Anexo 2. Requerimientos de Seguridad de la Información

El **PRESTADOR** se obliga a cumplir con lo siguiente:

Los controles operativos físicos, tecnológicos y organizacionales del **CLIENTE** aquí descritos, son enunciativos mas no limitativos para garantizar el cumplimiento y compromiso del **PRESTADOR** con la seguridad de la información del **CLIENTE.**

Al efecto, el **PRESTADOR** se obliga a realizar las modificaciones que sean necesarias con motivo de la actualización de las medidas de seguridad de la información y/o procesos operativos físicos, tecnológicos y organizacionales, así como, cumplir con cualquier requerimiento normativo y/o regulaciones aplicables al **CLIENTE** relacionado con el presente contrato.

1. **General**
   - 1.1. El **PRESTADOR** reconoce que la Seguridad de la Información es muy importante para las operaciones comerciales con el **CLIENTE** y se compromete a trabajar de manera constructiva con el **CLIENTE** para garantizar que, en todo lo referente a la provisión de los Servicios, la información del **CLIENTE** es protegida con medidas efectivas de Seguridad de la Información.
   - 1.2. El **PRESTADOR** garantiza que, al celebrar el presente acuerdo, y durante el término de este, sus políticas de Seguridad de la información serán:
     a. Suficientes para cumplir con sus obligaciones de acuerdo con el presente documento;
     b. Consistentes con las directrices de seguridad del **CLIENTE** que aplican a los Servicios y con las mejores prácticas de seguridad de la Información;
     c. Revisadas y actualizadas por lo menos una vez cada año, o cuando un evento o cambio significativo lo amerite.
   - 1.3. El **PRESTADOR** debe asegurar que sus políticas de Seguridad de la información sean informadas y entendidas por todos sus Trabajadores, así como, las políticas de Seguridad de la información del **CLIENTE** que deba atender en el proyecto a que se refiere este contrato.
   - 1.4. Cualquier incumplimiento u omisión al presente apéndice y a las políticas de Seguridad de la Información del **CLIENTE** por parte del **PRESTADOR** y/o de sus Trabajadores, está sujeto a las sanciones aplicables de acuerdo con el Código de Ética y Conducta de Proveedores del **CLIENTE**.
2. **Organización de la Seguridad de la Información**
   - 2.1. El **PRESTADOR** deberá garantizar que sus Trabajadores estén conscientes de la importancia de la Seguridad de la Información, de los requerimientos incluidos en el presente documento y de las políticas de Seguridad de la información del **PRESTADOR** y del **CLIENTE**, a través de un programa de concientización de seguridad de la información para sus Trabajadores, por lo menos anualmente.
   - 2.2. Cada una de las partes, el **CLIENTE** y el **PRESTADOR**, nombrarán un contacto de Seguridad, con el fin de que estos contactos asuman la responsabilidad para revisiones periódicas del programa de concientización de Seguridad de la información y/o para resolver en forma proactiva, o en algunos casos reactiva, todo asunto relacionado a la Seguridad de la Información que surja en conexión con la prestación de Servicios o con el presente acuerdo.
3. **Cumplimiento**
   - 3.1. El **PRESTADOR** al proveer cualquier servicio o bien, debe cumplir (y hacer que todos sus Trabajadores cumplan) con las leyes y regulaciones que apliquen con dicho servicio o bien, entre algunas de ellas están: protección de datos personales, derechos de propiedad intelectual, protección de registros de información,

disposiciones de la Comisión Nacional Bancaria y de Valores y Banco de México, entre otros.

3.2. El **PRESTADOR** debe tener políticas y procedimientos para vigilar el desempeño de los servicios de sus colaboradores en cumplimiento con sus obligaciones contractuales. Dichas políticas y procedimientos deben contener aspectos que permitan, mediante auditorias validar su cumplimiento y las mejores prácticas de Seguridad de la información(Iso 27001, Iso 27002) de acuerdo a las normas y legislaciones aplicables

3.3. El **PRESTADOR** debe conservar evidencias de dichas revisiones y resultados para demostrar cualquier deficiencia o incumplimiento que sea identificable; así mismo, debe realizar las adecuaciones o modificaciones necesarias derivadas de las desviaciones o incumplimiento de requerimientos

3.4. El **CLIENTE** podrá solicitar al **PRESTADOR**, en cualquier momento, revisiones, auditorías o certificación de cumplimiento del **PRESTADOR** respecto a los requerimientos de seguridad de la información y protección de datos descrita en el presente documento, dentro de los 20 días hábiles siguientes que haya sido requerido por el **CLIENTE**.

4. Seguridad en los Recursos Humanos

4.1. El **PRESTADOR** deberá asignar responsabilidades de Seguridad a sus Trabajadores que estarán involucrados en la prestación del Servicio, dichas responsabilidades deberán estar incluidas en los términos y condiciones laborales de cada uno de sus Trabajadores, o en acuerdos de confidencialidad de tipo vinculatorio, según sea apropiado.

