**ANEXO XX DI-SSI-034 MATRIZ DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO**

Yo, el suscrito **(Nombre del Representante Legal)** en mi calidad de representante legal de la empresa **(Nombre de la firma oferente)** de acuerdo con las condiciones que se estipulan en el presente anexo, en virtud de la INVITACIÓN ABIERTA No. XXX-2024 y BAJO GRAVEDAD DE JURAMENTO, certifico que:

Cumplo y acepto todos los requisitos establecidos para: (i) seguridad de la información, (ii) servicios en nube, (iii) controles de ciberseguridad y (iv) sistemas de información, detallados a continuación:

1. **Seguridad de la información**
2. Toda la información que gestione EL PROVEEDOR en el marco del contrato con LA PREVISORA S.A. es de propiedad de la Compañía y debe solamente ser usada para el propósito establecido en el contrato.
3. EL PROVEEDOR debe realizar la entrega de toda la información manejada durante la ejecución del contrato y la destruir esta una vez finalizado el servicio.
4. EL PROVEEDOR deberá enviar soportes de borrado seguro y destrucción de la información en todos los lugares donde se guarde información después de finalizado el contrato.
5. LA PREVISORA S.A. podrá revisar los procesos que lleva a cabo el proveedor o sus subcontratistas en cualquier momento a fin de verificar los controles de seguridad implementados
6. Cualquier incidente de seguridad de la información que afecte a LA PREVISORA S.A. o que involucre la información o la cadena de suministro debe ser reportado inmediatamente al supervisor del contrato y a la mesa de ayuda de LA PREVISORA S.A.
7. EL PROVEEDOR debe seguir los lineamientos establecidos por la Compañía para la gestión de accesos a sistemas de información, bases de datos, aplicaciones, áreas seguras, entre otras.
8. Los proveedores de aplicaciones tecnológicas deberán estar certificados en estándares como ISO 27001 u otros en seguridad de la información y anualmente deben enviar soportes de su vigencia.
9. Gestionar la seguridad de la información y la ciberseguridad, para lo cual podrán tener como referencia los estándares ISO 27001 - ISO 27032 o el que lo sustituya y las circulares vigentes de la Superintendencia Financiera de Colombia – SFC para efectos de seguridad de la información.
10. Implementar controles de seguridad para la información privada de LA PREVISORA S.A., que se maneja en los equipos y redes de EL PROVEEDOR.
11. Velar por que la información gestionada de LA PREVISORA S.A. esté libre de software malicioso.
12. Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.
13. Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.
14. Proteger las claves de acceso a los sistemas de información. Se debe evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo debe ser única y personalizada.
15. EL PROVEEDOR faculta a LA PREVISORA S.A. a revisar su PCN y DRP, con el fin de validar que los servicios convenidos funcionen en las condiciones pactadas.
16. Planes de Contingencia tecnológica: específicamente sobre la infraestructura tecnológica que apoya los servicios contratados con LA PREVISORA S.A.:
* Data center alterno en el que se repliquen todos los aplicativos, bases de datos, etc., que apalancan los servicios prestados a la Compañía.
* Canales de comunicación de contingencia que deben cumplir los mismos requisitos de seguridad que los canales de comunicación principales.
1. Los proveedores deberán remitir certificaciones que avalen centros de datos principales y alternos (TIER I, II o III, ICREA o similares), donde se demuestre el desempeño y la confiabilidad de las infraestructuras de los mismos.
2. Realizar pruebas a los escenarios propuestos mínimo 1 vez al año, con todos los servicios que prestan a LA PREVISORA S.A., los resultados de las pruebas deberán ser enviados junto con los planes de acción, Previsora podrá realizar seguimiento sobre estos.
3. **Requisitos para servicios en nube**

Se deberá dar cumplimiento a lo establecido Circular Básica Jurídica (C.E. 029/14) Parte I - Instrucciones generales aplicables a las entidades vigiladas Capítulo. VI - Reglas relativas al uso de servicios de computación en la nube.

