



Bogotá, 31 de julio de 2026
Concepto Jurídico N.º 015-OFJU-DG-2026

Ingeniero:

HENRY CORTÉS CONTRERAS

Oficial de Seguridad de la Información del INMLCF

Dirección General

Correo henry.cortes@medicinallegal.gov.co

Instituto Nacional de Medicina Legal y Ciencias Forenses

Bogotá D.C.

Asunto: Consulta sobre doble autenticación (MFA) con el fin de verificar la identidad de los usuarios y permitir el acceso al servicio de correo institucional.

De acuerdo con las funciones otorgadas a la Oficina Asesora Jurídica en el artículo 8 numeral 3 del Acuerdo 067 del 23 de septiembre 2025, le corresponde “Dar respuesta a las tutelas, acciones de cumplimiento y demás actuaciones jurídicas y/o administrativas de la entidad y emitir conceptos jurídicos”. Por lo anterior, me permito responder en los siguientes términos:

I. CONSULTA

A través de mensaje de datos por correo electrónico del 27 de mayo de 2026, el ingeniero Henry **Cortés Contreras**, como Oficial de Seguridad de la Información del INMLCF solicitó:

Se emita concepto jurídico sobre:

*<< (...) En mi calidad de **Oficial de Seguridad de la Información del INMLCF**, y teniendo en cuenta que dentro de mis funciones se encuentra la **protección de los datos personales**, respetuosamente solicito su concepto frente al siguiente escenario:*

*La entidad tiene previsto implementar un mecanismo de **doble autenticación (MFA)** con el fin de **verificar la identidad de los usuarios y permitir el acceso al servicio de correo institucional**.*

En este contexto, surge la siguiente inquietud:

*¿Es necesario solicitar autorización al titular de los datos cuando el proceso de autenticación se realiza a través del **teléfono celular personal del servidor público**?*

Adicionalmente, ¿cuál debería ser el procedimiento adecuado para su implementación, garantizando el cumplimiento de la normatividad de protección de datos personales?

II. PROBLEMAS JURÍDICOS

1. ¿Es necesario solicitar autorización al titular de los datos personales cuando la autenticación multifactor (MFA) se realiza mediante el uso del teléfono celular personal del servidor público?
2. ¿Cuál es el procedimiento adecuado para su implementación, garantizando el cumplimiento del régimen de protección de datos personales?

III. CONSIDERACIONES

3.1. Antecedentes

La autenticación multifactor (MFA) es un mecanismo de seguridad que exige dos o más factores de verificación para acceder a sistemas, reduciendo el riesgo de accesos no autorizados.

Su implementación responde al deber legal de proteger los datos personales conforme a la Ley 1581 de 2012 y al derecho fundamental al habeas data, así como a las obligaciones derivadas del Decreto 1078 de 2015 y la política de Gobierno Digital.

En consecuencia, la MFA constituye una medida técnica idónea y jurídicamente exigible para garantizar la confidencialidad, integridad y disponibilidad de la información en las entidades públicas.

3.2 Marco Jurídico

Normatividad que regula la doble autenticación

- Constitución Política de Colombia, artículo 15 (derecho a la intimidad y protección de datos - habeas data).
- Ley 1581 de 2012 – Régimen general de Protección de datos personales.
- Decreto 1377 de 2013 – reglamentación parcial de la ley
- Decreto 338 de 2022 – Lineamientos de Seguridad Digital en el Estado.
- (MSPI), Min TIC Modelo de Seguridad y Privacidad de la Información.
- ISO/IEC 27001:2022 (estándar de referencia adoptado por el MSPI).

IV. ANÁLISIS JURÍDICO

4.1. ¿Sobre la necesidad de autorización del titular de los datos personales cuando la autenticación multifactor (MFA) se realiza mediante el uso del teléfono celular personal del servidor público?

La Ley 1581 de 2012 establece como regla general que el tratamiento de datos personales requiere la autorización previa, expresa e informada del titular, salvo las excepciones previstas en la ley. En este sentido cuando una entidad pública implementa MFA mediante el celular personal del servidor, normalmente trata datos como el número de teléfono móvil, Identificadores del dispositivo, registros de autenticación, direcciones IP y metadatos asociados al acceso; todos estos constituyen datos personales o información susceptible de asociarse a una persona identificada o identificable.