4.2. El **PRESTADOR** debe proporcionar capacitación sobre cualquier política de Seguridad de la Información y Privacidad aplicable, a los colaboradores o contratistas que le asistan, realizando cualquier servicio o actividad a favor del **CLIENTE**, o que tenga acceso a la información del **CLIENTE**, y debe mantener registro de cada persona que reciba capacitación sobre temas de Seguridad de la Información y Privacidad, así como la fecha en la cual dicha capacitación fue concluida, así mismo deberá mantener tales registros(o resumen de ellos), disponibles para ser inspeccionados por el **CLIENTE**, en caso de que este así lo solicite.

4.3. El **PRESTADOR** deberá proporcionar información de contacto de la persona que realiza la capacitación a los colaboradores, para que el **CLIENTE** pueda validar el seguimiento:

Empresa	Nombre completo	área/ Puesto	Email	Tel. Móvil

4.4. El **PRESTADOR** debe capacitar a los Desarrolladores en las técnicas actualizadas de configuración segura (por ejemplo; OWASP, SANS, CWE, Top 25, CERT, Secure Coding, Desarrollo Seguro etc.) incluida la forma de evitar las vulnerabilidades de codificación comunes.

4.5. El **PRESTADOR** deberá realizar capacitación en materia de incidentes de seguridad de la Información para asegurar cumplimiento con lo descrito en la sección 11 Administración de incidentes de seguridad de la información.

4.6. El **PRESTADOR** tiene que asegurar que los activos de información sean manejados únicamente por las personas (colaboradores) cuya intervención sea precisa y necesaria para la finalidad del servicio, objeto del presente contrato y con sujeción al secreto profesional y confidencialidad.

4.7. El **PRESTADOR** debe asegurar que el equipo de cómputo asignado a sus Trabajadores, que son propiedad del **PRESTADOR**, cumpla con las siguientes medidas de seguridad: a. protección de malware o código malicioso con la última versión y firmas del sistema antivirus al mes corriente autorizado por el **CLIENTE**. b. Parches de seguridad actualizados, al menos al mes corriente. c. Software de prevención y detección de intrusos basado en host. d. Cifrado del disco duro. e. Agente DLP de Prevención de fuga de información del **CLIENTE** instalado.

4.8. La administración de los medios removibles, portables y puertos de comunicación bluetooth (en caso de aplicar y con previo consentimiento del **CLIENTE**) que contienen información del **CLIENTE** sea segura de acuerdo con las mejores prácticas de seguridad que cumplan con el almacenamiento en lugar o ambiente seguro; transporte y/o eliminación segura de la información; almacenamiento de los medios de respaldo en un lugar remoto, a una distancia significativas para que esté fuera de peligro de un desastre en el sitio principal.

4.9. El **PRESTADOR** se asegurará que sus Trabajadores procesen o almacenen información del **CLIENTE** únicamente en los sistemas informáticos del **CLIENTE** o del **PRESTADOR**, y que no procesen, almacenen o transfieran información del **CLIENTE** en recursos informáticos que no sean propiedad del **CLIENTE** y del **PRESTADOR**.

4.10. El **PRESTADOR** debe asegurar que después de cualquier cambio sustancial en las funciones o responsabilidades de cualquiera de sus Trabajadores, o al terminarse la contratación de dicho personal, deben entregar al **PRESTADOR** y al **CLIENTE** todo aquel activo de información (documentación, equipo e información) que le haya sido asignado durante su periodo de servicios, así como, desactivar o cambiar contraseñas que hayan sido utilizadas por su personal que se retira del Servicio.

4.11. El **PRESTADOR** debe contar con un proceso disciplinario definido y comunicado a su personal (colaboradores) por cualquier violación o falta grave en la Seguridad de la información del **CLIENTE**.

5. Evaluación y Tratamiento de Riesgos de la información

5.1. EL **PRESTADOR** se obliga a informar inmediatamente al **CLIENTE** si identifica un riesgo de Seguridad de la Información Significativo, y debe ofrecer suficiente información acerca de cualquier acción planeada o en proceso, así como, cualquier recomendación adicional para el cliente.

5.2. En caso de que el **CLIENTE** identifique un riesgo por parte del **PRESTADOR,** deberá proporcionar un plan de remediación para mitigar dicho riesgo o en su caso evaluar la factibilidad de trabajar con el **PRESTADOR.**

5.3. El **PRESTADOR** también deberá cooperar con la evaluación periódica de los riesgos de seguridad de la información del **CLIENTE**, proporcionando la información que el **CLIENTE** le solicite.

5.4. El **PRESTADOR** debe proveer asistencia al **CLIENTE** con las evaluaciones de riesgos de información del **CLIENTE.**

5.5. Cuando en el proceso de evaluación de riesgos de Seguridad de la información (ya sea llevada a cabo por el **PRESTADOR** o el **CLIENTE**) indique que se necesita llevar algún plan de acción preventivo o de remediación, el **CLIENTE** y el **PRESTADOR** deberán cooperar entre sí para poder identificar e implementar de manera adecuada dicha acción de acuerdo con los términos de este contrato

6. Seguridad física y ambiental

6.1. El **PRESTADOR** tomará medidas adecuadas de seguridad física y ambiental para controlar el acceso a sus instalaciones y a las del **CLIENTE** de acuerdo con las políticas establecidas.

6.2. El **PRESTADOR** debe prevenir la fuga de información, pérdida, robo o violación de los activos de información, y la interrupción de las actividades del **CLIENTE**.

