1. OBJETIVO

Asegurar el uso adecuado y efectivo de la criptografía y firma electrónica o digital para proteger la confidencialidad, autenticidad e integridad de la información confidencial o sensible de la institución al momento de almacenarse o transmitirse, aumentando la privacidad y seguridad de esta.

2. ALCANCE

Esta política se aplica al uso y la configuración del cifrado aplicado a los sistemas de tecnología, dispositivos informáticos, tecnologías de comunicación y servicios de GRUPO MOK COLOMBIA S.A.S, incluidos todos los empleados, miembros electos, contratistas, voluntarios, proveedores, aprendices, colocaciones de experiencia laboral/estudiantes y agencias asociadas que tienen acceso a estos sistemas, equipos y dispositivos.

3. MARCO NORMATIVO Y JURISPRUDENCIAL DE LA CONSTITUCIÓN PÓLITICA

- Constitución Política de Colombia, artículo 15.
- Ley 527 de 1999, en la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley estatutaria 1564 de 2012, artículo 244
- Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 19 de 2012, en el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Ley 1928 de 2018, artículo 25.
- Decreto 333 de 2014, el presente decreto tiene por objeto definir el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en el artículo 160 del Decreto19 de 2012.

- Decreto 1413 de 2017, por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- ISO/IEC 27001:2013, por la cual estipula los requisitos de Seguridad de la Información.
- Sentencia C-420 de 2020.

4. OBLIGATORIEDAD

Esta política es de obligatorio y estricto cumplimiento por parte de los directivos, colaboradores, asociados, agentes, consultores, proveedores y/o contratistas, que debido a su gestión o funciones deban tener acceso a información confidencial y sensible, teniendo en cuenta los lineamientos de criptografía y firma electrónica aplicables para los equipos de red, conexiones remotas, contraseñas de usuario o claves, entre otros.

5. TÉRMINOS Y DEFINICIONES

Algoritmo: Conjunto de instrucciones o reglas definidas y no-ambiguas, ordenadas y finitas que permite, típicamente, solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo otras tareas o actividades.

Autorización o Control de Acceso: Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.

Criptografía: Ámbito que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Cifrado: Procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

Cifrado simétrico: Indica que para el cifrado y descifrado se utiliza la misma clave, que debe intercambiarse de forma segura entre el emisor y el receptor.

Cifrado asimétrico: Se utilizan dos claves que están enlazadas matemáticamente entre sí y forman un par de claves. La clave pública se puede compartir con cualquier persona, pero la clave privada debe permanecer confidencial. Sólo una de las dos claves se utiliza para el descifrado, la otra es responsable del cifrado. El código privado descifra el texto secreto y lo transmite a un texto legible. El código público se utiliza para cifrar y ocultar el contenido.

Clave (de cifrado): Pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

Bit: Es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información

Hash: Es una primitiva criptográfica que produce una representación condensada de su entrada (por ejemplo, un mensaje u otros datos). Los nombres comunes para la salida de una función hash incluyen valor hash, hash, resumen de mensaje y huella digital.

FIPS: Federal Información Processing Estándares (FIPS; en español, Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno.

Firma electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Firmante: Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Mensaje de datos: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

6. DECLARACIÓN DE POLÍTICA

El cifrado funciona convirtiendo datos para que sean ilegibles e inaccesibles para personas no autorizadas. La única forma de leer los datos cifrados es utilizando una clave de descifrado. GRUPO MOK COLOMBIA S.A.S utiliza el cifrado para:

- Asegurar información y datos mientras se almacenan, procesan y manejan.
- Proteger las credenciales de usuario (contraseñas/inicios de sesión).
- Permitir comunicaciones y conexiones seguras.
- Habilitar la verificación, autenticación, identificación y validación.
- Asegurar conexiones en red/internet ad-hoc entre sistemas y dispositivos TIC.

7. LINEAMIENTOS DE CRIPTOGRAFÍA

- GRUPO MOK COLOMBIA S.A.S aplica cifrado para acceso privilegiado a equipos de red o servidores para fines de administración del sistema; es decir, SSH.
- GRUPO MOK COLOMBIA S.A.S utiliza controles criptográficos para la transmisión de información clasificada o reservada, fuera del ámbito de la compañía.

