ANEXO - REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

El Contratista maximizará la seguridad de su personal, sus procesos y sus tecnologías, y del personal, los procesos y las tecnologías de cada Vendedor y Subcontratista, durante la vigencia del MGSA y de todas las Órdenes de Compra celebradas en virtud de este, de conformidad con los requisitos establecidos en el presente Anexo y todas las Leyes aplicables (colectivamente, los "**Requisitos de SI**"). La Compañía se reserva el derecho de validar la efectividad de los Requisitos de SI, y el Contratista deberá proporcionar pruebas de la validación independiente del Vendedor, Subcontratista y otros terceros.

El Contratista es responsable del cumplimiento de los Requisitos de SI por parte de cada Vendedor y Subcontratista, y las referencias al "**Contratista**" en el presente incluyen a cada Vendedor y Subcontratista. Del mismo modo, las referencias a la "**Compañía**" en este documento incluyen a cada Comprador.

El término "**Producto**", como se utiliza en el presente, significa cualquier servicio, equipo, sistema o software suministrado por el Contratista a la Compañía en virtud del presente.

La Compañía podrá modificar los Requisitos de SI periódicamente mediante notificación por escrito al Contratista.

1. Controles de acceso

1.1 El Contratista proporcionará controles de acceso, autorización y responsabilidad basado en roles dentro de su Producto en relación con los Productos que se ajusten a los requisitos y lineamientos establecidos en los Requisitos de SI. Los controles deben ser adecuados a la sensibilidad de la información.

1.2 El Contratista establecerá roles separados para los usuarios habituales, los administradores, los desarrolladores y el personal de soporte con acceso a los Productos, y dicho acceso deberá limitarse únicamente al personal autorizado que haya recibido la capacitación adecuada sobre las responsabilidades administrativas y los procesos y procedimientos de seguridad. El control de acceso debe proporcionar el acceso mínimo necesario para cada función y denegar el acceso a usuarios no autorizados.

1.3 El Producto alojado del Contratista debe incluir controles para asegurar las cuentas de servicio y las cuentas genéricas e impedir su uso no autorizado. Las contraseñas de las cuentas de servicio y de las cuentas genéricas deben cambiarse al menos una vez al año.

1.4 El Contratista garantiza que los administradores del entorno de producción del Producto alojado utilizarán autenticación de dos factores cuando proporcionen soporte administrativo remoto para el entorno.

2. Arquitectura compartida

El Contratista identificará las partes en donde los recursos compartidos sean utilizados dentro de su arquitectura por otros clientes, y los controles de seguridad implementados para proteger los datos de la Compañía del acceso de usuarios y terceros no autorizados. Los contratos de servicios que incluyan un entorno dedicado no deben contener recursos compartidos, incluidos, entre otros, todos los componentes, sistemas e infraestructuras.

3. Respuesta a incidentes y notificación de violaciones de seguridad

El Contratista informará al Centro de Operaciones de Seguridad de Sempra (CFC@sempraglobal.com y +1(866) 734-3457 en US o (800) 626-6126 en México) de cualquier violación o cualquier otro incidente de seguridad, ya sea interno o externo, que comprometa o pueda comprometer los Productos, en un plazo de 24 horas a partir del momento en que tenga conocimiento de la violación o del incidente. A partir de entonces, el Contratista proporcionará actualizaciones periódicas de la situación, y describirá las acciones que se están llevando a cabo para mitigar los daños o responder adecuadamente. La primera de estas actualizaciones debe producirse en un plazo no mayor a 72 horas después de la notificación inicial del Contratista al Centro de Operaciones de Seguridad de Sempra.

4. Cifrado

Si la Compañía determina que se acepta el cifrado para evitar la divulgación no autorizada de información de la Compañía, los Productos del Contratista deben contener controles criptográficos que cumplan los requisitos de FIPS 197, de modo que los datos y la información confidenciales de la Compañía resulten inaccesibles para usuarios no autorizados. Cuando el Producto del Contratista utilice claves de cifrado, no se deben almacenar claves de cifrado codificadas en el código fuente del Producto. Las claves de cifrado se deben almacenar y proteger independientemente del Producto mientras estén en tránsito y en reposo, y se podrán revocar para su reimplementación y mantenimiento.

5. Estándares de contraseña e inicio de sesión

5.1 Siempre que sea posible, se deberá utilizar el inicio de sesión único en todos los productos y en conexión con los sistemas de información de la Compañía. Si, en relación con cualquier Producto, el inicio de sesión único no es posible, el Contratista deberá notificarlo a la Compañía y garantizar que dicho Producto cumpla con el nivel 2 (IG2) o superior del grupo de implementación de seguridad CIS en relación con los estándares de contraseña e inicio de sesión.

5.2 Sin limitar ninguna otra disposición del MGSA o de cualquier Orden de Compra:

(a) cada Producto debe proporcionar un ID único (identificable individualmente) para las cuentas de usuario; y

(b) se debe utilizar autenticación multifactor para acceder a los sistemas y datos que la Compañía identifique como sensibles o confidenciales, o que el Contratista deba entender razonablemente que son sensibles o confidenciales.

6. Seguridad de los datos

6.1 El Contratista certifica que sus Productos proporcionan la seguridad necesaria para cumplir todas las Leyes aplicables para almacenar, procesar y transmitir datos. Esto incluye específicamente todas las leyes y normativas que exigen protecciones específicas para la información personal identificable, la información financiera y de tarjetas de crédito, y los registros de auditoría. El Contratista permitirá la validación por terceros del cumplimiento de todos los requisitos legales y reglamentarios.