6.3. Las medidas preventivas adoptadas por el **PRESTADOR** de acuerdo con los párrafos anteriores deben incluir la implementación y mantenimiento de:

a. Perímetros claramente definidos de seguridad física, incluyendo controles físicos y lógicos de acceso adicionales para áreas que almacenan activos críticos de información.
b. Controles para la supervisión de visitantes en áreas seguras
c. Medidas para prevenir la fuga de información de sus instalaciones.

6.4. El **PRESTADOR** no deberá procesar, almacenar o transferir información del **CLIENTE** en ningún lugar que sea accesible al público en general, ni tener acceso a tal información desde ningún lugar que sea accesible al público en general.

6.5. El **PRESTADOR** debe asegurar que cualquier ubicación alterna o de respaldo que se utilice para propósitos de continuar con la operación de los procesos o servicios críticos de negocio del **CLIENTE**, esté sujeto a los mismos controles de seguridad de la información, a los que tiene en su ubicación principal de operación.

7. Control de Acceso

7.1. El **PRESTADOR** debe mantener y vigilar el control de acceso lógico, tanto a los sistemas, servicios y/o aplicaciones, como a la información del **CLIENTE** que se encuentre bajo su responsabilidad.

7.2. El **PRESTADOR**, debe restringir el acceso físico y lógico a los servidores y sistemas, únicamente al personal expresamente autorizado para su operación por el **CLIENTE**.

7.3. El **PRESTADOR** deberá garantizar que sus colaboradores, que tienen acceso a los sistemas informáticos o a la información del **CLIENTE** cumplan con:

a. Sus responsabilidades en lo que se refiere a procedimientos de control de acceso
b. Apliquen las mejores prácticas de seguridad de la Información en el uso de contraseñas, tales como no escribir contraseñas en papel, no compartirlas con nadie, y cambiar la contraseña periódicamente.
c. Almacenar la información del **CLIENTE** en áreas seguras y apropiadas, diseñadas para tal propósito.
d. El acceso remoto a los sistemas informáticos sea sujeto a procesos apropiados de autenticación e ingreso.
e. En caso de que el personal y equipos de el **PRESTADOR** se encuentren físicamente en las instalaciones del **CLIENTE,** deberán apegarse a las políticas de control de acceso físico y uso aceptable de las instalaciones del **CLIENTE.**
f. Cuando EL **PRESTADOR** utilice servidores propios o controlados para almacenar información del **CLIENTE** deber asegurar y garantizar:
   i. La ubicación de los servidores, ya sean de bases de datos, servidores de archivos y/o repositorios de información, entre otros, se encuentren en áreas físicamente seguras, en lugares que cuenten con acceso controlado por algún custodio de seguridad y/o cámaras de video vigilancia
   ii. Revisar que todos los controles de seguridad de los servidores se encuentren operando.
   iii. Se obliga a almacenar, resguardar, proteger y transferir los datos a través de sistemas y herramientas de transferencia segura, utilizando servidores que se encuentren protegidos con códigos de usuario y contraseñas de entrada y segundos mecanismos de autenticación, tanto generales como para el acceso de las diferentes carpetas e las que se encuentren instaladas las bases.

7.4. El **PRESTADOR**, debe implementar esquemas de segregación de funciones acorde a sus roles y actividades que desempeñan, y asignación de áreas de responsabilidad de tal manera que se reduzca la posibilidad de la modificación o el mal uso de los activos e información del **CLIENTE**

7.5. El **PRESTADOR** debe revisar los privilegios de acceso de usuario de aquellas aplicaciones, bases de datos y repositorios de documentos que sean utilizados por el **PRESTADOR**, o en representación del **CLIENTE** con la frecuencia especificada en las políticas de Seguridad de la Información del **PRESTADOR** o por lo menos una vez al año.

7.6. Asegurar que el **PRESTADOR** con el equipo de cómputo asignado (colaboradores). No tengan permisos de administrador local en su equipo y que no pueda instalar o borrar aplicaciones o modificar parámetros de configuración de su

equipo, sistema operativo o aplicaciones que disminuyan el nivel de protección de equipo y su contenido.

7.7. El **PRESTADOR** debe proteger la confidencialidad de las credenciales, se prohíbe prestar equipos de cómputo, contraseñas o cuentas de acceso para acceder a la red o aplicaciones del **CLIENTE.**

7.8. El **PRESTADOR** debe acceder sólo a la información que le ha autorizado por **CLIENTE** y únicamente por la cuenta que le haya provisto.

7.9. En caso de recibir cuentas de acceso se debe realizar el enrolamiento al Gestor de Identidad para recuperación y cambio de contraseña y en caso de que el servicio se prolongue por más de tres meses cambiarlas cada 90 días.

7.10. Eliminar o revocar las cuentas de acceso del personal (colaborador) del **PRESTADOR**, a solicitud de Gentera o cuando deje de prestar su servicio, en caso de que el sistema de información sea administrado por el **CLIENTE** deberá el **PRESTADOR** solicitar la depuración de la cuenta de acceso, a través del líder del servicio del **CLIENTE** de forma inmediata.

