RESOLUCIÓN RECTORAL
No. 05 de 2026

Por la cual se expide el Protocolo para el manejo de correos electrónicos

La rectora de la Fundación Universitaria CAFAM – UNICAFAM, en ejercicio de sus funciones, conforme a lo establecido por los estatutos de la institución, y

CONSIDERANDO

Que la Fundación Universitaria Cafam – UNICAFAM, en desarrollo de su naturaleza jurídica, de su autonomía universitaria y de los principios que orientan su gestión institucional, debe establecer mecanismos que promuevan la eficiente administración de los recursos tecnológicos y de los sistemas de información utilizados para el cumplimiento de sus funciones misionales y de apoyo.

Que los Estatutos de la Fundación Universitaria Cafam – UNICAFAM establecen los principios, la estructura organizacional, las competencias de sus órganos de gobierno y las directrices generales para el adecuado funcionamiento institucional, facultando a las autoridades universitarias para expedir las políticas, procedimientos y lineamientos necesarios para garantizar el desarrollo ordenado de las actividades académicas y administrativas.

Que la información que circula a través de los canales electrónicos institucionales constituye un activo estratégico para la Institución, cuyo adecuado tratamiento resulta esencial para garantizar la continuidad de las operaciones, la toma de decisiones, la protección de los intereses institucionales y el cumplimiento de los fines misionales de UNICAFAM.

Que mediante la Política de Tratamiento y Protección de Datos Personales de la Fundación Universitaria Cafam – UNICAFAM, la Institución estableció los principios, deberes y responsabilidades relacionados con la recolección, almacenamiento, uso, circulación, transmisión y protección de los datos personales, imponiendo a todos los miembros de la comunidad universitaria la obligación de garantizar la confidencialidad, integridad y adecuada gestión de la información a la que tengan acceso en ejercicio de sus funciones o actividades.

Que la Política General de Seguridad de la Información de UNICAFAM reconoce la necesidad de implementar medidas administrativas, organizacionales y tecnológicas orientadas a preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, así como a promover el uso seguro y responsable de los recursos tecnológicos puestos a disposición de la comunidad universitaria.

Que el correo electrónico institucional constituye un medio oficial de comunicación de la Fundación Universitaria Cafam – UNICAFAM, a través del cual se desarrollan actividades académicas, administrativas, financieras, jurídicas, comerciales y de relacionamiento con los diferentes grupos de interés, razón por la cual su utilización debe sujetarse a criterios de seguridad, responsabilidad, oportunidad, eficiencia y observancia de la normativa institucional vigente.

Que el Reglamento Interno de Trabajo establece deberes relacionados con el adecuado uso de los bienes, recursos, herramientas tecnológicas y sistemas de información de la Institución, así como la obligación de proteger la información institucional y observar las políticas, procedimientos y directrices adoptadas por la Universidad para el cumplimiento de sus actividades.

Que la creciente dependencia de los medios digitales de comunicación hace necesario establecer lineamientos institucionales específicos que orienten el envío, recepción, gestión y conservación de las comunicaciones realizadas a través del correo electrónico institucional, con el propósito de fortalecer la seguridad de la información, promover buenas prácticas de comunicación organizacional, reducir riesgos operativos y garantizar la adecuada representación institucional de UNICAFAM ante sus diferentes grupos de interés.

Que las cuentas de correo electrónico institucionales constituyen herramientas de trabajo suministradas por la Fundación Universitaria Cafam – UNICAFAM para el cumplimiento de funciones académicas, administrativas y contractuales, por lo que su utilización debe realizarse de conformidad con las políticas institucionales, los deberes derivados de la relación laboral, académica o contractual y los lineamientos de seguridad de la información adoptados por la Institución.

Que la adopción de un Protocolo para el Envío de Correos Electrónicos Institucionales contribuirá a fortalecer los principios de responsabilidad, transparencia, eficiencia administrativa, protección de datos personales, seguridad de la información y uso adecuado de los recursos tecnológicos institucionales.

