1. OBJETIVO

Establecer los lineamientos y controles para la administración de las cuentas de correo electrónico institucional durante ausencias temporales, traslados, cambios de funciones y desvinculaciones de servidores públicos y contratistas, garantizando la continuidad de la gestión institucional y de los servicios, así como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, de acuerdo con las disposiciones institucionales de seguridad de la información, gestión documental y protección de datos aplicables.

2. ALCANCE

Este instructivo aplica a las cuentas de correo electrónico institucional administradas por la entidad, de acuerdo con su arquitectura tecnológica y modelo de administración, incluyendo:

- Cuentas nominales asignadas a servidores públicos o contratistas.
- Cuentas funcionales asociadas a procesos, dependencias o servicios institucionales.
- Buzones compartidos.
- Listas de distribución institucionales.

Aplica, según la necesidad funcional y los controles definidos, en los siguientes eventos:

- Vacaciones.
- Licencias.
- Comisiones.
- Incapacidades.
- Suspensiones.
- Traslados.
- Cambios de funciones.
- Terminación de contratos.
- Retiro o desvinculación de servidores públicos.
- Cualquier otra situación administrativa u operativa que afecte temporal o definitivamente la administración, acceso o uso autorizado de una cuenta institucional.

El alcance de este instructivo comprende las configuraciones, permisos y acciones técnicas sobre las cuentas de correo, pero no sustituye los procedimientos de gestión humana, gestión documental, seguridad de la información, gestión de incidentes, entrega de cargo ni los procedimientos específicos de las plataformas institucionales.

3. MARCO DE REFERENCIA

La aplicación de este instructivo deberá articularse con la normativa, políticas, procedimientos e instrumentos institucionales vigentes, entre ellos:

- Ley 594 de 2000 – Ley General de Archivos.
- Ley 1581 de 2012 – régimen general de protección de datos personales, cuando resulte
- aplicable.
- Decreto 1080 de 2015 y demás disposiciones que regulen la gestión documental pública, en lo
- pertinente.
- ISO 9001:2015 – Sistemas de gestión de la calidad, como referente del sistema de gestión
- institucional.
- ISO/IEC 27001:2022 – Sistemas de gestión de seguridad de la información.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- ISO 15489-1:2016 – Gestión de documentos de archivo.
- Política de Seguridad y Privacidad de la Información.
- Política de Gestión Documental.
- Programa de Gestión Documental (PGD), cuando aplique.
- Tablas de Retención Documental (TRD), Tablas de Valoración Documental (TVD) y demás instrumentos archivísticos vigentes, según corresponda.
- Procedimiento de Soporte Técnico / Mesa de Servicios.
- Procedimiento institucional para la gestión de incidentes de seguridad de la información.
- Demás disposiciones legales, reglamentarias y administrativas aplicables.

4. DEFINICIONES

Cuenta nominal: Cuenta de correo institucional asignada individualmente a un servidor público o contratista para el desarrollo de sus funciones.

Cuenta funcional: Cuenta de correo asociada a un proceso, dependencia, servicio o función institucional y no a una persona específica.

Buzón compartido: Buzón al que acceden varios usuarios autorizados mediante permisos individuales para atender actividades institucionales.

Lista de distribución: Mecanismo institucional utilizado para distribuir mensajes a un conjunto definido de destinatarios.

Redirección o reenvío: Configuración que remite mensajes entrantes a otra cuenta institucional autorizada, durante un período definido y bajo condiciones previamente aprobadas.

Acceso temporal autorizado: Permiso excepcional, individual, controlado y limitado en el tiempo para consultar o gestionar información contenida en una cuenta institucional por una necesidad funcional justificada.

Mínimo privilegio: Principio según el cual se conceden únicamente los permisos necesarios para realizar una actividad, durante el tiempo estrictamente requerido.

Trazabilidad: Capacidad de identificar y reconstruir quién solicitó, autorizó, ejecutó, modificó, verificó y cerró una actuación sobre una cuenta institucional.