8. Gestión de Activos

8.1. El **PRESTADOR**, debe actuar siempre con un nivel adecuado y debida diligencia en el uso, resguardo y protección de los activos de información del **CLIENTE** para evitar el uso inadecuado, daño, robo o pérdida de los activos de información, se deben proteger responsablemente todos los activos de información que permita evitar afectaciones al **CLIENTE** en su operación normal, imagen reputacional, o exposición a riesgos operacionales, financieros, legales o de cualquier otro tipo, que sean parte del presente contrato.

8.2. El **PRESTADOR** debe mantener un inventario del personal y equipos que ejecutan los servicios, identificando software y hardware a utilizar, nombre y cuenta de acceso, ubicación, proyecto y contacto del **CLIENTE**.

8.3. El **PRESTADOR** debe garantizar que el software instalado en dichos equipos es legal, cuenta con licencias vigentes y activas y no tiene software con versiones de prueba o gratuitas.

8.4. El **PRESTADOR** debe asegurar que la configuración de los puertos USB o bluetooth no permita la conexión de dispositivos externos para la copia o ejecución de aplicaciones o información desde o hacia el equipo de cómputo personal.

8.5. En caso de que el **PRESTADOR** por motivos de otras asignaciones distintas a la del **CLIENTE**, no pueda inhabilitar los puertos USB, deberá contar con controles que garanticen que los activos de información del **CLIENTE** no son tratados de forma distinta a lo establecido en la cláusula 9.1 del presente anexo.

8.6. El **PRESTADOR** debe aplicar en los equipos de trabajo del **PRESTADOR** los parches se seguridad al sistema operativo, y software instalado; y actualizar los mismos en lapsos no mayores a un mes, aplicable a equipos que desempeñan funciones críticas de la organización.

8.7. El **PRESTADOR** debe Instalar herramientas, antivirus y antimalware, mantener actualizadas las firmas y ejecutar el escaneo y remediación de malware de manera inmediata de acuerdo a las necesidades de operación, así como, asegurar que no se usa software, paginas o sitios que se encuentren en listas negras del **CLIENTE** por ser sitios no seguros o bloqueados por su riesgo.

8.8. El **PRESTADOR** que utilice equipos de cómputo de su propiedad y/o dispositivos móviles cuyo acceso a la red del **CLIENTE** haya sido autorizado conforme a las cláusulas 8.1, 8.2 y 8.3 Seguridad en las comunicaciones, deberá apegarse a lo establecido en el presente anexo. SOLO SE PUEDEN CONECTAR EQUIPOS AUTORIZADOS COMO LAPTOPS, NO ESTÁN PERMITIDOS CELULARES O IPADS.

8.9. El **PRESTADOR** debe permitir el monitoreo, por parte del **CLIENTE** desde su entorno, por la conexión realizada por el **PRESTADOR** a la red del **CLENTE.**

8.10. El personal del **PRESTADOR** deberá bloquear el acceso a sus equipos de cómputo cuando el usuario se ausente momentáneamente o cerrar su sesión de

usuario cuando deje de utilizar el equipo, independientemente de que la configuración lo bloquee en automático después de un periodo de tiempo.

8.11. El **PRESTADOR** debe tener una política del uso de dispositivos móviles debidamente documentada que incluya una definición clara del uso de aplicaciones, así como, los requisitos y lineamientos que garanticen el cumplimiento de Seguridad de la Información y Protección de Datos personales.

8.12. Todos los servicios basados en la nube, utilizados en los dispositivos móviles de la compañía por el **PRESTADOR** deben ser autorizados para el uso y el almacenamiento de los datos del **CLIENTE.**

8.13. El **PRESTADOR** tendrá un proceso documentado de validación de aplicaciones para probar problemas de compatibilidad de dispositivos móviles, sistemas operativos y aplicaciones.

8.14. El **PRESTADOR** debe asegurar el cumplimiento de los mecanismos para el adecuado manejo, control y seguridad de la información generada, recibida, transmitida, procesada o almacenada en la ejecución de los Servicios o comisiones que se refieran a la utilización de infraestructura tecnológica, de telecomunicaciones o de procesamiento de información, que se realicen parcial o totalmente fuera del territorio nacional.

8.15. El **PRESTADOR** se abstendrá de almacenar, distribuir o duplicar la información del **CLIENTE**, a menos que sea necesario para la ejecución de los Servicios.

8.16. Si el **PRESTADOR** va a disponer o destruir cualquier activo crítico que tenga que ver con la información del **CLIENTE**, deberá asegurarse que la información almacenada en dicho activo se borre de manera irrecuperable antes de proceder con la disposición o destrucción, y que dicho activo también se destruya de manera irrecuperable.

8.17. El **PRESTADOR** notificará en forma inmediata cuando detecte que un activo utilizado para procesar o almacenar información relacionada con la prestación del Servicio ha sido perdido, robado o se ha generado un incidente de Seguridad de la Información.

8.18. El **PRESTADOR** debe realizar la devolución, borrado y/o destrucción de los activos de información en caso de terminación de funciones, reasignaciones, servicio o contrato, con la evidencia correspondiente, de común acuerdo con el **CLIENTE**, considerando la importancia de los activos de acuerdo con su confidencialidad en un plazo no mayor a 30 días naturales.