Que, en mérito de lo expuesto, En mérito de lo expuesto,

RESUELVE

Artículo único. Adoptar el **Protocolo para el Envío de Correos Electrónicos Institucionales de la Fundación Universitaria Cafam – UNICAFAM**, el cual forma parte integral de la presente resolución.

La presente resolución rige a partir de la fecha de su expedición y deroga las disposiciones internas que le sean contrarias.

Bogotá D.C., diez (10) de julio de 2026.

DIANA MARGARITA PÉREZ CAMACHO
Rectora

PROTOCOLO PARA EL ENVÍO DE CORREOS ELECTRÓNICOS INSTITUCIONALES

1. Objeto

El presente Protocolo tiene por objeto establecer lineamientos mínimos para el envío adecuado, seguro y responsable de correos electrónicos institucionales en la Fundación Universitaria Cafam – UNICAFAM, con el fin de proteger la información institucional, garantizar el tratamiento adecuado de los datos personales, fortalecer la seguridad de la información y promover buenas prácticas de comunicación organizacional.

2. Alcance

El Protocolo aplica a todas las comunicaciones enviadas o gestionadas mediante cuentas de correo electrónico institucionales, así como a aquellas comunicaciones electrónicas que, en desarrollo de funciones, actividades, obligaciones contractuales o encargos institucionales, involucren información de UNICAFAM, datos personales, información académica, laboral, administrativa, financiera, jurídica, contractual o cualquier otra información sujeta a reserva, confidencialidad o protección especial.

3. Ámbito de aplicación personal

El presente Protocolo es de obligatorio cumplimiento para directivos, trabajadores, profesores, contratistas, practicantes, monitores, estudiantes autorizados para desarrollar actividades institucionales y demás personas que utilicen cuentas de correo electrónico institucionales o que gestionen información de UNICAFAM mediante medios electrónicos suministrados o autorizados por la Institución.

4. Principios aplicables

El envío de correos electrónicos institucionales que involucren datos personales deberá realizarse conforme a los principios establecidos en la Política de Tratamiento y Protección de Datos Personales de UNICAFAM y en la normativa aplicable sobre la materia.

En particular, deberán observarse los siguientes principios:

4.1. Finalidad

Los datos personales solo podrán ser utilizados para finalidades legítimas, previamente informadas y autorizadas por el titular, o para aquellas finalidades permitidas por la normativa aplicable y por la Política de Tratamiento y Protección de Datos Personales de UNICAFAM.

4.2. Libertad

El tratamiento de datos personales requerirá autorización previa, expresa e informada del titular, salvo en los casos exceptuados por la ley o cuando exista una base jurídica que habilite su tratamiento conforme a la normativa vigente.

4.3. Veracidad o calidad

La información enviada mediante correo electrónico institucional deberá ser completa, exacta, actualizada, comprobable y comprensible. Antes del envío, el remitente deberá verificar que la información corresponda al destinatario correcto y que no se incorporen datos erróneos, desactualizados o pertenecientes a terceros no relacionados con la finalidad de la comunicación.

4.4. Transparencia y acceso

El titular de los datos personales tiene derecho a conocer, actualizar y rectificar su información, así como a ejercer los demás derechos previstos en la Política de Tratamiento y Protección de Datos Personales de UNICAFAM y en la normativa aplicable.

4.5. Acceso y circulación restringida

Los datos personales solo podrán circular dentro de los límites autorizados por el titular, por la ley y por las finalidades institucionales debidamente informadas. En consecuencia, el remitente deberá limitar los destinatarios del correo electrónico a las personas que requieran conocer la información para el cumplimiento de una finalidad legítima, académica, administrativa, contractual, laboral, legal o institucional.

4.6. Seguridad

En el envío de correos electrónicos institucionales deberán observarse las medidas técnicas, humanas, administrativas y organizacionales definidas por UNICAFAM para proteger la información frente a pérdida, adulteración, consulta, uso, acceso o divulgación no autorizada o fraudulenta.