Kaía: Mesa de Servicios institucional utilizada para registrar, gestionar, aprobar, ejecutar, verificar y cerrar solicitudes relacionadas con servicios TIC, conforme a su configuración y procedimientos.

Documento de archivo: Información producida o recibida en el desarrollo de las funciones institucionales que deba conservarse de acuerdo con las reglas e instrumentos de gestión documental aplicables.

5. PRINCIPIOS GENERALES

- Titularidad institucional de la información: la información institucional generada, recibida, almacenada o gestionada mediante cuentas institucionales deberá tratarse conforme a las responsabilidades y controles de la entidad. La asignación de una cuenta a una persona no implica propiedad personal sobre la información institucional.
- Continuidad del servicio: las ausencias, traslados, cambios de funciones o desvinculaciones no deberán afectar injustificadamente la prestación de los servicios, la ejecución de los procesos ni la atención de usuarios.
- Necesidad funcional: todo acceso, transferencia, redirección o tratamiento sobre una cuenta deberá estar sustentado en una necesidad del servicio.
- Mínimo privilegio: deberán otorgarse únicamente los permisos necesarios y por el tiempo estrictamente requerido.
- Segregación de funciones: cuando sea posible, las funciones de solicitar, autorizar, ejecutar y verificar deberán recaer en roles diferenciados.
- Identidad individual: no se deberán compartir contraseñas ni utilizar credenciales del titular original. Cuando se requiera acceso temporal, deberá asignarse a una identidad individual y autorizada.
- Confidencialidad y protección de datos: el acceso a la información deberá limitarse a quienes tengan autorización y necesidad funcional, aplicando las medidas institucionales de protección de datos.
- Integridad y disponibilidad: las actuaciones no deberán alterar indebidamente la información y deberán preservar la continuidad y disponibilidad requeridas por el proceso.
- Trazabilidad: toda actuación deberá quedar registrada y ser susceptible de auditoría, incluyendo como mínimo solicitante, autorización, responsable de ejecución, fecha/hora, acción y resultado, cuando la plataforma lo permita.
- Gestión documental: la identificación, organización, conservación, transferencia y disposición de documentos de archivo se realizará conforme a los instrumentos archivísticos y procedimientos institucionales aplicables.

6. ROLES Y RESPONSABILIDADES

6.1 Jefe de Oficina

o responsable del proceso

- Identificar las necesidades de continuidad derivadas de ausencias, traslados, cambios de funciones o desvinculaciones.
- Determinar la redistribución temporal o permanente de funciones.
- Definir la persona responsable de asumir los asuntos pendientes, cuando corresponda.
- Solicitar mediante Kaía las actuaciones requeridas sobre las cuentas institucionales.
- Justificar la necesidad funcional y el período requerido.
- Autorizar las actuaciones que correspondan dentro de sus competencias.
- Verificar con el responsable técnico que las medidas temporales hayan sido cerradas cuando finalice la necesidad.

6.2 Oficina de Gestión Humana

- Informar oportunamente a la Oficina de CTeI y a las áreas que corresponda las novedades administrativas relacionadas con ausencias, traslados, cambios de funciones y desvinculaciones, de acuerdo con los flujos institucionales.
- Coordinar, cuando corresponda, la entrega formal de cargo e información institucional.
- Gestionar las novedades administrativas que constituyan el evento habilitante para las acciones de acceso, modificación o bloqueo.

6.3 Oficina técnica responsable de la administración de cuentas

La Oficina Asesora de Ciencia, Tecnología e Innovación (CTeI) será la dependencia técnica responsable de la administración de las cuentas de correo electrónico institucional, dentro del ámbito de sus competencias.

Para la ejecución, coordinación y seguimiento de las actividades previstas en el presente instructivo, la Oficina de CTeI designará al profesional grado 10 Carlos Alberto Vásquez Sánchez, adscrito a la oficina de CTeI quien actuará como responsable operativo y punto de contacto institucional, dentro del ámbito de sus funciones y competencias.