9. Administración de comunicaciones y operaciones

9.1. Cuando la prestación de Servicios requiera que el **PRESTADOR** administre u opere cualquier instalación de procesamiento de información. El **PRESTADOR** deberá hacerse responsable del aseguramiento de la operación de dicha instalación, incluyendo:

a. Comunicación de dichos procedimientos a los trabajadores del **PRESTADOR**.
b. Mantenimiento y mejoramiento de procedimientos relacionados con la transmisión y protección de la información del **CLIENTE**

1.2. La información y el software relacionados con la prestación del Servicio deben ser respaldados con regularidad por el **PRESTADOR**, permitiendo su recuperación en un estado confiable en caso de alguna contingencia.

1.3. Las redes de computadoras por las que se transmite información y en las que se encuentran conectados recursos de procesamiento de información del **CLIENTE**, deben contener controles respecto a la disponibilidad, confidencialidad e integridad.

10. Adquisición, Desarrollo y Mantenimiento de los sistemas de Información

10.1. Cuando el **PRESTADOR** necesite adquirir, desarrollar o mantener un Sistema de Información para la prestación de Servicios del **CLIENTE**, el **PRESTADOR** deberá asegurar que dicho Sistema esté protegido con las mejores prácticas de seguridad de

la información y teniendo presentes las medidas de seguridad y cumplimiento descritas en el presente anexo.

10.2. Los Sistemas de Información del **PRESTADOR** deben considerar controles para la protección de la información y la infraestructura que soporta su generación, procesamiento, almacenamiento, transmisión y destrucción, en cada fase de su ciclo de vida.

10.3. Los Sistemas de Información del **PRESTADOR**, deben considerar desde la fase de definición de requerimientos, la identificación, justificación, documentación y formalización de necesidades de seguridad

10.4. Asegurar la separación física y lógica, al igual que la administración de los ambientes de desarrollo, pruebas y producción.

10.5. El diseño y la implementación de todas las aplicaciones del **PRESTADOR** deben incluir validaciones de los datos de entrada y salida, así como para el procesamiento interno.

10.6. Las aplicaciones del **PRESTADOR**, conforme a la clasificación de la información que usa, deben proteger la confidencialidad, integridad y autenticidad de la información a través de técnicas criptográficas.

10.7. Prevención, detección y recuperación de código malicioso.

10.8. Mantener controles de seguridad apropiados para proteger las llaves criptográficas propiedad del **PRESTADOR** utilizadas para brindar los servicios al **CLIENTE** de acuerdo con los estándares y mejores prácticas de seguridad de la información

10.9. Los archivos, datos, código fuente y software de los sistemas de información del **PRESTADOR**, deben ser protegidos, de acuerdo con su nivel de importancia, en los diversos entornos incluyendo al menos ambientes para producción, desarrollo y pruebas.

10.10. Las vulnerabilidades técnicas de los sistemas de información del **PRESTADOR** deben ser identificadas, evaluadas y atendidas conforme al nivel de riesgo determinado.

10.11. El **PRESTADOR** se compromete a realizar escaneos estáticos y/o dinámicos al código fuente y/o librerías públicas/open source, de acuerdo con las mejores prácticas, herramientas reconocidas en el mercado como son MicroFocus Fortify VeraCode, IBM, AppScan, etc. corregir las deficiencias de código, así como entregar un reporte una vez al año o cuando se presente un cambio mayor al **CLIENTE** respecto a estas actividades y la solución de estas, sin un costo adicional para el **CLIENTE.**

10.12. En lo que respecta a la **Seguridad en código fuente,** el **PRESTADOR** se obliga a lo siguiente:

a. El **CLIENTE** podrá realizar revisiones periódicas(certificación) del cumplimiento de la aplicación de actualizaciones de seguridad.

b. En el caso de software personalizado, se debe definir que, durante la vigencia del contrato, se incluya un acuerdo por el cual se asegure que el código fuente será resguardo por un tercero (acuerdo escrow), con el objetivo de garantizar acceso al mismo en el supuesto que ocurra un incumplimiento por parre de el **PRESTADOR.**

c. El **PRESTADOR** debe implementar procedimientos que aseguren la calidad del código fuente que deben comprender, pero no limitarse al uso de las mejores prácticas de programación específicas (incluyendo de seguridad) a cada uno de los lenguajes utilizados, revisión entre pares de los desarrollos y seguimiento de estándares cuando los mismos estén disponibles.

d. EL **PRESTADOR** debe realizar de forma periódica los procedimientos de seguridad de la información, tanto en etapas de desarrollo como cada vez que se libera una nueva versión mayor del producto. Prestará evidencia auditable de la ejecución de estos procedimientos como parte de la entrega a EL **CLIENTE,** preferentemente validado por un auditor externo certificado.

e. Implementar procedimientos para identificar y remediar vulnerabilidades o amenazas potenciales en el producto ofrecido. Estos productos deben comprender, pero no limitarse a la revisión de código estático y sesiones de hackeo ético.

f. El **PRESTADOR** debe entregar a EL **CLIENTE** software libre de vulnerabilidades de seguridad en el código y la lógica del mismo (de acuerdo con su proceso interno de desarrollo y pruebas). En caso de que el código no sea escaneable se ejecutaran pruebas de caja negra en ambiente productivo y se remediaran las vulnerabilidades críticas, altas y medias explotables identificadas.

g. EL **PRESTADOR** debe entregar evidencia de capacitación periódica a su personal sobre técnicas de codificación segura y actualización en seguridad informática.

h. EL **PRESTADOR** se obliga a notificar a EL **CLIENTE** de manera proactiva, las vulnerabilidades de seguridad detectadas (después de la entrega) en el software proporcionado, así como las instrucciones para remediarlas.

i. EL **PRESTADOR** se compromete a aplicar el contenido a definir de los boletines de seguridad y actualizaciones en el ambiente productivo de EL **CLIENTE.**

j. En caso de ser software comercial (producto cerrado) se debe informar a EL **CLIENTE** un informe anual de las vulnerabilidades y el proceso de notificación y actualización de versiones para remediarlas.

k. En caso de ser software personalizado para EL **CLIENTE** se deberá definir junto con EL **PRESTADOR** las auditorias de forma periódica.

