugar seguro sujeto a estrictos controles de acceso físico.

c. Cuando un dispositivo de almacenamiento de Servicio en la Nube de Hyland haya llegado al final de su vida útil, los

procedimientos incluyen un proceso de desmantelamiento diseñado para evitar que los Datos del Cliente sean expuestos a personas no autorizadas utilizando las técnicas recomendadas por NIST para destruir datos como parte del proceso de desmantelamiento.

d. Si el dispositivo de almacenamiento no puede ser desmantelado con estos procedimientos, el dispositivo será virtualmente destruido, desmagnetizado, borrado o físicamente destruido de acuerdo con las prácticas estándar de la industria.

VI. Controles de acceso.

a. Mantener una política de acceso lógica y los procedimientos correspondientes. Los procedimientos de acceso lógico definirán la solicitud, aprobación y proceso para otorgar accesos para el personal de Hyland. El proceso de acceso lógico restringirá el acceso de los usuarios de Hyland (local y remoto) con base en su puesto (acceso apropiado con base en el puesto/perfil) para las aplicaciones y bases de datos. Se hará una rectificación periódica del acceso de usuarios de Hyland para determinar los accesos y privilegios. Se documentarán los procedimientos para incluir y dar baja a los usuarios del personal de Hyland en momento oportuno. Se documentarán los procedimientos relacionados con inactividad del usuario del personal de Hyland que conducen a la suspensión y eliminación de la cuenta.

b. Limitar el acceso a los Datos del Cliente para el personal de Hyland que tiene la necesidad de acceder a los Datos del Cliente como condición para desempeñar los servicios de Hyland en virtud de este Contrato. Hyland utilizará el principio de "menor privilegio" y el concepto de "mínimo necesario" para determinar el nivel de acceso de todos los usuarios de Hyland a los Datos del Cliente. Hyland utiliza contraseñas robustas sujetas a requisitos de complejidad y rotación periódica e el uso de autenticación multifactor.

c. Garantizar la existencia de controles de acceso estrictos para acceso de Hyland a los Datos del Cliente. Los administradores del Cliente controlan el acceso de sus usuarios, los permisos de los usuarios y la retención de los Datos del Cliente en la medida en que dichos controles estén disponibles para el Cliente con respecto al Servicio en la Nube de Hyland.

VII. Limites del Sistema.

a. Hyland no es responsable por ningún componente de sistema que no se encuentra dentro de la Plataforma en la Nube de Hyland, n incluidos los dispositivos de red, la conectividad de red, las estaciones de trabajo, los servidores y el software de propiedad del Cliente o de terceros y operado por estos. Hyland podrá proveer soporto para estos componentes bajo su razonable discreción.

b. Los procesos ejecutados dentro de la Plataforma den la Nube de Hyland están limitados a aquellos que son ejecutados por un empleado de Hyland (o un tercero autorizado por Hyland) o procesos que sean ejecutados dentro de los límites del sistema establecidos por Hyland, en su totalidad. Esto incluye, entre otros, la instalación de hardware, la instalación de software, la replicación de datos, la seguridad de los datos y los procesos de autenticación.

c. Ciertos procesos empresariales pueden cruzar estos límites, lo que significa que una o más tareas se ejecutan fuera de los límites del sistema establecidos por Hyland para la Plataforma en la Nube de Hyland, una o más tareas son ejecutadas por personas que no son persona de Hyland (o terceros autorizados), o una o más tareas se ejecutan en función de solicitudes por escrito realizadas por el Cliente. En tal caso, Hyland proporcionará soporte para dichos procesos en la medida en que se produzcan dentro de los límites establecidos del sistema de Hyland, pero Hyland no es responsable de proporcionar soporte para dichos procesos en la medida en que se produzcan fuera de dichos límites establecidos del sistema. A su discreción razonable, Hyland puede proporcionar soporte limitado para procesos que ocurran fuera de dichos límites del sistema establecidos para la Plataforma en la Nube de Hyland. Entre los ejemplos de procesos empresariales que cruzan estos límites se incluyen, entre otros, los cambios de configuración del Servicio en la Nube de Hyland, el procesamiento que se produce dentro del Servicio en la Nube de Hyland, el procesamiento que se produce dentro del Servicio en la Nube de Hyland, la autorización de usuarios y la transferencia de archivos.

