UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

DIRECTIVA INTERNA N° 001-2026-OTI-UNAP "ADMINISTRACIÓN Y USO DEL CORREO ELECTRÓNICO EN LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA"

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

IQUITOS – LORETO

2026

UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

ÓRGANOS RESPONSABLES Y APROBACIÓN DE LA DIRECTIVA

ROL	ÓRGANO	SELLO Y FIRMA
ELABORADO POR	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	RENZO GIANCARLO DA SILVA DE OLIVEIRA DDD Jefe de la Oficina de Tecnología de la Información - UNAP JEFATURA
REVISADO POR	UNIDAD DE MODERNIZACIÓN	UNIV. NACIONAL DE LA AMAZONIA PERUANA UNIDAD DE MODERNIZACIÓN OPP
APROBADO POR	RECTORADO	Resolución Rectoral N° 1420-2026-UNAP, del 23 de octubre de 2026

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	octubre 2026	Versión Inicial

Contenido

I. OBJETIVO 7
II. FINALIDAD 7
III. BASE LEGAL 7
IV. ALCANCE 9
V. ACRÓNIMOS 9
VI. DEFINICIONES 10
VII. RESPONSABILIDADES 12
7.1. Responsabilidad de la máxima autoridad administrativa. 12
7.2. Responsabilidad de la Oficina de Tecnologías de la Información como administrador del servicio de correo electrónico institucional 13
7.3. Responsabilidad del Oficial de Seguridad y Confianza Digital 16
7.4. Responsabilidad de los titulares de las cuentas de correo electrónico institucional 17
7.5. Responsabilidad de los usuarios de las cuentas de correo electrónico institucional 17
7.6. Responsabilidad del Comité de Gobierno Digital 18
7.7. Responsabilidad del Oficial de Datos Personales 18
7.8. Responsabilidad de las dependencias y unidades orgánicas 19
7.9. Responsabilidad de las unidades de gestión de personal, abastecimiento y registro académico 19
7.10. Responsabilidad frente a incidentes y uso indebido 20
VIII. DISPOSICIONES GENERALES 20
8.1. Naturaleza del correo institucional 20
8.2. Carácter oficial de las comunicaciones 20
8.3. Dominio institucional 20
8.4. Clasificación y presunción de publicidad de la información 20
8.5. Mesa de Partes Digital y sistemas de negocio 21
8.6. Infraestructura autorizada 21
8.7. Uso obligatorio y responsable 21
8.8. Sanciones por uso indebido 21
IX. DISPOSICIONES ESPECÍFICAS 21
9.1. Gestión del servicio y niveles de servicio 21
9.2. Creación del Correo Institucional y Asignación. 21

9.3. Estructura del Nombre de Usuario e Identificadores. 23
9.4. Las Contraseña, MFA y credenciales 25
9.5. Soporte en el Manejo y Acceso. 27
9.6. Uso incorrecto del correo electrónico institucional 27
9.6.1. Del mal uso de la cuenta de correo electrónico institucional 27
9.6.2. Del contenido de los mensajes y la conducta ética 27
9.6.3. De la seguridad digital 28
9.2.4. Del uso en la comisión de delitos 28
9.7. Suspensión, restricción y cese del uso del servicio. 29
9.8. Asignación y gestión de cuotas de almacenamiento del correo electrónico institucional. 29
9.9. Firma estandarizada en el correo electrónico institucional. 31
9.10. Seguridad de la Información 32
9.11. Vigencia de la cuenta de correo electrónico institucional. 32
9.12. Registros de auditoría y monitoreo 33
9.13. Continuidad, respaldos, RTO y RPO 33
9.14. Acceso desde dispositivos móviles 34
9.15. Acceso a información pública contenida en cuentas institucionales 34
9.16. Conservación de información oficial 34
9.17. Fiscalización y Control del Correo Institucional. 35
X. DISPOSICIONES COMPLEMENTARIAS 36
Primera. Supervisión y control del servicio 36
Segunda. Auditoría de cuentas institucionales 37
Tercera. Gestión de incidentes y correos indebidos 37
Cuarta. Medidas correctivas y responsabilidades 37
Quinta. Revisión anual de cuentas funcionales 37
Sexta. Cuentas vinculadas a Mesa de Partes o recepción documental 37
Séptima. Actualización normativa 38
Octava. Interpretación y casos no previstos 38
ANEXO 1: SOLICITUD DE CREACION DE CUENTA NOMINAL PARA PERSONAL ADMINISTRATIVO Y DOCENTES 39
ANEXO 2: SOLICITUD DE CREACIÓN, MODIFICACIÓN O RENOVACIÓN DE CUENTA FUNCIONAL 40