10.13. El **PRESTADOR** deberá tener parámetros de Hardening de acuerdo con mejores prácticas(Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST)) a nivel sistema operativo, base de datos, dispositivos de red, etc.

10.14. Activar los logs en bitácoras de los accesos y actividades administrativas en los servidores y donde técnicamente sea posible, así como almacenar esta información de acuerdo con el tiempo de retención definido en común acuerdo con el **CLIENTE**. Dichas bitácoras deberán estar protegidas con controles locales para evitar su borrado o alteración, en caso de que el tipo de operación del presente contrato y las regulaciones aplicables, así lo requieran

10.15. Enviar los logs de los accesos a las herramientas de El **CLIENTE** (SIEM o equivalente), caso sea necesario configurar la integración de los logs, esto es responsabilidad del **CLIENTE.**

10.16. El **PRESTADOR** llevará a cabo, sin costo para el **CLIENTE**, revisiones regulares (incluyendo el uso de herramientas para el cumplimiento técnico, evaluaciones de vulnerabilidades, inspecciones manuales y pruebas de penetración) de los Sistemas de Información del **PRESTADOR** y procedimientos operativos relacionados para determinar el alcance del cumplimiento de las políticas de Seguridad del **PRESTADOR**

11. Administración de Incidentes de Seguridad de la Información

11.1 El **PRESTADOR** debe mantener comunicación con sus Trabajadores, e implementar medidas necesarias para identificar, prevenir, notificar y responder a debilidades e incidentes de seguridad que afecten los Servicios, activos de información vinculados con la prestación del Servicio, o a la imagen corporativa del **CLIENTE**, incluyendo procedimientos claros que especifiquen las acciones que se deben llevar a cabo para:

a. Reportar cualquier sospecha u observación de un incidente de seguridad o debilidad de seguridad en los sistemas o servicios
b. Contener incidentes de seguridad

c. Recuperación de incidentes de seguridad y corrección de fallas del sistema
d. Comunicación con los afectados o involucrados en la recuperación del incidente de seguridad
e. Análisis de las causas de los incidentes de seguridad
f. Planeación e implementación de acciones correctivas necesarias para prevenir la recurrencia.
g. Recolección, comparación y preservación de la evidencia de forma admisible, y
h. Cuantificación y monitoreo de los tipos, volúmenes y costos de los incidentes de seguridad.

11.2. Las actividades en las que se involucran activos importantes de información del **CLIENTE**, y recursos relacionados con la misma, deben monitorearse, registrando eventos relacionados con seguridad de la información.

11.3. Los incidentes de seguridad de la información deben ser reportados al momento de su detección e identificación para su atención inmediata, efectiva y ordenada, que facilite la mejora continua en la protección de la información del **CLIENTE**.

11.4 Los eventos y las debilidades observadas en los activos importantes de información del **CLIENTE**, y aquellos activos relacionados con la misma, por Trabajadores que atenten contra la seguridad de la información deben ser comunicados(as) inmediatamente al contacto de Seguridad del **CLIENTE(csirt@gentera.com.mx)**

11.5. La respuesta a incidentes de seguridad de la información debe ser inmediata, efectiva y ordenada, facilitando la recolección de evidencia y la mejora continua en la protección de la información del **CLIENTE**.

11.6. Cuando un incidente de seguridad requiera una investigación en contra de un Trabajador o subcontratista del **PRESTADOR**, el **PRESTADOR** debe en cumplimiento con las leyes y regulaciones aplicables, tomar todas las precauciones necesarias para la recolección, retención, análisis, preservación y presentación de la evidencia, ya que puede estar en los sistemas de información del **PRESTADOR**, para concluir satisfactoriamente con dichas investigaciones. Cuando el **CLIENTE** inicie y notifique al **PRESTADOR** de acciones investigativas en relación con una sospecha de incidente de seguridad que involucre a Personal del **CLIENTE** o a la información del **CLIENTE**, el **PRESTADOR** debe proporcionar toda la ayuda necesaria que el **CLIENTE** pueda solicitar.

11.7 Realizar gestión de amenazas y vulnerabilidades que puedan presentar incidentes de seguridad con impactos adversos para el **CLIENTE**

11.8 EL **PRESTADOR** debe proporcionar una matriz de escalación para la atención a incidentes de seguridad de la información, la cual debe ser actualizada por lo menos cada 150 días o cuando haya cambios en su personal.