VIII. Cifrado.

a. Los Datos del Cliente deberán ser cargados solamente al Servicio den la Nube de Hyland en formato encriptado cómo SFTP, TLS/SSL, o algún método equivalente.

b. Los Datos del Cliente se encriptarán en reposo.

c. Cuando el uso de la funcionalidad de cifrado pueda ser controlado o modificado por el Cliente, en caso de que el Cliente decida modificar el uso o desactivar cualquier funcionalidad de cifrado, lo hará por su cuenta y riesgo.

IX. Seguridad Física y Ambiental.

a. La Plataforma en la Nube de Hyland utiliza centros de datos o proveedores de servicios externos que han demostrado el cumplimiento de una o más de las siguientes normas (o un equivalente razonable): Organización Internacional de Normalización ("ISO") 27001 y/o Informes de Controles de Organizaciones de Servicios ("SOC") para Organizaciones de Servicios del Instituto Americano de Contadores Públicos Certificados ("AICPA"). Estos proveedores proporcionan conectividad a Internet, seguridad física, energía y sistemas ambientales y otros servicios para la Plataforma en la nube de Hyland.

b. Hyland utiliza arquitectura y tecnologías diseñadas para promover tanto la seguridad como la alta disponibilidad.

X. Seguridad de las Operaciones.

a. Mantener documentados los procedimientos operativos de la nube de Hyland.

b. Mantener controles de gestión de cambio para garantizar que los cambios a los sistemas de producción del Servicio en la Nube de Hyland realzados por Hyland estén autorizados y revisados adecuadamente antes de su implementación. El Cliente es responsable de probar todos los cambios de configuración, cambios de autenticación y actualizaciones implementadas por el Cliente o por Hyland a petición del Cliente antes del uso del Servicio en la Nube de Hyland en producción. En casos en los que el Cliente depende de Hyland para implementar cambios a su nombre, los Administradores de Seguridad del Cliente ("CSAs") deberán enviar una solicitud por escrito (por ejemplo, un correo electrónico u otro método proporcionado por Hyland) describiendo el cambio, o establecer en una Propuesta de Servicios. Hyland realizará cambios de configuración programados que se espera afecten el acceso del Cliente a su Servicio en la Nube de Hyland durante una ventana de mantenimiento planificada. Hyland puede hacer cambios de configuración que no afecten al Cliente durante el horario laboral regular.

c. Monitorear los niveles de uso y capacidad dentro de la Plataforma en la Nube de Hyland para planear adecuada y proactivamente el crecimiento futuro.

d. Utilización de tecnologías de protección contra virus y malware, configuradas para cumplir los estándares comunes del sector diseñados para proteger los Datos del Cliente y los equipos ubicados dentro de la Plataforma en la Nube de Hyland frente a infecciones de virus o cargas útiles maliciosas similares.

e. Implementar procedimientos de recuperación de desastres y continuidad del negocio. Estos incluirán la replicación de los Datos del Cliente a un centro de datos secundario.

f. Mantener un proceso de registro del sistema y la seguridad para capturar registros críticos del sistema establecidos por Hyland. Estos registros deberán ser guardados por un periodo mínimo de seis meses y revisados periódicamente.

g. Mantener los requisitos de refuerzo del sistema y los estándares de configuración para los componentes desplegados en la Plataforma en la Nube de Hyland. Garantizar que los servidores, los sistemas operativos y el software de soporte utilizados en la Plataforma en la Nube de Hyland reciben todos los parches de seguridad Críticos y Altos de forma oportuna, pero en ningún caso más de 90 días después de su publicación, sujeto a la siguiente frase. En caso de que alguno de estos parches de seguridad afecte negativamente al Servicio en la Nube de Hyland, Hyland hará todo lo posible por implementar controles compensatorios hasta que esté disponible un parche de seguridad que no afecte negativamente al Servicio en la Nube de Hyland.

h. Realizar escaneos o análisis de vulnerabilidades de la Plataforma en la Nube de Hyland al menos trimestralmente y remediar todas las vulnerabilidades críticas y altas identificadas de acuerdo con sus procedimientos de gestión de parches.

i. Realizar pruebas de penetración de la Plataforma en la Nube de Hyland por lo menos una vez al año.

