ACÁPITE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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 No. 1199, del 18 de febrero de 1992 ante la Notaría Veintinueve (29) del Círculo de Bogotá D.C., con domicilio principal en la ciudad de Bogotá D.C.

De igual forma FIDUAGRARIA S.A. cuenta con una Política de Seguridad de la Información y Política de Ciberseguridad aprobadas en acta de Junta Directiva número 444 del 16 de diciembre de 2025, en las cuales 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. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.10 RELACIÓN CON LOS PROVEEDORES

5.10.1 Objetivo

Preservar los niveles de seguridad de la información y ciberseguridad 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 Fiduciaria.

5.10.3 Descripción

Seguridad de la Información y Ciberseguridad 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 establecidos 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 esta, 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 a 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 básica jurídica 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.*
- *Todo proveedor o terceros críticos contratados directamente o mediante Unidades de Gestión y consorcios, deben diligenciar el formato evaluación seguridad de la información y ciberseguridad para proveedores críticos en cumplimiento a lo establecido en la circular externa 007 de 2018, circular externa 005 de 2019 y circular externa 025 de 2020 de la SFC.*

Gestión de la prestación de servicios de proveedores

- *Los proveedores que desarrollen software, o presten servicios a la Fiduciaria, deben:*
  - ✓ *Cumplir con los requerimientos de seguridad y 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 – Gestión de Seguridad de la Información, Ciberseguridad y Continuidad del Negocio.*
  - ✓ *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 salida de manera confiable, utilizado 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 y asegurar que dichos archivos solo tengan privilegios de lectura.*
  - ✓ *Cumplir con los requisitos establecidos contractualmente.*
  - ✓ *La Fiduciaria promoverá la validación de seguridad de las soluciones tecnológicas suministradas por proveedores, previo a su entrada en operación, como parte de su enfoque preventivo de gestión de riesgos de ciberseguridad.*
  - ✓ *La Fiduciaria promoverá la validación de seguridad de las soluciones tecnológicas y sistemas de información suministrados, desarrollados o implementados por proveedores, previo a su entrada en operación, como parte de su enfoque preventivo de gestión de riesgos de ciberseguridad.*

6. POLÍTICA GENERAL DE CIBERSEGURIDAD

6.2 LINEAMIENTOS ESTRATÉGICOS DE CIBERSEGURIDAD

Seguridad en la relación con terceros y proveedores críticos

- *Evaluación de riesgos, controles y capacidades de ciberseguridad de proveedores que accedan a información de la Fiduciaria.*
- *Adopción de lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC para contratación, seguimiento y terminación del vínculo.*
- *Exigir desarrollo seguro y cumplimiento de estándares como OWASP, ISO27032 y NIST.*

6.4 ROLES Y RESPONSABILIDADES

Proveedores y Terceros Críticos

- *Cumplir con los requisitos técnicos y contractuales de ciberseguridad definidos por Fiduagraria.*
- *Garantizar controles adecuados de protección, acceso y desarrollo seguro.*
- *Notificar incidentes que comprometan los servicios o información confiada.*
- *Permitir auditorías o revisiones cuando aplique.*

6.6 SEGURIDAD EN LA NUBE (CLOUD SECURITY)

Lineamientos de Seguridad en la Nube

1. ***Gobernanza y responsabilidad compartida***

Todo servicio en la nube deberá contar con un modelo de responsabilidad compartida claramente documentado, que especifique las obligaciones de Fiduagraria S.A. y del proveedor cloud en materia de seguridad y ciberseguridad.

2. ***Evaluación de riesgos y selección de proveedores Cloud***

- *Previo a la adopción de un servicio en la nube se realizará una evaluación de riesgos cibernéticos, considerando criticidad del proceso, clasificación de la información, residencia de datos, dependencia tecnológica y requerimientos de continuidad.*
- *Solo se contratarán proveedores que demuestren controles de seguridad alineados con estándares reconocidos (p.ej. ISO/IEC 27001, SOC 2 u otros equivalentes).*

3. ***Requisitos contractuales y cumplimiento regulatorio***

- *Los contratos deberán incluir cláusulas específicas de seguridad de la información y ciberseguridad contemplando como mínimo:*
  - *Protección de datos personales y sensibles,*
  - *Medidas técnicas y organizativas de seguridad,*
  - *Notificación y gestión de incidentes de ciberseguridad,*
  - *Niveles de servicio (ANS) y tiempos de atención,*
  - *Condiciones de auditoría, acceso a reportes y certificaciones,*
  - *Condiciones de terminación, portabilidad y borrado seguro de la información.*
- *La contratación de servicios en la nube deberá cumplir con la regulación de la Superintendencia Financiera de Colombia y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC.*

6.7 EVALUACIÓN DE RIESGOS CIBERNÉTICOS

Responsables

Terceros críticos: deben entregar análisis de riesgos de los servicios contratados.

6.9 GESTIÓN DE VULNERABILIDADES

Responsables

Terceros críticos: deberán aplicar controles de seguridad y entregar evidencias de remediación cuando su infraestructura soporte servicios de la Fiduciaria, conforme al Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC y la CE 007 de 2018 de la SFC.

Cualquier duda con gusto será atendida.

LORENA RODRÍGUEZ LÓPEZ

GERENTE INTEGRAL DE RIESGOS