ANEXO 3: SOLICITUD DE SUSPENSIÓN, BAJA O ELIMINACIÓN DE CUENTA INSTITUCIONAL 41

ANEXO 4: GUÍA PARA ACTIVAR LA AUTENTICACIÓN DE MÚLTIPLES FACTORES EN LA CUENTA INSTITUCIONAL (GMAIL) 42

ANEXO 5: MATRIZ RACI DEL CICLO DE VIDA DE CUENTAS INSTITUCIONALES47

ANEXO 6: FLUJOGRAMA TEXTUAL DE CREACIÓN Y BAJA DE CUENTAS..... 48

ANEXO 7: DIAGRAMA DE FUJO DE CREACIÓN DE USUARIO 49

ANEXO 8: DIAGRAMA DE FUJO DE INICIO DE SESIÓN, CAMBIO DE CLAVE Y ACTIVACIÓN DE AUTENTICACIÓN MULTI-FACTOR..... 50

ANEXO 9: DIAGRAMA DE FUJO DE REPORTE DE INCIDENCIAS 51

ANEXO 10: DIAGRAMA DE FUJO DE REDUCCIÓN DE TAMAÑO DE ALMACENAMIENTO EN LA NUBE 52

ANEXO 11: DIAGRAMA DE FUJO DE SUSPENSIÓN DE CUENTA 53

ANEXO 12: DIAGRAMA DE FUJO DEL CESE E INACTIVIDAD DEL USUARIO..... 54

ANEXO 13: DECLARACIÓN JURADA DE ENTREGA DE INFORMACIÓN OFICIAL55

ANEXO 14: INVENTARIO Y REVISIÓN ANUAL DE CUENTAS FUNCIONALES..... 56

LINEAMIENTOS DEL CORREO ELECTRÓNICO INSTITUCIONAL

I. OBJETIVO

Establecer los lineamientos institucionales para la gestión, operación, supervisión, uso seguro, conservación y control del servicio de correo electrónico institucional de la Universidad Nacional de la Amazonía Peruana (UNAP), bajo el dominio unapiquitos.edu.pe, de conformidad con la Directiva N.° 001-2026-PCM/SGTD y la normativa vigente en materia de gobierno digital, seguridad y confianza digital, transparencia, acceso a la información pública y protección de datos personales.

La presente Directiva regula el ciclo de vida de las cuentas de correo electrónico institucionales nominales y funcionales, los roles y responsabilidades de los actores involucrados, las condiciones de uso aceptable, la seguridad técnica, la gestión de incidentes, la conservación de información oficial y la disponibilidad del servicio como activo digital institucional.

II. FINALIDAD

Garantizar que el servicio de correo electrónico institucional y la información contenida en este se gestionen, utilicen, protejan y conserven de forma eficiente, segura y trazable, fortaleciendo la confidencialidad, integridad, disponibilidad y autenticidad de las comunicaciones electrónicas institucionales, así como mitigando y previniendo incidentes de seguridad digital.
Asimismo, la Directiva busca:

1. Asegurar el uso del correo institucional como canal oficial de comunicación interna y externa de la UNAP, sin sustituir a los sistemas de negocio, sistemas documentales o Mesa de Partes Digital cuando correspondan.

2. Proteger la información institucional, académica, administrativa y los datos personales tratados mediante el servicio de correo electrónico.