El profesional designado estará encargado de coordinar, tramitar, hacer seguimiento y verificar el cumplimiento de las actividades asignadas a la Oficina de CTeI, sin perjuicio de

la responsabilidad institucional que permanece en cabeza de dicha oficina y de las competencias de las demás dependencias involucradas..

- Administrar técnicamente las cuentas institucionales.
- Evaluar técnicamente el mecanismo solicitado y aplicar el que resulte autorizado y adecuado.
- Implementar las configuraciones autorizadas.
- Gestionar los permisos temporales mediante identidades individuales.
- Bloquear, desactivar o modificar cuentas y permisos cuando corresponda.
- Verificar la aplicación y posterior reversión de configuraciones temporales.
- Conservar las evidencias técnicas y registros de trazabilidad definidos.
- Escalar incidentes de seguridad o anomalías detectadas conforme al procedimiento institucional.

6.4 Servidores públicos y contratistas

- Realizar la entrega formal de la información institucional bajo su responsabilidad conforme a los procedimientos aplicables.
- Informar oportunamente las ausencias programadas cuando corresponda.
- Activar o solicitar la activación del mensaje automático de ausencia cuando aplique.
- Cumplir las disposiciones de gestión documental, seguridad de la información y protección de datos.
- No compartir credenciales ni permitir el uso de su cuenta por terceros.

7. GESTIÓN DE AUSENCIAS TEMPORALES

7.1 Solicitud

Cuando el jefe de la oficina a la que se encuentre adscrito el servidor público o contratista deberá registrar la solicitud mediante Kaía, incluyendo como mínimo:

- Nombre del servidor público o contratista ausente.
- Cuenta institucional afectada.
- Tipo de ausencia.
- Fecha y, cuando aplique, hora de inicio y finalización.

- Necesidad funcional que debe atenderse.
- Persona designada para asumir las actividades, cuando corresponda.
- Justificación.
- Mecanismo solicitado, si la oficina identifica uno, sin perjuicio de la evaluación técnica.
- Nivel de urgencia, cuando el sistema de Mesa de Servicios lo contemple.

7.2 Criterios para seleccionar el mecanismo

La oficina de CTeI evaluará la necesidad y aplicará el mecanismo que permita garantizar la continuidad con el menor nivel de exposición de información y el menor privilegio posible.

Se establece la siguiente jerarquía de preferencia:

1. Mensaje automático de ausencia, cuando solo sea necesario informar al remitente.
2. Uso de mecanismos institucionales de acceso compartido o delegación con permisos individuales, cuando estén disponibles y resulten adecuados.
3. Redirección o reenvío controlado y temporal, únicamente cuando exista una necesidad funcional justificada y autorizada.
4. Acceso temporal al buzón, como medida excepcional cuando las alternativas anteriores no satisfagan la necesidad.

7.3 Mensaje automático de ausencia

La respuesta automática deberá indicar, cuando corresponda:

- Período de ausencia.
- Oficina responsable.
- Canal institucional de contacto.
- Persona o equipo designado para la atención.
- Información estrictamente necesaria, evitando divulgar datos personales o información sensible innecesaria.

7.4 Redirección o reenvío

La redirección o reenvío podrá configurarse únicamente cuando la necesidad funcional lo justifique y exista autorización. La configuración deberá:

- Dirigirse a una cuenta institucional autorizada.

- Ser limitada al período aprobado.
- Mantener copia en el buzón original cuando la plataforma y la necesidad de continuidad lo permitan.
- Evitar el reenvío indiscriminado de información cuando sea posible aplicar mecanismos más selectivos.
- Quedar registrada en Kaía.
- Ser verificada y retirada al finalizar la necesidad.

El reenvío automático no constituye el mecanismo preferente general. Su uso deberá evaluarse frente a alternativas de menor exposición.