4.7. Confidencialidad

Toda persona que tenga acceso a datos personales o información institucional deberá guardar reserva respecto de dicha información y abstenerse de divulgarla, reproducirla, reenviarla o compartirla sin autorización legal, contractual, institucional o del titular, según corresponda.

5. Lineamientos generales para el envío de correos electrónicos institucionales

Toda comunicación electrónica institucional deberá ser preparada, revisada y enviada de manera responsable, cuidadosa y coherente con la finalidad de la comunicación, el tipo de información involucrada y los destinatarios autorizados.

Cuando el correo electrónico contenga datos personales, información sensible, reservada, confidencial o de especial protección, el remitente deberá extremar las medidas de verificación, seguridad y control de destinatarios, evitando la exposición innecesaria de información.

6. Preparación del correo electrónico

Antes de redactar y enviar un correo electrónico institucional, el remitente deberá observar los siguientes criterios:

6.1. Identificación de la finalidad

El remitente deberá verificar que el correo responda a una finalidad legítima, necesaria y relacionada con el cumplimiento de funciones, actividades u obligaciones académicas, administrativas, laborales, contractuales, jurídicas o institucionales.

Cuando el correo involucre datos personales, la finalidad deberá ser compatible con las autorizaciones otorgadas por los titulares o con las finalidades previstas en la Política de Tratamiento y Protección de Datos Personales de UNICAFAM.

6.2. Definición de destinatarios

El remitente deberá limitar el envío únicamente a las personas que requieran conocer la información para el cumplimiento de la finalidad correspondiente.

Antes del envío, deberá verificarse que las direcciones de correo electrónico sean correctas y correspondan a los destinatarios autorizados.

6.3. Redacción del mensaje

El mensaje deberá redactarse de manera clara, respetuosa, precisa, institucional y proporcional a la finalidad de la comunicación.

Deberá evitarse incluir datos personales innecesarios en el cuerpo del mensaje. Cuando se trate de datos sensibles, información reservada o información de especial protección, solo podrá incluirse cuando resulte estrictamente necesario y se apliquen las medidas de seguridad correspondientes.

6.4. Asunto del correo

El asunto del correo deberá describir de manera clara y general la finalidad de la comunicación, evitando incluir datos personales sensibles, números de identificación, diagnósticos, información disciplinaria, financiera, académica detallada o cualquier información que pueda exponer indebidamente al titular del dato.

7. Manejo de documentos adjuntos y enlaces

7.1. Documentos adjuntos

Cuando sea necesario adjuntar documentos, el remitente deberá verificar previamente que:

a. El documento corresponda al destinatario correcto.
b. El contenido sea pertinente para la finalidad del envío.
c. No incluya información de terceros que no deba ser compartida.
d. No contenga datos personales innecesarios para la finalidad de la comunicación.
e. Se hayan aplicado las medidas de seguridad requeridas según la naturaleza de la información.

Cuando los documentos adjuntos contengan información reservada, confidencial, sensible o sujeta a especial protección, deberán utilizarse los mecanismos de seguridad definidos por UNICAFAM, por la Política General de Seguridad de la Información o por la dependencia competente.

7.2. Contraseñas y mecanismos de protección

Cuando resulte necesario proteger un archivo mediante contraseña u otro mecanismo de seguridad, la clave o mecanismo de acceso deberá remitirse por un canal distinto al correo electrónico mediante el cual se envía el documento, siempre que ello sea técnicamente posible y conforme a los lineamientos institucionales vigentes.

7.3. Uso de enlaces institucionales

Siempre que sea viable, y de acuerdo con la naturaleza y criticidad de la información, se privilegiará el uso de repositorios, plataformas o herramientas institucionales autorizadas que permitan gestionar permisos de acceso, controlar la disponibilidad de la información y garantizar trazabilidad.

No deberán utilizarse plataformas, servidores, repositorios o cuentas personales para compartir información institucional, salvo autorización expresa de la dependencia competente y siempre que se garanticen las condiciones de seguridad requeridas.

