ACÁPITE POLÍTICA DE SEGURIDAD DE Y CIBERSEGURIDAD DE LA INFORMACIÓN

Por medio de la presente, informamos que FIDUAGRARIA S.A. es una sociedad anónima sometida a control y vigilancia por la Superintendencia Financiera de Colombia, legalmente constituida mediante escritura pública número 1199 con domicilio principal en la ciudad de Bogotá D.C.

De igual forma FIDUAGRARIA S.A. cuenta con una Política de Seguridad de y Ciberseguridad de la Información Aprobada en acta de Junta Directiva número 375 del 25 de noviembre de 2020, en la cual se dictan los lineamientos pertinentes aplicables para todos los proveedores y terceros que tienen acceso a la información de la entidad descrita a continuación:

5.10 RELACIÓN CON LOS PROVEEDORES

5.10.1 Objetivo:

Preservar los niveles de seguridad y Ciberseguridad de la información a la cual tienen acceso los proveedores y terceros.

5.10.2 Alcance:

Aplica para todos los proveedores y terceros que tienen acceso a la información de la entidad.

5.10.3 Descripción:

Seguridad y ciberseguridad de la información en las relaciones con los proveedores

- *La Fiduciaria tiene identificado y bajo mecanismos de control de acceso a los distintos proveedores que por la naturaleza de la prestación de sus servicios requieren acceso a las instalaciones.*
- *La Fiduciaria tiene establecido mecanismos de control en sus relaciones con proveedores y terceros, con el objetivo de asegurar que los servicios provistos, cumplan con las políticas, normas y procedimientos de seguridad de la información y Ciberseguridad.*
- *Los funcionarios responsables de la supervisión de contratos o convenios con proveedores y terceros, deben divulgar las políticas, normas y procedimientos sobre seguridad de la información de la Fiduciaria a dichas partes. Así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los proveedores y terceros se realice de manera segura.*
- *Los líderes de proceso responsables de activos de información o supervisores de contrato no deben brindar acceso de la información de la Fiduciaria o de los activos de información, a los proveedores o terceros hasta no tener firmados y formalizados, mediante un contrato o acuerdo, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad.*
- *Todos los proveedores y terceros que vayan a tener acceso a información confidencial de la Fiduciaria, contratados directamente o mediante Unidades de Gestión, deben diligenciar el*

formato evaluación de seguridad para proveedores, con el fin de dar cumplimiento a lo establecido en la circular externa 042 de 2012 y 007 de 2018 de la SFC.

- *Todo proveedor y terceros contratados directamente o mediante Unidades de Gestión, que provea servicios de computación en la nube debe dar cumplimiento a lo establecido en la circular externa 005 de 2019 de la SFC.*

Gestión de la prestación de servicios de proveedores

- *Los proveedores que desarrollen software, o presten servicios a la entidad, deben:*

  - ✓ *Cumplir con los requerimientos de seguridad y los controles deseados.*
  - ✓ *Asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.*
  - ✓ *Establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.*
  - ✓ *Usar los protocolos de seguridad definidos por la Gerencia Integral de Riesgos y Oficina de Cumplimiento – Sistema SGSI y Ciberseguridad.*
  - ✓ *Considerar y aplicar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos.*
  - ✓ *Garantizar las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.*
  - ✓ *Garantizar que no se divulgue información sensible en respuestas de error y adicionalmente prevenir la revelación de la estructura de directorios de los sistemas de información construidos.*
  - ✓ *Desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.*
  - ✓ *Cumplir con los requisitos establecidos contractualmente.*
  - ✓ *Realizar pruebas de seguridad al Software desarrollado antes de su paso a producción.*

Cualquier duda con gusto será atendida.

RAÚL FERNANDO RODRÍGUEZ LONDOÑO

GERENTE I INTEGRAL DE RIESGO Y OFICIAL DE CUMPLIMIENTO