3. Prevenir el uso indebido del servicio, la suplantación de identidad, el spam, el fraude electrónico, la fuga de información y otros riesgos de seguridad digital.

4. Promover buenas prácticas de comunicación, responsabilidad digital, trazabilidad, conservación documental y reducción del uso de papel.

III. BASE LEGAL

La presente Directiva se enmarca en el Sistema de Gestión de Seguridad de la Información (SGSI) de la UNAP y se sustenta, sin carácter limitativo, en las siguientes normas:

1. Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
2. Ley N° 30096, Ley de delitos informáticos.
3. Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
4. Ley N° 27269, Ley de Firmas y Certificados Digitales, 28 de mayo de 2000 y modificatorias.

5. Ley N° 27291, Ley que modifica el código civil permitiendo la utilización de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica, del 24 de junio de 2000.
6. Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
7. Ley N° 27419, Ley sobre Notificación por Correo Electrónico.
8. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y modificatorias.
9. Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública, del 18 de octubre de 2005.
10. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
11. Ley N° 29733, Ley de Protección de Datos Personales.
12. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, del 13 de septiembre de 2018 y modificatoria.
13. Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
14. Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, norma que crea el Sistema Nacional de Transformación Digital (SNTD) en el Perú.
15. Decreto de Urgencia N° 007-2020, que establece el Marco de Confianza Digital.
16. Decreto Supremo N° 126-2025-PCM, que aprueba el Reglamento del Decreto de Urgencia N.° 007-2020, Marco de Confianza Digital.
17. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital, del 19 de febrero de 2021 y modificatoria.
18. Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, del 19 de julio de 2008 y modificatorias.
19. Decreto Supremo N° 031-2005-MTC - Reglamento de la Ley N° 28493 que regula el envío del correo electrónico comercial no solicitado (SPAM).
20. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General, del 25 de enero de 2019.
21. Resolución Directoral N° 022-2022-INACAL/DN, Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros: NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014, del 12 de enero de 2023.
22. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
23. Resolución Jefatural N° 207-2002-INEI, que aprueba la Directiva N° 010-2002-INEI/DTNP "Normas Técnicas para la asignación de nombres de Dominio de las entidades de la Administración Pública", del 11 de julio de 2002.
24. Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEI/DTNP, "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", 3 de abril de 2003.
25. Resolución de Secretaría de Gobierno Digital N° 001-2018-PCM/SEGDI, que aprueba los Lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano, del 4 de enero de 2018.
26. Decreto Supremo N° 007-2024-JUS, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.

27. Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley N° 29733 Ley de Protección de Datos Personales.
28. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
29. Resolución de Secretaría de Gobierno y Transformación Digital N° 001-2026-PCM/SGTD, que aprueba la Directiva N° 001-2026-PCM/SGTD - Directiva que regula el servicio de correo electrónico institucional en las entidades públicas.
30. Resolución de Asamblea Estatutaria N° 001-2014-AE-UNAP, que aprueba el Estatuto de la Universiada Nacional de la Amazonía Peruana, 15 de diciembre 2014 y sus modificatorias.
31. Resolución de Consejo Universitario N° 157-2021-UNAP, que aprueba el Reglamento de Organización y Funciones (ROF) de la Universidad Nacional de la Amazonía Peruana (UNAP).
32. Resolución Rectoral N° 0851-2021-UNAP - Se aprueba la Directiva N° 003-2021-UR/OGPP-UNAP "Lineamientos para la elaboración, modificación y aprobación de directivas en la Universidad Nacional de la Amazonía Peruana"

IV. ALCANCE

La presente Directiva es de aplicación obligatoria para todos los miembros de la comunidad universitaria y personas usuarias del servicio de correo electrónico institucional de la UNAP, incluyendo autoridades, funcionarios, empleados de confianza, servidores públicos, docentes, personal administrativo, estudiantes de pregrado y posgrado, egresados, locadores de servicios, personas bajo modalidades formativas, personal externo autorizado, oficinas administrativas, facultades, escuelas profesionales, escuela de posgrado, unidades orgánicas, comisiones, proyectos, servicios, sistemas automatizados y demás dependencias que dispongan o requieran una cuenta de correo institucional bajo el dominio unapiquitos.edu.pe.