XI. Seguridad de las Comunicaciones.

a. Implementar controles de seguridad de la Plataforma en la Nube de Hyland para proteger los recursos de información dentro de la Plataforma en la Nube de Hyland.

b. Cuando se admita, tras la implementación y después anualmente, el Cliente puede solicitarle a Hyland acceso limitado al Servicio en la Nube de Hyland del Cliente para una lista de direcciones IP predefinidas sin costo adicional.

XII. Relaciones con el Proveedor. Mantener un Programa de Gestión de Proveedores para los proveedores críticos. Este programa garantizará la evaluación anual de los proveedores críticos.

XIII. Incidente de Seguridad.

a. Emplear estándares de respuesta a incidentes que se basan en los estándares de la industria aplicables, como ISO 27001:2013 y el Instituto Nacional de Estándares y Tecnología ("NIST"), para mantener los componentes de seguridad de la información del entorno del Servicio en la Nube de Hyland.

b. Las respuestas a estos incidentes siguen la secuencia documentada de respuesta a incidentes de Hyland. Esta secuencia incluye la fase de activación del incidente, la fase de evaluación, la fase de escalado, la fase de respuesta, la fase de recuperación, la fase de desescalada y la fase de revisión posterior al incidente.

c. Si Hyland determina que el Servicio en la Nube de Hyland del Cliente ha sido negativamente afectado por un incidente de seguridad, Hyland entregará un resumen del análisis de causa raíz. Dicha notificación no se retrasará injustificadamente, pero ocurrirá una vez que se hayan tomado las medidas correctivas iniciales para contener la amenaza de seguridad o estabilizar el Servicio en la Nube de Hyland.

d. El análisis de causa raíz incluirá la duración del evento, la resolución, el resumen técnico, problemas pendientes y el seguimiento, incluyendo las acciones que debe realizar el Cliente para prevenir problemas futuros. No se divulgará públicamente la información del Servicio en la Nube de Hyland, incluyendo elementos de datos que requieren confidencialidad y medidas de seguridad adicionales (incluidos los de otros clientes afectados en el incidente). Si el Cliente necesita detalles adicionales de un incidente, deberán enviar una solicitud al equipo de Soporte de Hyland GCS, que se gestionará caso por caso. El proceso de divulgación de información puede requerir una revisión en sitio para proteger la confidencialidad y seguridad de la información solicitada.

e. Hyland le notificará al Cliente sobre cualquier Incidente de Seguridad dentro de las primeras 48 horas. Un “Incidente de Seguridad” significa la determinación por parte de Hyland de una divulgación real de Datos del Cliente no cifrados a una persona o entidad no autorizada que comprometa la seguridad, confidencialidad o integridad de los Datos del Cliente.

XIV. Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio.

a. Mantener un plan de continuidad del negocio y recuperación de desastres.

b. Revisar y probar el plan una vez al año.

XV. Datos Agregados.

a. Hyland es propietaria de todos los datos de registro y de facturación del Cliente y del Usuario recopilados y utilizados por Hyland que sean necesarios para la configuración de usuario, uso y facturación para el Servicio den la Nube de Hyland (“Información de Cuenta”) y todos los datos agregados, anónimos y estadísticos derivados de la del uso y operación del Servicio en la Nube de Hyland, incluyendo sin ninguna limitación, el número de registros en el Servicio en la Nube de Hyland, el número y los tipos de transacciones, configuraciones y reportes procesados como parte del Servicio en la Nube de Hyland y los resultados de desempeño del Servicio en la Nube de Hyland (los “Datos Agregados”).

b. Hyland puede utilizar la Información de Cuenta y los Datos Agregados con el fin de operar el negocio de Hyland. Para mayor claridad, la Información de Cuenta y los Datos Agregados no incluyen Datos del Cliente.