1. EL PROVEEDOR debe contar y mantener vigentes, al menos, la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).
2. La información que se procese en los servicios de computación en la nube es propiedad de LA PREVISORA S.A. y el proveedor de servicios o sus subcontratistas no los puedan usar para ningún propósito diferente al establecido en el contrato.
3. EL PROVEEDOR debe ofrecer los procedimientos o formatos de datos estandarizados o interfaz de servicio que puedan garantizar la portabilidad del servicio, en caso de cambio de proveedor (API).
4. EL PROVEEDOR debe establecer un proceso formal en caso de que un incidente de seguridad de la información se llegue a materializar en la infraestructura – plataforma o software ofrecido por EL PROVEEDOR. – Informática forense.
5. EL PROVEEDOR deberá efectuar semestralmente pruebas de vulnerabilidades a la solución ofrecida y entregar los informes de estas a LA PREVISORA S.A.
6. En caso de requerirse realizar alguna remediación EL PROVEEDOR, deberá coordinar las actividades necesarias para el cierre de los hallazgos y mantener informada de la gestión realizada a la Compañía.
7. EL PROVEEDOR deberá notificar cualquier incidente relacionado con la seguridad de los datos de LA PREVISORA S.A. o de sus clientes y de la plataforma tecnológica.
8. Se debe establecer un ANS para el reporte, atención y solución de incidentes reportados tanto de la plataforma tecnológica como de la información.
9. EL PROVEEDOR debe garantizar la independencia de su información y de sus copias de respaldo de la información de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.
10. Mantener cifrada la información clasificada como confidencial en tránsito o en reposo, usando estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES, RSA o 3DES.
11. De común acuerdo, LA PREVISORA S.A. y EL PROVEEDOR establecerán el control de la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube.
12. EL PROVEEDOR debe monitorear los servicios prestados para detectar operaciones o cambios no deseados e informar a LA PREVISORA S.A. y/o adelantar las acciones preventivas o correctivas cuando se requiera.
13. EL PROVEEDOR debe disponer de redundancias para los servicios ofrecidos.
14. En el evento de toma de posesión de LA PREVISORA S.A. por parte de la Superintendencia Financiera de Colombia - SFC, Fogafin, Fogacoop, o quienes estas designen, estos pueden acceder a la información y a la administración de los sistemas de información que operan en la nube.
15. EL PROVEEDOR puede subcontratar parte del servicio o realizar cambios a los acuerdos establecidos con sus subcontratistas. En todos los casos, los subcontratistas deben cumplir con las obligaciones, requerimientos y certificaciones establecidas en este documento.
16. Las jurisdicciones en donde se procesará la información deben contar con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
17. EL PROVEEDOR debe implementar y suministrar técnicas de múltiple factor de autenticación para el acceso a las consolas de administración de LA PREVISORA S.A.
18. La Superintendencia Financiera de Colombia - SFC o quien esta designe estará facultada para: acceder a la información o datos que se procesan en la nube para el debido ejercicio de sus funciones de supervisión y vigilancia, verificar el cumplimiento de las exigencias regulatorias, acceder a los datos e información y a la administración de los sistemas en los eventos de toma de posesión (prerrogativa que también debe incluir a Fogafin, Fogacoop, o a quienes estas designen).
19. EL PROVEEDOR debe suministrar la siguiente información:
* La documentación completa de los procesos y procedimientos que se ejecutan en la nube.
* La documentación de las aplicaciones que operan en la nube.
* La documentación de los flujos de datos de los procesos misionales o de gestión contable y financiera que alimentan o consumen las aplicaciones dispuestas por el proveedor de servicios en la nube, cuando aplique.
* Los diagramas de red que permitan identificar la plataforma que soporta el servicio contratado.
* Los procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con EL PROVEEDOR de servicios en la nube
* Los reportes generales de auditoría, pruebas de vulnerabilidades y estado actual de los servicios contratados.
1. **Controles de ciberseguridad**

Los proveedores de administración de sistemas y de software, así como aquellos en los que se tercericen los procesos de la Compañía (o parte de ellos) deberán cumplir al menos con lo siguiente:

1. Mantener el inventario de activos (hardware y software), así como de los controles de seguridad de la información y ciberseguridad establecidos para la prestación del servicio
2. Permitir realizar análisis de vulnerabilidades de la infraestructura y aplicaciones, el proveedor deberá realizar planes de remediación para los hallazgos (altos, medios y bajos).
3. Aplicación de líneas base definidas para hardware (servidores, equipos de usuario final, equipos de comunicación) y software que se usen para la prestación del servicio de LA PREVISORA S.A. y emitir informe de cumplimiento mínimo una vez al año.
4. Se deben generar rastros de auditoría para los sistemas de información involucrados en la prestación del servicio, con el propósito de generar evidencia digital.
5. Se debe implementar protección para el navegador web y el correo electrónico.
6. Se debe implementar un sistema de protección antimalware (debidamente licenciado) en los equipos que se usen para la prestación del servicio.
7. Generar copias de seguridad de los datos de LA PREVISORA S.A. y realizar pruebas de restauración de estas.
8. Implementar equipos de protección del perímetro del proveedor tales como Firewall y cuando se preste el servicio web se proteja como mínimo con WAF (Firewall de aplicaciones Web).
9. La información que se encuentre en tránsito o en reposo debe estar cifrada con mecanismos de cifrado fuerte.
10. Aplicar el principio de mínimo privilegio para la operación del servicio.
11. Capacitar y sensibilizar a sus funcionarios involucrados con los servicios a prestar a LA PREVISORA S.A., en temas de seguridad de la información y ciberseguridad.
12. Implementar el proceso de desarrollo seguro de software de acuerdo con las políticas de LA PREVISORA S.A. así como las mejores prácticas.
13. Documentar e implementar un proceso de gestión de incidentes de seguridad de la información y ciberseguridad.
14. **Requisitos para sistemas de información**
15. Garantizar que los requisitos de seguridad de la información se tuvieron en cuenta antes, durante y después de la puesta en producción del sistema de información.
16. El sistema de información debe surtir el proceso de pruebas de Ethical Hacking en la fase de pruebas y producción.
17. El sistema de información debe cumplir con los requisitos de OWASP (para aplicaciones Web)
18. El sistema de información debe generar trazabilidad de los eventos que se generen ya sea a nivel de aplicación o por los usuarios de la aplicación.
19. Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.
20. Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
21. Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este aplicativo. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del aplicativo, deberá realizarse una prueba adicional; el supervisor del contrato validará el cumplimiento de este requisito cuando lo considere necesario.
22. Promover y poner a disposición mecanismos que reduzcan la posibilidad de que la información de LA PREVISORA S.A. y sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
23. Configurar 5 minutos como tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
24. Informar al usuario, al inicio de cada sesión, la fecha y hora del último ingreso a este aplicativo.
25. Implementar mecanismos que permitan a LA PREVISORA S.A. verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.
26. Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás. Las buenas prácticas indican que deben mantener los mismos esquemas de seguridad en pruebas y producción, con el fin de identificar fallos y vulnerabilidades.
27. Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.
28. Cuando se necesite tomar copias de la información de los usuarios para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.
29. Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.
30. Contar con interfaz para los usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.

Atentamente,

**Firma** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Nombre del representante legal:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**C.C. N°** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **de** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Nombre o razón social de EL OFERENTE:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NIT:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Dirección comercial de EL OFERENTE:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Teléfonos:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Fax:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ciudad:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Correo electrónico:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_