- GRUPO MOK COLOMBIA S.A.S requiere de cifrado para la conexión remota a sus sistemas a través de VPN.
- GRUPO MOK COLOMBIA S.A.S utiliza solo algoritmos que hayan sido publicados y analizados por investigadores y/o aprobadas por estándares u organizaciones internacionales confiables, FISPS, IEEE, ANSI, por ejemplo:
    - Todas las funciones hash aprobadas son funciones hash criptográficas y se definen en FIPS 180, FIPS 202 y SP 800-185.
    - Se han aprobado dos clases de algoritmos de clave simétrica: los que se basan en algoritmos de cifrado de bloques (p. ej., AES, como se especifica en FIPS 197) y los que se basan en el uso de funciones hash (p. ej., un código de autenticación de mensaje con clave hash, como se especifica en FIPS 198).
    - Se permite uso de algoritmos de llave asimétrica o también conocidos como de llave púbica. Aunque las claves pública y privada de un par de claves están relacionadas, el conocimiento de la clave pública no se puede utilizar para determinar la clave privada, se permite emplear RSA, ELGAMAL, Curvas elípticas, entre otros.
    - Demás algoritmos aprobados a través de FIPS 140.
    - Demás algoritmos de cifrado que, aunque no se encuentren aprobados en FIPS, tengan una base de, como mínimo, cifrado de 128 bits.
- GRUPO MOK COLOMBIA S.A.S no permite el uso de algoritmos propios algoritmos o rudimentarios.
- Las claves de algoritmos simétricos y las claves privadas son como contraseñas, por lo que GRUPO MOK COLOMBIA S.A.S vela porque estas claves no se reutilicen.
- GRUPO MOK COLOMBIA S.A.S puede usar un programa de computadora para generar claves, siempre que este programa haya sido diseñado para generar claves difíciles de predecir. Por ejemplo, el lenguaje de programación Java tiene un potente generador de números aleatorios que se puede usar para generar

claves, pero también tiene una función aleatoria más rápida pero insegura que no se debe usar.

- La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información no podrá ser almacenada en texto plano y deberá hacer uso de mecanismos criptográficos. GRUPO MOK COLOMBIA S.A.S establece el no almacenamiento o visibilidad de contraseñas, pero sí permite la visibilidad del hash de cifrado de las contraseñas.
- GRUPO MOK COLOMBIA S.A.S permite y recomienda el uso de los siguientes productos de cifrado, mas no se limita únicamente a:
    - Cifrado de disco de arranque: BitLocker, Symantec Endpoint Encryption, PGP Desktop, Veracrypt (sucesor de TrueCrypt), Veracrypt, Symantec.
    - Cifrado de archivos: 7-Zip, Cryptainer LE, Imágenes de disco, EFS, FileVault, PGP Desktop, TrueCrypt, WinZip, WinSCP, WinZip
    - Correo electrónico: escritorio openPGP o PGP.
    - Herramientas nativas de Windows, Linux y de herramientas de lenguajes de programación que produzcan claves lo suficientemente fuertes.
- El cifrado empleado en computadoras de escritorio y portátiles debe permitir que se genere una clave criptográfica
- Todas las computadoras de escritorio y portátiles deben actualizarse con los últimos parches de seguridad y sistema operativo, cuando se considere oportuno, ya que estas actualizaciones pueden incluir parches de seguridad para fallas o vulnerabilidades descubiertas en el software de encriptación.
- Los dispositivos como computadoras portátiles y teléfonos móviles proporcionados por la compañía deben estar protegidos con una contraseña, PIN y/o desbloqueo por biométrico. El cifrado de datos debe estar habilitado cuando esté disponible. Si bien el uso de un PIN solo para asegurar un teléfono móvil no constituye encriptación, juega un papel vital en el soporte de la encriptación de dispositivos móviles

- Las aplicaciones autorizadas por GRUPO MOK COLOMBIA S.A.S deben usar protocolos de comunicación encriptados seguros como HTTPS/TLS1.2 (o superior) cuando se comunican a través de Internet.
- Cuando sea necesario, GRUPO MOK COLOMBIA S.A.S proporciona memorias USB encriptadas. Estos dispositivos de almacenamiento son solo para el almacenamiento temporal de datos. GRUPO MOK COLOMBIA S.A.S permite el uso de memorias USB emitidas por GRUPO MOK COLOMBIA S.A.S (y dispositivos de almacenamiento similares) bajo las siguientes condiciones:
    - Los usuarios deben establecer una contraseña para acceder al dispositivo.
    - La contraseña para dispositivos portátiles encriptados debe estar de acuerdo con la política de contraseñas de GRUPO MOK COLOMBIA S.A.S.
- Los datos de GRUPO MOK COLOMBIA S.A.S almacenados en memorias USB encriptadas (o dispositivos de almacenamiento similares) deben transferirse a un área segura y apropiada en la red informática de GRUPO MOK COLOMBIA S.A.S después de la finalización de la necesidad de uso. Los datos de la compañía no deben permanecer en la memoria USB después de la finalización de su necesidad de uso.
- En el caso de que no se hayan seguido los procedimientos locales para la creación de contraseñas de encriptación, se les puede pedir a los empleados que proporcionen detalles de las contraseñas de encriptación utilizadas en todos esos dispositivos portátiles; sin embargo, en ninguna circunstancia se deben revelar contraseñas de redes u otros sistemas de TI.

8. GESTIÓN DE CLAVES

- Las claves deben ser almacenadas en repositorio seguro y al cual debe tener acceso únicamente personal autorizado.