6.2 En caso de que se sospeche o se produzca una violación de seguridad o una vulneración que afecte la infraestructura del Contratista, esté o no relacionada con un Producto, la Compañía podrá, a su entera discreción, bloquear o restringir todos y cada uno de los métodos y fuentes de acceso del Contratista, incluidas las comunicaciones, la conectividad y las integraciones (colectivamente, "Derecho de bloqueo"). Sin perjuicio de cualquier otro requisito u obligación de la Compañía conforme al MGSA o en cualquier Orden de Compra, si la Compañía ejerce su Derecho de bloqueo, la Compañía no tendrá ninguna responsabilidad ante el Contratista que surja o esté relacionada de cualquier otra manera con este. El acceso requerido del Contratista solo se restablecerá una vez que el Contratista haya demostrado efectivamente, a través de un tercero independiente y competente, que el Producto y los sistemas relacionados ya no suponen una amenaza potencial o real para la Compañía.

7. Detalles de registro y errores

El Contratista registrará todo el uso de la aplicación, el acceso de los usuarios, el uso indebido y los mensajes de error suficientemente detallados para supervisar y analizar el uso de los Productos, y conservará toda la información durante un mínimo de 90 días a partir de la fecha de registro. El Contratista se asegurará de que los Productos incluyan pistas de auditoría, entradas de registro con marca de tiempo e identificaciones de registro únicos. La Compañía tiene derecho a solicitar los registros en cualquier momento y sin costo alguno para esta.

8. Vulnerabilidades y defectos

8.1 El Contratista mantendrá un proceso de seguimiento de vulnerabilidades y defectos que revise los defectos potenciales para determinar el impacto en la seguridad de los Productos del Contratista y en los componentes y paquetes de software que los soportan, sin costo alguno para la Compañía. El Contratista deberá, a su cargo, probar y remediar todas las vulnerabilidades de software divulgadas públicamente y publicadas en la Base de Datos Nacional de Vulnerabilidades (*National Vulnerability Database*) (http://nvd.nist.gov/) y por el Proyecto Abierto de Seguridad de Aplicaciones Web (*Open Web Application Security Project*) (www.owasp.org) dentro de los 30 días posteriores de su publicación. Generalmente, esto evitará que los Productos sean fácilmente susceptibles a secuencias de comandos en sitios cruzados (*cross-site scripting)*, inyección SQL, desbordamiento de búfer, validación de datos y otros ataques similares.

8.2 El Contratista garantiza que los Productos no contendrán ningún código que pueda facilitar el acceso inesperado o no aprobado o interrupciones de los Productos, incluyendo: virus informáticos, gusanos (*worms*), bombas de tiempo (*time bombs*), puertas traseras (*backdoors)*, troyanos (*trojans)*, huevos de pascua (*easter eggs*) y otras formas de código malicioso, y proporcionará documentación que detalle dichos procesos a solicitud de la Compañía y sin costo alguno para esta.

9. Evaluaciones y pruebas de seguridad de terceros

9.1 El Contratista contratará a un tercero independiente ("Compañía de pruebas"), que será aprobado por la Compañía, a expensas del Contratista, para probar los Productos en busca de vulnerabilidades a través de pruebas de seguridad detalladas anuales mediante una Certificación Estándar de la Industria (por ejemplo, ISO 27001, SOC 2 Tipo 2, etc.). En lugar de una Certificación Estándar de la Industria, el Contratista puede elegir que la Compañía realice una prueba anual de los controles de Seguridad de la información que soportan los Productos, su entorno de alojamiento en Producción y su infraestructura de soporte operativo.

9.2 El Contratista exigirá a la Compañía un informe en el que se detallen los resultados de las pruebas realizadas y facilitará una copia de dicho informe a la Compañía en un plazo no mayor a 30 días desde la realización de las pruebas correspondientes. Si cualquiera de dichos informes muestra vulnerabilidades en los Productos, el Contratista proporcionará de inmediato a la Compañía un plan de remediación propuesto, con un cronograma de finalización, sin costo alguno para esta.

9.3 Todas las vulnerabilidades, defectos y errores del Producto revelados al Contratista deberán ser corregidos y remediados por este, a su cargo, en un plazo no mayor a 30 días a partir de la fecha del informe de pruebas de la Compañía correspondiente o de la fecha en la que el Contratista tenga conocimiento de dichas vulnerabilidades, defectos o errores.

10. Derecho a informar

La Compañía podrá informar, a una o más organizaciones públicas de notificación de vulnerabilidades, sobre cualquier defecto o condición de configuración que genere vulnerabilidades consideradas en estos Requisitos de SI, si dichos defectos o condiciones de configuración no se resuelven o reparan de otro modo en un plazo no mayor a 90 días posteriores a su detección, o antes si así lo acuerdan tanto la Compañía como el Contratista. Ninguna disposición contenida en los Requisitos de SI se interpretará como una limitación a las demás obligaciones del Contratista en materia de no divulgación o protección de la información descritas en el MGSA y en cualquier Orden de Compra.

11. Destrucción

El Contratista acepta que, cuando se haya superado el periodo de retención de datos, los datos ya no sean necesarios, o a solicitud de la Compañía, el Contratista destruirá los datos de forma que queden completamente inutilizables e irrecuperables, y proporcionará a la Compañía un certificado de destrucción, a solicitud de esta.

12. Documentación formal

El Contratista acepta proporcionar documentación formal para el uso, mantenimiento e implementación segura del Producto del Contratista. La documentación del Producto se actualizará en un plazo no mayor a treinta (30) días a partir de una actualización, mejora, parche o cambio similar del Producto. La documentación del producto incluirá un inventario de todos los componentes, configuraciones y dependencias.

13. Conflictos

Ninguna disposición del presente se interpretará como una limitación de las obligaciones del Contratista en materia de no divulgación o protección de la información contenidas en otras partes del MGSA y en cualquier Orden de Compra.