8. Configuración técnica y uso del correo institucional

8.1. Uso de cuentas institucionales

Las comunicaciones oficiales de carácter académico, administrativo, financiero, jurídico, contractual, laboral o institucional deberán realizarse mediante cuentas institucionales autorizadas por UNICAFAM.

No deberán utilizarse cuentas personales para remitir información institucional, salvo situaciones excepcionales debidamente justificadas y autorizadas por la dependencia competente.

8.2. Medidas de autenticación

Los usuarios deberán utilizar las medidas de autenticación, acceso y seguridad implementadas institucionalmente para el uso del correo electrónico corporativo, incluyendo aquellas definidas por el Área de Tecnologías o la dependencia competente.

8.3. Firma institucional

Los correos electrónicos institucionales deberán incorporar la firma institucional definida por UNICAFAM, de acuerdo con los lineamientos establecidos por la Oficina de Comunicaciones o la dependencia competente.

8.4. Aviso de confidencialidad y protección de datos personales

Los correos electrónicos institucionales deberán incorporar, cuando corresponda, el aviso de confidencialidad y protección de datos personales definido institucionalmente, incluyendo el enlace a la Política de Tratamiento y Protección de Datos Personales de UNICAFAM.

8.5. Uso de copia y copia oculta

El remitente deberá utilizar los campos “Para”, “CC” y “CCO” de manera responsable, de acuerdo con la finalidad de la comunicación y la necesidad de conocimiento de los destinatarios.

En los envíos masivos deberá utilizarse el campo “CCO” o la plataforma institucional autorizada para proteger la identidad, dirección electrónica y datos de contacto de los destinatarios.

9. Revisión previa al envío

Antes de enviar un correo electrónico institucional, el remitente deberá realizar una revisión mínima que incluya:

a. Verificar que los destinatarios sean correctos y estén autorizados para recibir la información.

b. Confirmar que el asunto y el cuerpo del mensaje correspondan a la finalidad de la comunicación.

c. Revisar que los documentos adjuntos correspondan al destinatario correcto.

d. Verificar que no se incluyan datos personales o información institucional innecesaria.

e. Confirmar que, cuando sea necesario, se hayan aplicado medidas de seguridad sobre los documentos o enlaces compartidos.

f. Revisar que no se envíe información de terceros sin autorización o sin una finalidad legítima.

g. Confirmar que se utilicen la cuenta y la firma institucionales correspondiente.

10. Envío de correos masivos

Para efectos del presente Protocolo, se entiende por correo masivo aquel dirigido simultáneamente a varios destinatarios, especialmente cuando estos no pertenecen a la misma dependencia, grupo interno de trabajo o relación funcional directa.

En los envíos masivos deberán observarse, además de los lineamientos generales, las siguientes reglas:

a. Verificar que la finalidad del envío sea legítima y compatible con las autorizaciones otorgadas por los titulares de los datos o con las finalidades previstas en la Política de Tratamiento y Protección de Datos Personales de UNICAFAM.

b. Utilizar el campo “CCO” o la plataforma institucional autorizada para evitar la exposición de direcciones electrónicas y datos de contacto.

c. Abstenerse de incluir en el cuerpo del correo información personal de los destinatarios o de terceros, salvo que sea estrictamente necesaria y esté autorizada.

d. Verificar que los documentos adjuntos, enlaces o archivos compartidos no permitan el acceso a información personal, académica, laboral, financiera, jurídica o institucional de personas distintas al destinatario autorizado.

e. Utilizar, cuando corresponda, las herramientas institucionales autorizadas para comunicaciones masivas.

f. Evitar el envío de comunicaciones masivas desde cuentas personales, servidores externos o plataformas no autorizadas institucionalmente.

11. Envío de diplomas, certificados, constancias y documentos académicos

El envío de diplomas, certificados, constancias, actas, documentos académicos o documentos equivalentes deberá realizarse con especial cuidado, en atención a que estos pueden contener datos personales, información académica y datos sujetos a protección.