7.5 Acceso temporal autorizado al buzón

Solo podrá habilitarse cuando la necesidad funcional no pueda resolverse mediante mecanismos menos invasivos. La solicitud deberá justificar:

- La necesidad de consultar información histórica o realizar una actuación específica.
- La imposibilidad o insuficiencia de mecanismos menos invasivos.
- El período requerido.
- El alcance mínimo de los permisos.

Los accesos concedidos:

- Serán individuales y no mediante las credenciales del titular original.
- Tendrán fecha y hora de inicio y finalización, cuando la plataforma lo permita.
- Serán limitados a los permisos estrictamente necesarios.
- Deberán ser revocados al concluir la necesidad del servicio.
- Quedarán registrados para fines de trazabilidad y auditoría.

En ningún caso se permitirá compartir contraseñas o credenciales de acceso.

7.6 Cierre y reversión

Finalizada la ausencia, el jefe de la oficina a la que se encuentre adscrito el servidor público o contratista deberá solicitar mediante Kaía el cierre de las medidas temporales implementadas.

- Eliminar las configuraciones temporales.
- Revocar los permisos otorgados.

- Verificar que no permanezcan reglas, delegaciones o accesos temporales activos.
- Registrar la fecha de cierre y el resultado.
- Adjuntar evidencia de la implementación y cierre cuando corresponda.

8. GESTIÓN DE TRASLADOS Y CAMBIOS DE FUNCIONES

Cuando un servidor público o contratista cambie de oficina o asuma nuevas funciones, el responsable del proceso solicitará mediante Kaía las acciones requeridas sobre la cuenta y demás permisos relacionados, de acuerdo con los procedimientos institucionales.

- Revisión de permisos asociados a las funciones anteriores.
- Asignación o modificación de permisos conforme al nuevo perfil funcional.
- Redirección temporal de mensajes, cuando esté justificada.
- Transferencia de información institucional necesaria para la continuidad.
- Actualización de listas de distribución.
- Modificación o revocación de delegaciones y accesos.
- Verificación del retiro de permisos que ya no sean necesarios.

Todas las actuaciones deberán quedar registradas en Kaía.

9. GESTIÓN DE RETIRO O DESVINCULACIÓN

9.1 Activación del proceso

Una vez recibida la notificación formal de terminación del vínculo o retiro, las áreas responsables deberán activar, según corresponda, las acciones de entrega de información, revisión de accesos y bloqueo de la cuenta, de acuerdo con los procedimientos institucionales y los tiempos definidos.

9.2 Entrega de información institucional

Antes de la terminación del vínculo, cuando sea posible, deberá realizarse la entrega formal de la información institucional bajo responsabilidad del servidor público o contratista.

La entrega deberá ajustarse a:

- Procedimientos internos de gestión documental.
- Instrumentos archivísticos vigentes.

- TRD/TVD y demás instrumentos aplicables.
- FUID, cuando corresponda.
- Requisitos de seguridad de la información y protección de datos.

La información objeto de entrega podrá incluir, según corresponda:

- Documentos de archivo contenidos o gestionados mediante correo electrónico.
- Documentos de trabajo que deban continuar bajo responsabilidad institucional.
- Expedientes electrónicos.
- Repositorios documentales.
- Carpetas compartidas.
- Sistemas de información administrados.
- Otros registros necesarios para garantizar la continuidad.

No deberá interpretarse que todos los mensajes de correo deben incorporarse automáticamente al archivo institucional. La identificación y conservación de documentos de archivo deberá realizarse conforme a los instrumentos y procedimientos de gestión documental aplicables.

9.3 Acciones sobre la cuenta

Una vez formalizada la desvinculación, podrán solicitarse, según la necesidad y autorización:

- Redirección temporal y controlada de comunicaciones, cuando sea necesaria.
- Acceso temporal excepcional para consulta de información histórica, cuando esté justificado.
- Transferencia de información institucional.
- Bloqueo o desactivación de la cuenta.
- Revocación de permisos y delegaciones.
- Revisión de accesos asociados a servicios y plataformas institucionales, de acuerdo con los procedimientos correspondientes.