Empresa	Nivel	Nombre completo	área/ Puesto	Email	Tel. Fijo	Tel. Móvil	Tipo de contacto

12. Niveles de servicio de incidentes de seguridad de la información

12.1. Durante la prestación de los servicios al amparo del presente contrato EL **PRESTADOR** debe observar los siguientes niveles de servicio de atención de incidentes de seguridad de la información referidos en el numeral 8.17 a efecto de dar cabal cumplimiento da las obligaciones contraídas en el presente

Concepto	Métrica	mínimo acéptale
Atención a incidente de seguridad de la información	**Bajo**	**120 minutos**
	Medio	**60 minutos**
	Alto	**30 minutos**
	Critico	**10 minutos**
	Bajo	**5 días naturales**

Entrega de plan de remediación	**Medio**	**2 días naturales**
	Alto	**12 horas**
	Critico	**8 horas**
Entrega de reporte técnico del incidente RCA (Root cause Analysis	**Bajo**	**7 días naturales**
	Medio	**5 días naturales**
	Alto	**3 días naturales**
	Critico	**2 días naturales**

11.2 En caso de incumplimiento de alguno de los anteriores SLA´s el **PRESTADOR** será acreedor a sanciones estipuladas en el contrato marco de conformidad a la cláusula de responsabilidades.

13. **Nube**

El **PRESTADOR** debe de mantener siempre la confidencialidad, integridad y disponibilidad de la información del **CLIENTE** en el modelo de servicio y/o modelo de implementación en la nube según sea el caso (SaaS, PaaS, Iaas).

Para el caso específico de servicios nuevos a contratar en la nube dentro del alcance de los procesos necesarios para la operación del **CLIENTE**, el **PRESTADOR** del servicio, deberá atender las revisiones requeridas por el **CLIENTE** y/o por parte de la CNBV, proporcionando la dirección exacta del lugar de procesamiento y almacenamiento de información, teniendo presente que sólo es aceptable:

•En países con convenios de colaboración con las Autoridades Financieras.

•En países donde el proveedor del servicio reside y cuyo derecho interno/regulación aplicable proporcione protección a los datos de las personas, resguardando su debida confidencialidad, o bien, los países de residencia mantengan suscritos con México acuerdos internacionales en dicha materia o de intercambio de información entre los organismos supervisores, tratándose de entidades financieras.

El **PRESTADOR** debe notificar y contar con la autorización del **CLIENTE** antes de realizar cambios en la prestación del servicio que incluya:

11.1. Reubicación de la infraestructura técnica a una ubicación geográfica diferente o jurisdicción legal.

11.2. Procesamiento o almacenamiento de información en una jurisdicción geográfica o legal.

11.3. Nuevas subcontrataciones o partes externas en la prestación del servicio.

11.4. Garantizarán contar con políticas en materia de Protección de Datos Personales afines a los principios de la legislación mexicana y las mejores prácticas internacionales y se obliga a cumplir con las obligaciones de confidencialidad establecidas en el presente contrato respecto a los Datos Personales que pudiera recibir con motivo de la prestación de los servicios.

11.5. Contar con mecanismos que garanticen lo siguiente:

a) Permitir al **CLIENTE** conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

b) Permitir a **CLIENTE** limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.

c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio.

d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al **CLIENTE** y que este último haya podido recuperarlos.
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al **CLIENTE**.

11.6. Asegurar la implementación de controles y/o certificación de mejores prácticas de Seguridad de la Información y Privacidad en relación al cómputo en la nube tales como: ISO 27017 e ISO 27018.

Administración de la Continuidad del Negocio

12.1. El **PRESTADOR** deberá documentar, probar, mantener y adoptar medidas técnicas, administrativas y logísticas para mantener la continuidad de su negocio en caso de un desastre, incidente de seguridad o cualquier otra pérdida o interrupción del Servicio que involucre los sistemas informáticos.

12.2. Las medidas técnicas y administrativas mencionadas en el párrafo anterior deben asegurar:

a. La gestión de riesgos técnicos y operacionales que se deriven de los activos de información del **PRESTADOR** y del procesamiento de información del **CLIENTE** llevado a cabo por el **PRESTADOR**.
b. Prevención, detección y recuperación efectiva de interrupciones en las actividades del **CLIENTE** relacionadas con el Servicio contratado.
c. Protección de los procesos críticos del **CLIENTE** contra los efectos de fallas en los Servicios, sistemas y aplicaciones, o ante desastres, con el fin de asegurar una pronta restauración de dichos procesos.

   Mantener una gestión de cambios formal del sistema y procedimientos de administración de problemas para el sistema operativo y software de aplicación, dichos procedimientos deben cubrir: cómo los cambios son registrados y aprobados; cómo el riesgo e impacto de cambios son evaluados; cómo los cambios son probados antes de ser implementados en un ambiente productivo; cómo la implementación es planeada e implementada; y los pasos a seguir para recuperación de alguna consecuencia desfavorable ante un cambio, incluyendo revertir los efectos de cambio.
d. Asegurar que la información del **CLIENTE** se encuentre fácilmente disponible dentro de los tiempos establecidos en el Servicio
e. Documentar los procedimientos para los Trabajadores del **PRESTADOR** respecto a: Procesamiento, almacenamiento, comunicación, intercambio, eliminación, respaldo y recuperación de la información acorde con las mejores prácticas de seguridad de la información; monitoreo de las actividades recurrentes de procesamiento de datos; reinicio del sistema, recuperación y otros procedimientos que se tengan que aplicar en casos de errores o cualquier otro incidente operacional inesperado o dificultad técnica; reportes de salida y manejo de medios; y retención y revisión del registro de auditoría y de información del sistema.