El uso del correo electrónico institucional constituye una habilitación de uso para fines institucionales, académicos, administrativos o de gestión universitaria. No otorga derecho de propiedad al titular ni al usuario y se sujeta a las condiciones, responsabilidades y restricciones establecidas en esta Directiva.

V. ACRÓNIMOS

1. CNSD: Centro Nacional de Seguridad Digital.
2. CSIRT: Equipo de Respuesta a Incidentes de Seguridad Digital.
3. DKIM: DomainKeys Identified Mail.
4. DMARC: Domain-based Message Authentication, Reporting and Conformance.
5. DNS: Sistema de Nombres de Dominio.
6. IMAP: Internet Message Access Protocol.
7. IP: Internet Protocol.
8. MFA: Autenticación de múltiples factores.
9. ODP: Oficial de Datos Personales.
10. OSCD: Oficial de Seguridad y Confianza Digital.
11. OTI: Oficina de Tecnologías de la Información.
12. PCDA: Programa de Control de Documentos Archivísticos.
13. PCM: Presidencia del Consejo de Ministros.
14. PIN: Personal Identification Number.

15. POP/POP3: Post Office Protocol, versión 3.
16. RPO: Objetivo de Punto de Recuperación.
17. RTO: Objetivo de Tiempo de Recuperación.
18. SGSI: Sistema de Gestión de Seguridad de la Información.
19. SGTD: Secretaría de Gobierno y Transformación Digital.
20. SLA: Service Level Agreement.
21. SMTP: Simple Mail Transfer Protocol.
22. SPF: Sender Policy Framework.
23. SSL: Secure Sockets Layer.
24. TLS: Transport Layer Security.
25. UNAP: Universidad Nacional de la Amazonía Peruana.

VI. DEFINICIONES

a) **Activo digital:** Elemento, objeto o recurso en formato digital que tiene un valor potencial o real para una organización, sobre los que se deben establecer controles de seguridad, a fin de garantizar su integridad, disponibilidad y confidencialidad. Por ejemplo, en el contexto de la presente directiva, se consideran activos digitales: el servicio de correo electrónico institucional, la cuenta de correo, los mensajes de correo electrónico, los ficheros adjuntos, los registros de auditoría (logs), los contactos y cualquier información procesada o almacenada dentro de la infraestructura del servicio.

b) **Administrador del servicio de correo electrónico institucional:** Es la unidad de organización de tecnologías de la información o la que haga sus veces en la entidad pública, responsable de la configuración, mantenimiento, soporte, operación y monitoreo del servicio de correo electrónico institucional. Asimismo, es responsable de gestionar el ciclo de vida de las cuentas de correo electrónico institucional (en adelante, el administrador del servicio).

c) **Autenticación adaptativa:** Método de autenticación dinámica que valida el acceso del usuario basándose en el análisis de su perfil de riesgo y el contexto de la conexión (tales como ubicación geográfica, tipo de dispositivo, dirección IP, comportamiento histórico, etc.). Este enfoque permite ajustar el nivel de exigencia de seguridad en tiempo real, permitiendo la persistencia de la sesión en contextos de confianza y solicitando factores adicionales únicamente ante la detección de anomalías o riesgos potenciales, optimizando así la experiencia del usuario.

d) **Autenticación de múltiples factores**: Mecanismo de seguridad que requiere la presentación de dos o más factores (evidencias) de autenticación independientes para verificar la identidad de un usuario. Estos factores se clasifican generalmente en: algo que el usuario sabe (p.ej. contraseña), algo que el usuario tiene (p.ej. teléfono inteligente, token físico), y algo que el usuario es (p.ej. biometría).

e) **Buzón de correo electrónico:** Espacio lógico de almacenamiento en línea asociado a una cuenta de correo electrónico específica, destinado a la gestión de los mensajes de correo electrónico enviados, recibidos, entre otros estados. Su capacidad está sujeta a cuotas de almacenamiento definidas por el administrador del servicio.