Para estos casos deberán observarse las siguientes reglas:

a. Verificar que el destinatario del documento sea el titular de la información o la persona expresamente autorizada para recibirla.

b. Confirmar que el documento adjunto corresponda exclusivamente al titular destinatario del correo.

c. Evitar el envío conjunto de documentos pertenecientes a varios titulares, salvo que exista una finalidad legítima, autorización correspondiente y medidas de seguridad adecuadas.

d. Utilizar cuentas institucionales autorizadas para el envío.

e. Aplicar las medidas de seguridad que correspondan según la naturaleza del documento y los lineamientos institucionales vigentes.

f. Abstenerse de compartir documentos académicos con terceros sin autorización previa, expresa e informada del titular, salvo que exista obligación legal o requerimiento de autoridad competente.

12. Códigos QR, enlaces de validación y mecanismos de consulta

Los mecanismos de validación digital utilizados por UNICAFAM, incluidos códigos QR, enlaces de consulta, repositorios o herramientas equivalentes, deberán configurarse de manera que permitan acceder únicamente a la información necesaria para verificar la autenticidad del documento correspondiente.

Cuando se utilicen códigos QR o enlaces de validación asociados a diplomas, certificados, constancias o documentos académicos, estos no deberán permitir el acceso a documentos de otros titulares ni a información adicional que no resulte necesaria para la finalidad de verificación.

Los códigos QR, enlaces de validación o mecanismos equivalentes deberán compartirse únicamente con el titular del documento o con el tercero autorizado por este, salvo que exista obligación legal o requerimiento de autoridad competente.

13. Remisión de información académica a terceros

Cuando un estudiante, egresado, trabajador, profesor o titular de información solicite que UNICAFAM remita directamente información académica, laboral, certificaciones, constancias, diplomas, actas, certificados de notas u otros documentos a un tercero, deberá otorgar autorización previa, expresa e informada, conforme a la Política de Tratamiento y Protección de Datos Personales de UNICAFAM.

La autorización deberá contener, como mínimo:

a. Nombres y apellidos completos del titular.

b. Tipo y número de documento de identificación del titular.

c. Finalidad específica del envío de la información.

d. Identificación del destinatario de la información, incluyendo nombre de la persona o entidad, dirección de correo electrónico y, cuando aplique, nombre de la institución u organización receptora.

e. Descripción precisa de la información o documentos que se autoriza remitir.

f. Fecha de autorización.

g. Manifestación expresa de autorización para el tratamiento y envío de la información.

h. Medio o mecanismo mediante el cual se otorgó la autorización.

La autorización deberá conservarse en el expediente físico o electrónico que corresponda, de acuerdo con las Tablas de Retención Documental y los lineamientos institucionales vigentes.

14. Conservación de correos electrónicos institucionales

La conservación, organización, eliminación, transferencia y disposición final de correos electrónicos que constituyan documentos de archivo deberá realizarse conforme a las Tablas de Retención Documental, las políticas de archivo y los demás lineamientos institucionales aplicables.

Los usuarios deberán evitar la conservación indefinida de información personal, sensible, reservada o confidencial en buzones, carpetas personales o repositorios no autorizados.

Cuando un correo electrónico constituya soporte de una actuación académica, administrativa, contractual, jurídica, financiera, laboral o institucional, deberá conservarse de acuerdo con los procedimientos definidos por la dependencia competente.

15. Prohibiciones especiales

En el uso del correo electrónico institucional se prohíbe:

a. Enviar información institucional, datos personales o documentos protegidos a destinatarios no autorizados.

b. Remitir documentos que contengan datos personales de terceros sin finalidad legítima o autorización correspondiente.

c. Utilizar cuentas personales para el envío de información institucional, salvo autorización excepcional de la dependencia competente.

d. Compartir contraseñas, credenciales de acceso o mecanismos de autenticación.

e. Reenviar información confidencial, reservada o sensible sin autorización.

f. Utilizar plataformas, repositorios o servicios externos no autorizados para almacenar o compartir información institucional.

g. Incluir datos sensibles en el asunto del correo electrónico.

h. Realizar envíos masivos exponiendo las direcciones electrónicas de los destinatarios.

i. Alterar, manipular o modificar documentos institucionales sin autorización.

j. Suplantar identidades, cargos, dependencias o cuentas institucionales.

k. Usar el correo institucional para fines contrarios a la ley, a la ética institucional, a los reglamentos internos o a las políticas de UNICAFAM.