12.3. El **PRESTADOR** se debe asegurar que cualquier ubicación alterna o de respaldo que se utilice para propósitos de continuar con la operación del negocio del **CLIENTE** está sujeto a los mismos controles de seguridad de la información, a los que tiene en su ubicación principal de operación. El **PRESTADOR** debe notificar al contacto de Seguridad del **CLIENTE** si utiliza, o planea utilizar la ubicación alterna y explicar los motivos por los que va a ser utilizada dicha ubicación, y garantizar que la seguridad de la información del **CLIENTE** y de los sistemas, servicios y aplicaciones del **CLIENTE** no sean afectados, previa validación y autorización del **CLIENTE**.

12.4. El **PRESTADOR** debe asegurarse que sus planes para la continuidad del negocio sean revisados, actualizados y probados al menos una vez al año. El **PRESTADOR** debe informar al **CLIENTE** las pruebas realizadas y los resultados obtenidos derivado de los planes de continuidad definidos previamente.

14. **Certificaciones**

14.1. El **PRESTADOR** se obliga a notificar anualmente y/o a entregar al **CLIENTE** las certificaciones que sean aplicables a los servicios objeto del contrato.

15. **Uso apropiado de herramientas de inteligencia artificial y otras tecnologías digitales.**

El **PRESTADOR** se compromete a garantizar la seguridad de la información en todas las actividades que impliquen el uso de inteligencia artificial (IA) y otras tecnologías digitales relacionadas, asegurando implementar y mantener medidas de seguridad de la información para proteger los datos y la infraestructura tecnología del **CLIENTE**. El **PRESTADOR** deberá:

15.1. El **PRESTADOR** debe utilizar las herramientas de inteligencia artificial (IA) de manera responsable y ética, esto NO incluye utilizarlas para:

a. Fines ilegales, fraudulentos o engañosos como fraude financiero, suplantación de identidad, hacking o cualquier otro tipo de actividad delictiva.

b. Difundir contenido ofensivo, discriminatorio, difamatorio, amenazante, violación a la privacidad o que promueva la violencia, el odio o la discriminación hacia cualquier individuo o grupo.

15.2. El **PRESTADOR** debe cumplir con las leyes y regulaciones aplicables al utilizar herramientas de inteligencia artificial (IA). Esto incluye el cumplimiento de las leyes de protección de datos, propiedad intelectual, privacidad y cualquier otra legislación relevante, así como las mejores practicas de seguridad de la información.

15.3. El **PRESTADOR** debe respetar los derechos de autor y propiedad intelectual al utilizar herramientas de inteligencia artificial (IA). No está permitido plagiar, copiar o infringir los derechos de autor o propiedad intelectual de terceros.

15.4. El **PRESTADOR** al utilizar herramientas de inteligencia artificial (IA) públicas deben acceder a ellas sólo a través de credenciales de inicio de sesión que no sean del **CLIENTE.**

15.5. El uso de las herramientas de inteligencia artificial (IA) debe estar relacionado con las actividades de la prestación del servicio y los objetivos comerciales legítimos del **CLIENTE**. No se permite el uso personal y/o no relacionado con la prestación del servicio.

15.6. El **PRESTADOR** al utilizar herramientas de inteligencia artificial (IA) en la prestación del servicio debe proteger la privacidad y la confidencialidad de la información, no está permitido divulgar información confidencial o privada a través de estas herramientas.

15.7. Los recursos de herramientas de inteligencia artificial (IA), como capacidad de cómputo y almacenamiento, el **PRESTADOR** debe utilizarlos de manera eficiente y solo para los fines autorizados.

15.8. El **PRESTADOR** debe utilizar las herramientas de inteligencia artificial (IA) de otros Terceros, de acuerdo con las pautas establecidas por el proveedor del servicio y respetar los límites y restricciones impuestas.

15.9. El **PRESTADOR** debe verificar y validar los resultados obtenidos de las herramientas de inteligencia artificial (IA). No aceptar automáticamente los resultados proporcionados sin cuestionar o validar la información. Utilizar el sentido común y la verificación cruzada para garantizar la precisión y la calidad de los resultados generados.

15.10. El **PRESTADOR** debe aceptar que al utilizar herramientas de inteligencia artificial (IA) con infraestructura o servicios del **CLIENTE**, el área de Seguridad de la Información está autorizada para realizar monitoreo y supervisión de uso para detectar cualquier actividad sospechosa o inapropiada.

15.11. El PRESTADOR no podrá utilizar información del CLIENTE para entrenar modelos públicos de Inteligencia Artificial

15.12. El PRESTADOR no podrá utilizar información del CLIENTE dentro de plataformas de Inteligencia Artificial abiertas de uso publico sin restricciones de acceso,

15.13. El PRESTADOR que utilice Inteligencia Artificial generativa para la realización de sus actividades asociadas al CLIENTE deberá notificar de su uso los servicios relacionados y los alcances de los entregables establecidos.