- Si se proporciona una clave criptográfica para recuperar el acceso a una computadora, se debe revocar la clave existente y se debe generar una nueva clave para evitar la fuga de datos.
- Las claves criptográficas deben administrarse y protegerse de manera segura a lo largo de todo su ciclo de vida, desde la generación inicial y el almacenamiento hasta el archivo, la recuperación, la distribución, el retiro y la eventual destrucción.
- GRUPO MOK COLOMBIA S.A.S vela porque los algoritmos criptográficos, las longitudes de clave y el uso estén de acuerdo con todas las políticas y procedimientos pertinentes de la compañía y de acuerdo con las mejores prácticas profesionales.
- En caso de que se comprometa una clave criptográfica, se debe revocar la clave existente y se debe generar una nueva clave (o par de claves).
- Las claves criptográficas de algoritmos simétricos y asimétricos de GRUPO MOK COLOMBIA S.A.S deben tener una periodicidad o duración de máximo 18 meses. Las claves públicas normalmente no son confidenciales y se pueden cambiar con menos frecuencia.
- GRUPO MOK COLOMBIA S.A.S no permite almacenar claves en un lugar público, o colocar claves en el código fuente al que pueden acceder todos los desarrolladores.

9. LINEAMIENTOS DE FIRMA ELECTRONICA O DIGITAL

- GRUPO MOK COLOMBIA S.A.S establece como medio de identificación electrónico flexible la firma electrónica o digital para los colaboradores debidamente autorizados, así como los proveedores y contratistas (firmantes) que tengan relación contractual con la compañía, teniendo en cuenta que esta permite el uso de firmas electrónicas y digitales, para lo cual el proveedor de este servicio debe estar aprobado y/o acreditado por la ONAC y SIC o por una entidad competente en la materia.

- El certificado de firma electrónica o digital otorgado por el Organismo Nacional de Acreditación de Colombia- ONAC, permite dar fe de un acto o voluntad por parte de los firmantes, de conformidad con el artículo 28 de la Ley 527 de 1999. Del mismo modo, esta certificación cumple una función notarial para que el documento ostente su validez correspondiente.
- GRUPO MOK COLOMBIA S.AS. no excluye la neutralidad tecnológica para el aval de la firma electrónica de los firmantes conforme a la normatividad aplicable a la materia.
- GRUPO MOK COLOMBIA S.A.S considera que los datos utilizados para la creación de las firmas electrónicas y digitales son veraces, confiables y corresponden exclusivamente al firmante, por lo cual el Área de seguridad de la información y alta dirección serán los encargados de autorizar y validar el uso de la firma electrónica de los colaboradores que lo soliciten y justifiquen su petición.
- En el caso de detectar alteraciones no autorizadas en los mensajes de datos que contengan firmas electrónicas, los firmantes se comunicarán mediante correo electrónico al Área de Riesgos para levantar el incidente de seguridad, frente a esto GRUPO MOK COLOMBIA S.A.S emitirá instrucciones y medidas de seguridad, con el fin de salvaguardar los derechos de habeas data e intimidad de los firmantes.
- Los métodos utilizados como firma electrónica o digital en GRUPO MOK COLOMBIA S.A.S son seguros, y tendrá en cuenta los siguientes factores:
    - El uso de la firma electrónica quedará inválido, si la información o mensaje de datos son cambiados por el firmante.
    - La información que contenga la firma electrónica o digital será accesible para su posterior consulta de los colaboradores, contratistas y demás sujetos del GRUPO MOK COLOMBIA S.A.S.

- GRUPO MOK COLOMBIA S.A.S., solicitará concepto técnico emitido por un perito o un órgano independiente y especializado, con el fin de verificar la autenticidad y no repudio de las firmas electrónicas o digitales.

10. CONTROL DE CAMBIOS

VERSIÓN No.	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA
1	Primera elaboración del documento **Nota**: Se elaboró bajo el código **GI-PLT-012**	Analista de soporte	14/11/2017
2	Actualización general del documento **Nota**: Se dio la actualización del documento bajo el código **GI-PLT-012**	Analista de seguridad de la información	20/05/2021
3	Actualización controles criptográficos **Nota**: Se dio la actualización del documento bajo el código **GI-PLT-012**	Analista de seguridad de la información	20/08/2021
4	Revisión y actualización de lineamientos y gestión de claves criptográficas. Adición del marco normativo y lineamientos de firma electrónica o digital. La política cambia de código a **CO-SI-PLT-015**	Oficial de Seguridad de la Información y Oficial Protección de Datos Personales	14/10/2022

11. REGISTRO DE COLABORADORES

Elaboró:	Revisó:	Aprobó:
Nombre: Alejandro Erazo Bolaños y Sharon Morales Cepeda	**Nombre:** John Ochoa	**Nombre:** Miguel Omar Ríos Cabra
Cargo: Oficial de Seguridad de la Información Oficial de Protección de Datos	**Cargo:** Directos de Riesgos y Seguridad Global	**Cargo:** Gerente de Cumplimiento y Seguridad Global