9.4 Bloqueo y revocación

Recibida y validada la notificación formal de terminación del vínculo, la Oficina de CTeI deberá bloquear o desactivar el acceso a la cuenta dentro del tiempo establecido institucionalmente, documentando la actuación mediante Kaía.

- Bloquear o desactivar el acceso del usuario.
- Revocar permisos y delegaciones asociados.
- Retirar accesos que ya no sean necesarios.
- Verificar que no permanezcan accesos temporales o reglas de reenvío no autorizadas.
- Registrar la fecha/hora de ejecución y resultado.

9.5 Conservación de la información

La conservación de la información asociada a las cuentas institucionales se realizará conforme a las TRD, TVD, demás instrumentos archivísticos vigentes, políticas de seguridad de la información y requerimientos legales, regulatorios o judiciales aplicables.

La eliminación o disposición final de documentos de archivo deberá efectuarse únicamente conforme a los instrumentos archivísticos y procedimientos autorizados. No se deberán establecer períodos arbitrarios de eliminación por el solo hecho de que la persona haya sido desvinculada.

10. SEGURIDAD DE LA INFORMACIÓN Y CONTROL

Toda actuación deberá preservar, según corresponda:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticidad.
- Trazabilidad.

La Oficina de CTeI deberá mantener los registros disponibles en los sistemas institucionales, según corresponda, de:

- Solicitudes.
- Aprobaciones.
- Implementaciones.
- Modificaciones.
- Accesos temporales.
- Revocaciones.

- Cierres.
- Incidentes o excepciones relacionados.

La evidencia oficial de las actuaciones corresponderá a los registros generados en Kaía y demás sistemas corporativos autorizados, de acuerdo con las reglas institucionales de conservación y acceso.

11. GESTIÓN DE INCIDENTES Y EXCEPCIONES

11.1 Incidentes

Cualquier evento que pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de una cuenta deberá reportarse por los canales institucionales definidos para la gestión de incidentes.

- Acceso no autorizado.
- Uso o divulgación indebida de credenciales.
- Redirección o delegación no autorizada.
- Acceso posterior a una desvinculación.
- Pérdida o eliminación no autorizada de información.
- Envío indebido de información.
- Sospecha de compromiso de la cuenta.
- Configuraciones que no hayan sido retiradas al finalizar el período autorizado.

La atención del incidente se realizará conforme al procedimiento institucional de gestión de incidentes de seguridad de la información.

11.2 Excepciones y emergencias

Cuando exista una situación que amenace la continuidad del servicio y no permita seguir el flujo ordinario, la actuación excepcional deberá ser autorizada por el responsable competente y quedar registrada posteriormente o de inmediato, según las capacidades de la Mesa de Servicios.

Las excepciones deberán documentar como mínimo: motivo, riesgo, acción realizada, responsable, autorización, duración y medidas adoptadas para retornar al control ordinario.

12. PROHIBICIONES

- Compartir contraseñas o credenciales institucionales.
- Permitir el uso de una cuenta nominal por otra persona mediante las credenciales del titular.
- Entregar credenciales a terceros o a personal no autorizado.
- Utilizar cuentas institucionales para suplantar identidades.
- Configurar accesos, delegaciones o reenvíos sin autorización formal.
- Eliminar información institucional sin autorización y sin aplicar los procedimientos archivísticos correspondientes.
- Ejecutar actuaciones fuera de los mecanismos de registro establecidos, salvo excepciones formalmente justificadas.
- Utilizar cuentas institucionales para fines contrarios a las políticas y disposiciones de la entidad.