XVI. Investigación de Seguridad.

a. Monitoreando el cumplimiento de su programa de seguridad de la información. Esto incluye revisiones internas periódicas. Los resultados son compartidos con el lideres de Hyland y cualquier desviación se monitorea hasta tener la remediación.

b. Mantener un programa periódico de auditoría externa. Las certificaciones completas, cómo los informes SOC 2 disponibles, se facilitan al cliente previa solicitud por escrito.

c. El Cliente puede realizar auditorías (que incluyan evaluaciones, cuestionarios, revisiones guiadas u otras solicitudes para validar los controles de seguridad de Hyland) (cada una en adelante “Investigación de Seguridad”) de las operaciones de Hyland que participen en la entrega y el soporte continuos del Servicio en la Nube de Hyland adquirido por el Cliente anualmente (sin superar

una vez durante un periodo de 12 meses); siempre que el Cliente notifique a Hyland con antelación por escrito su deseo de realizar dicha Investigación de Seguridad mientras no coincida o cubra la misma información o alcance de: (1) cualquier control ya suministrado por una auditoría externa o evaluación ya realizada por Hyland, cómo el reporte SOC 2, ISO 27001 u otras auditorias similares o evaluación que esté a disposición del Cliente por medio de solicitud escrita del Cliente; o (2) cualquier contenido ya suministrado por Hyland a través de los SIG, CAIQ completados o cuestionarios similares a disposición del Cliente por medio de solicitud. Por cada Investigación de Seguridad, (1) Hyland y el Cliente deben acordar mutuamente el calendario, el alcance y los criterios de dicha Investigación de Seguridad, que sujeto a lo anterior, puede incluir el diligenciamiento de cuestionarios suministrados por el Cliente; (2) documentación confidencial y restringida, cómo políticas internas, prácticas y procedimientos de Hyland, incluyendo cualquier documentación solicitada por el Cliente que no pueda ser extraída de las instalaciones de Hyland debido a limitaciones físicas o políticas de restricción no serán puestas a disposición externamente o removidas de las instalaciones de Hyland y dichas revisiones deberán realizarse en las instalaciones de la empresa matriz de Hyland en Ohio, EEUU o a través de mecanismo de compartimiento de pantalla que Hyland programará para prohibir cualquier tipo de copia o captura de pantallas; (3) el Cliente está bajo el entendimiento y consentimiento que Hyland no permitirá acceso al sistema o dispositivos internos utilizados para alojar o dar soporte a los ofrecimientos de Hyland; (4) en la medida que el Cliente desee contratar a un tercero para realizar dicha Investigación de Seguridad, Hyland deberá aprobar a dicho tercero previamente por escrito, y el Cliente deberá asegurar la firma de un Acuerdo de Confidencialidad entre Hyland y el tercero, asegurando cumplir las normas de seguridad de Hyland, e el Cliente gestionará el compromiso con el tercero, asegurándose de que el tercero comprende el alcance de la Investigación de Seguridad como fue acordado mutuamente entre Hyland y el Cliente y cómo el Cliente utiliza el Servicio en la Nube de Hyland; y, (5) el Cliente deberá pagar a Hyland las tarifas (según las tarifas estándar de Hyland) por los Servicios Profesionales (incluyendo cualquier costes y gastos adicionales) que sean requeridos o solicitados a Hyland por la Investigación de Seguridad. Cuando sea necesario, Hyland proveerá un espacio privado y razonable en las instalaciones de la empresa matriz de Hyland en Ohio, EEUU para análisis de datos y reuniones. Siguiendo una solicitud escrita, razonable y con antelación, Hyland y el Cliente podrán acordar mutuamente poner a disposición a empleados o contratistas necesarios para entrevistas en persona o telefónicas durante dicha Investigación de Seguridad a cuenta y cargo del Cliente. Se prohíbe al Cliente, y el Cliente prohibirá a terceros que realice una Investigación de Seguridad, de distribuir o publicar los resultados de dicha Investigación de Seguridad a otra tercera parte sin el consentimiento previo por escrito de Hyland. No obstante cualquier disposición en contrario en el presente Contrato, ningún contenido del presente Contrato (incluyendo este aparte) requerirá a Hyland o alguno de sus afiliados a revelar alguna información que esté sujeta al privilegio abogado-cliente.