16. Gestión de incidentes

Se entenderá como incidente, para efectos del presente Protocolo, cualquier evento que pueda comprometer la confidencialidad, integridad, disponibilidad, circulación restringida o seguridad de la información institucional o de los datos personales gestionados mediante correo electrónico.

Podrán constituir incidentes, entre otros:

a. Envío de información a destinatarios equivocados.

b. Divulgación no autorizada de datos personales.

c. Envío de documentos pertenecientes a un titular distinto del destinatario.

d. Exposición de direcciones de correo electrónico en envíos masivos.

e. Pérdida de confidencialidad de información institucional.

f. Acceso indebido a cuentas de correo electrónico.

g. Sospecha de suplantación, fraude, phishing o compromiso de credenciales.

h. Uso de plataformas no autorizadas para compartir información institucional.

i. Cualquier evento que involucre datos personales y pueda afectar los derechos de sus titulares.

17. Reporte de incidentes

Toda persona que identifique o cause accidentalmente un incidente relacionado con el envío de correos electrónicos institucionales deberá reportarlo de manera inmediata a la dependencia competente, conforme a la Política General de Seguridad de la Información al Área de Tecnologías.

El reporte deberá realizarse tan pronto como se tenga conocimiento del evento y deberá incluir, en la medida de lo posible:

a. Fecha y hora del incidente.
b. Descripción del evento.
c. Cuenta de correo desde la cual se realizó el envío o se detectó el evento.
d. Destinatarios involucrados.
e. Tipo de información comprometida.
f. Acciones inmediatas realizadas por el usuario.
g. Evidencias disponibles, cuando existan.

18. Atención, contención y seguimiento de incidentes

Una vez reportado el incidente, UNICAFAM adoptará las medidas de contención, análisis, corrección, mitigación, documentación y seguimiento que correspondan, de acuerdo con la Política General de Seguridad de la Información, los procedimientos institucionales aplicables y la normativa sobre protección de datos personales.

Cuando el incidente involucre datos personales, se deberán valorar las medidas necesarias para proteger los derechos de los titulares y cumplir las obligaciones legales e institucionales que resulten aplicables.

19. Responsabilidad de los usuarios

Los usuarios del correo electrónico institucional son responsables por el uso adecuado de sus cuentas, la protección de sus credenciales, la verificación previa de destinatarios, la revisión de documentos adjuntos, la observancia de medidas de seguridad y el cumplimiento de la normativa institucional aplicable.

El incumplimiento del presente Protocolo podrá dar lugar a las acciones administrativas, disciplinarias, contractuales, académicas o legales que correspondan, de acuerdo con la naturaleza del vínculo de la persona involucrada y las disposiciones institucionales aplicables.

20. Interpretación y aplicación armónica

El presente Protocolo deberá interpretarse de manera armónica con los Estatutos de UNICAFAM, la Política de Tratamiento y Protección de Datos Personales, la Política General de Seguridad de la Información, el Reglamento Interno de Trabajo, las Tablas de Retención Documental, los lineamientos de comunicaciones institucionales y las demás disposiciones internas que regulen el uso de herramientas tecnológicas, la protección de datos personales y la seguridad de la información.

21. Revisión y mejora continua

El presente Protocolo podrá ser revisado, ajustado o actualizado cuando se presenten cambios normativos, tecnológicos, institucionales, operativos o de gestión de riesgos que así lo ameriten, o cuando las dependencias competentes identifiquen oportunidades de mejora para fortalecer la protección de datos personales, la seguridad de la información y la eficiencia de las comunicaciones institucionales.

Fin del documento

Control de revisiones y actualizaciones.

Primera versión.	10/07/2026	Resolución Rectoral 5 de 2026