13. REGISTROS Y EVIDENCIAS

Registro / evidencia	Responsable	Medio	Contenido mínimo	Conservación
Solicitud de servicio	Oficina solicitante	Kaía	Cuenta, evento, fechas, necesidad, responsable, autorización	Según TRD / reglas institucionales
Aprobación	Jefe o responsable autorizado	Kaía	Aprobador, fecha, alcance, período	Según TRD / reglas institucionales
Evidencia de implementación	Oficina de CTeI	Kaía / plataforma autorizada	Acción, responsable, fecha/hora, resultado	Según política y TRD aplicable
Registro de acceso temporal	Oficina de CTeI	Plataforma / Kaía	Usuario, permisos, inicio, fin, revocación	Según política de seguridad y reglas institucionales
Evidencia de cierre	Oficina de CTeI	Kaía	Configuración retirada, permisos revocados, verificación	Según TRD / reglas institucionales
Entrega de información / FUID	Oficimna / Gestión Humana	Sistema de Gestión Documental	Información entregada y soporte documental	Según instrumentos archivísticos
Registro de incidente o excepción	Responsable definido por el procedimiento	Sistema de incidentes / Kaía	Evento, riesgo, acciones, autorización, cierre	Según procedimiento aplicable

14. SEGUIMIENTO, MEDICIÓN E INDICADORES

El responsable del proceso deberá realizar seguimiento periódico a la eficacia de este instructivo. Se proponen como indicadores mínimos:

Indicador	Fórmula	Meta propuesta*	Frecuencia
Atención oportuna de solicitudes	Solicitudes atendidas dentro del tiempo establecido / total solicitudes × 100	≥95 %	Mensual
Cierre oportuno de accesos temporales	Accesos cerrados dentro del plazo / total accesos temporales × 100	100 %	Mensual
Bloqueo oportuno por desvinculación	Cuentas bloqueadas dentro del tiempo definido / total desvinculaciones × 100	100 %	Mensual
Trazabilidad completa	Solicitudes con evidencia completa / total solicitudes × 100	≥98 %	Trimestral

*Las metas son propuestas de gestión y deberán ser validadas por la entidad de acuerdo con sus riesgos, capacidad operativa y acuerdos de nivel de servicio.

15. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
1	05/08/2026	Emisión inicial del instructivo.	Equipo de la Oficina Asesora de CTel
2	21/08/2026	Revisión integral: precisión de responsabilidades, controles de acceso, gestión documental, cierre, incidentes, excepciones, registros e indicadores.	Equipo responsable / revisión de calidad

16. MATRIZ OPERATIVA DE DECISIÓN

Situación	Mecanismo principal	Autorización	Acceso al buzón	Control de cierre
Vacaciones / ausencia corta	Mensaje automático	Jefe de dependencia	No	Verificar desactivación al regreso
Ausencia que requiere atención de mensajes	Mecanismo institucional de delegación o redirección controlada	Jefe + evaluación técnica	No necesariamente	Retirar configuración al finalizar

Consulta histórica excepcional	Acceso temporal individual	Jefe + responsable técnico, según competencias	Sí	Revocar y verificar
Traslado / cambio de funciones	Revisión y ajuste de permisos	Responsable del proceso	Según necesidad	Retirar permisos anteriores
Desvinculación	Bloqueo + gestión documental + revisión de accesos	Gestión Humana / responsable autorizado	Excepcional	Verificar bloqueo y revocación
Incidente	Procedimiento de incidentes	Según protocolo institucional	Según investigación	Cierre documentado

17. ANEXOS Y DOCUMENTOS RELACIONADOS

- Formato o solicitud de Mesa de Servicios para administración de cuentas.
- Procedimiento de gestión de incidentes de seguridad de la información.
- Procedimiento de entrega de cargo.
- Política de Seguridad y Privacidad de la Información.
- Política de Gestión Documental.
- Programa de Gestión Documental e instrumentos archivísticos vigentes.
- Procedimiento de administración de usuarios y control de accesos, si existe.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1	02/09/2026	Creación del Documento