En atención al problema jurídico planteado, se concluye que la implementación de mecanismos de autenticación multifactor (MFA) mediante el uso del teléfono celular personal del servidor público, debe contar con su anuencia como medio de autenticación. Es importante precisar que, tratándose del uso de dispositivos pertenecientes a la esfera personal del servidor público, resulta jurídicamente necesario que el servidor voluntariamente otorgue su aceptación, a fin de garantizar los principios de libertad, transparencia y proporcionalidad en el tratamiento de datos personales, así como de mitigar riesgos jurídicos para la entidad.

En consecuencia, en caso de que el servidor no desee habilitar su dispositivo celular personal como medio de verificación, la entidad debe asegurar medidas complementarias o alternativas tecnológicas que aseguren la adecuada información al titular, la minimización del dato y la posibilidad de ofrecer alternativas de autenticación, en concordancia con el régimen de protección de datos personales y el modelo de seguridad de la información aplicable.

4.2 ¿Cuál es el procedimiento adecuado para su implementación, garantizando el cumplimiento del régimen de protección de datos personales?

Para garantizar la implementación adecuada de la autenticación multifactor (MFA), se considera procedente adoptar las siguientes medidas:

1. **Definición de la finalidad.** Establecer de manera expresa que la MFA tiene como finalidad el control de acceso a los sistemas de información, en cumplimiento de obligaciones de seguridad digital y protección de la información institucional.
2. **Principio de transparencia.** Informar al servidor público, de manera previa y suficiente, sobre: el dato que se utilizará (por ejemplo, número de celular), la finalidad del tratamiento, la forma de uso (OTP, aplicaciones, entre otros) y si el dato será almacenado o utilizado temporalmente.
3. **Obtención de consentimiento (cuando aplique).** Si se utilizan dispositivos personales, debe ser claro que el servidor autoriza su número personal y su dispositivo voluntariamente o dejar constancia de su conocimiento y aceptación del tratamiento.
4. **Ofrecimiento de alternativas.** Garantizar mecanismos alternativos de autenticación (tokens, dispositivos institucionales, correo electrónicos alternativos u otros), con el fin de evitar la imposición del uso de dispositivos personales y asegurar el principio de proporcionalidad.
5. **Principio de minimización de datos.** Limitar el uso del dato personal estrictamente a la finalidad de autenticación, evitando su reutilización o almacenamiento innecesario.

6. **Documentación y formalización.** Incorporar el tratamiento en los instrumentos institucionales correspondientes, tales como la política de tratamiento de datos personales, la política de seguridad de la información y los procedimientos de control de acceso.
7. **Gestión del riesgo.** Integrar la MFA dentro del análisis de riesgos del sistema de gestión de seguridad de la información, definiendo controles y planes de tratamiento adecuados.

En todo caso, el servidor público, en aplicación de los principios de responsabilidad, colaboración, moralidad, imparcialidad y buena fe, debe estar presto a colaborar con la administración en el sentido de facilitar la gestión de la autenticación de datos en el marco de la implementación de la seguridad de las tecnologías de la información, en el marco de las alternativas que pueda generar la Entidad estatal, en este sentido si no pretende hacerlo con su dispositivo móvil de uso personal, si se encuentra en el deber de permitir los acceso por canales diferentes, tales como el correo electrónico adicional u otros medios de validación que permita la verificación correspondiente.

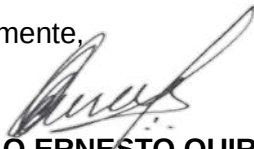
Conclusión:

La implementación de la autenticación multifactor (MFA) en la entidad es jurídicamente viable y se ajusta al régimen de protección de datos personales, siempre que su adopción se realice bajo criterios de finalidad legítima, transparencia, proporcionalidad y seguridad.

Cuando la autenticación involucre el uso de dispositivos personales del servidor público, resulta relevante obtener su aceptación y en todo caso se recomienda garantizar alternativas tecnológicas de validación, con el fin de mitigar riesgos jurídicos y asegurar el cumplimiento integral de los principios que rigen el tratamiento de datos personales.

Este concepto se rinde en los términos del artículo 28 de la Ley 1437 de 2011, por lo que no es de obligatorio cumplimiento ni ejecución.

Atentamente,


CAMILO ERNESTO QUIROGA MORA
 Jefe Oficina Jurídica

	Nombre, apellido y cargo	Firma	Fecha
Proyectó	Scherezada Cardona – Profesional Especializado - Oficina Jurídica		2026-07-31
Revisó y Aprobó	Camilo Ernesto Quiroga Mora– Jefe oficina Jurídica		31-07-2026