f) **Cliente de correo electrónico:** Software que permite gestionar (redactar, enviar, recibir y organizar) mensajes de correo electrónico. Puede ser una aplicación instalada en un dispositivo (computadora de escritorio, tablet o teléfono inteligente) o una aplicación web utilizada a través de un navegador (Webmail) para conectarse al servicio de correo electrónico institucional.

g) **Credencial de acceso**: Es el conjunto de datos, objetos o características biométricas que permiten verificar la identidad de un usuario ante el servicio de correo electrónico institucional. Comprende los factores de conocimiento (p.ej. contraseñas, PIN), los factores de posesión (p.ej. tokens, dispositivos móviles) y de inherencia (p.ej. huella digital, reconocimiento facial).

h) **Cuenta de correo electrónico institucional:** Activo digital asignado por la entidad pública a un titular que lo faculta para utilizar el servicio de correo electrónico institucional para el cumplimiento de sus funciones. Se accede con una credencial de acceso y tiene vinculado un buzón de correo electrónico para su gestión.

i) **Cuenta nominal:** Cuenta asignada de forma personal e intransferible a una persona natural con vínculo institucional vigente. En este tipo de cuenta, el titular y el usuario son la misma persona.

j) **Cuenta funcional:** Cuenta destinada a servicios, unidades orgánicas, sistemas automatizados o personas sin vínculo institucional, que debe contar con un titular institucional responsable y uno o más usuarios autorizados.

k) **Dirección de correo electrónico:** Cadena de caracteres única e irrepetible con formato estandarizado "identificador@nombrededominio" cuya función es el enrutamiento de los mensajes de correo electrónico. Permite la identificación del remitente o destinatario y asegura que los mensajes sean dirigidos al buzón de correo electrónico correspondiente.

l) **Mensaje de correo electrónico:** Unidad de información enviada o recibida por medio de un servicio de correo electrónico, ya sea que se encuentre almacenado de forma centralizada en el buzón de correo electrónico (en línea) o haya sido trasladado a un medio de almacenamiento local (fuera de línea). Presenta una estructura estandarizada compuesta por:

- Metadatos (Cabecera): Datos que permiten la trazabilidad y validación técnica del mensaje, comprendiendo marcas de tiempo, identificadores de mensaje, ruta de servidores intermediarios y, en los casos en que resulte técnicamente viable, la dirección IP de origen del dispositivo remitente, entre otros.

- Contenido (Cuerpo): Información principal del mensaje, que incluye el texto, ficheros adjuntos y cualquier otro elemento anexo.

m) **Nombre de dominio:** Cadena de caracteres de estructura jerárquica que identifica a la entidad pública en Internet y que se traduce, mediante el DNS, en direcciones IP. El nombre de dominio se constituye en un activo digital de la entidad pública.

Por ejemplo: pcm.gob.pe, minsa.gob.pe, unmsm.edu.pe, bn.com.pe, etc.

n) **Servicio de correo electrónico institucional:** Conjunto de recursos tecnológicos destinados a la gestión, transporte y entrega de mensajes de correo electrónico. Es provisto por la entidad pública, y se constituye como un activo digital, servicio digital y canal oficial de comunicación interna y externa de la entidad pública.

o) **Sistemas de negocio:** Conjunto de aplicaciones informáticas, servicios digitales o plataformas tecnológicas (sean de escritorio, móviles, web o híbridas) implementadas con el propósito principal de soportar el flujo de trabajo y la gestión de información de los procesos misionales, de apoyo y estratégicos de una entidad pública.

p) **Spam:** Correo electrónico con fines publicitarios, masivos o de contenido no solicitado que satura el servicio de correo electrónico institucional y eleva los riesgos de seguridad de la información, incluyendo mensajes con fines de suplantación de identidad (phishing) o difusión de software malicioso.

q) **Titular de una cuenta de correo electrónico institucional:** Es la persona natural que mantiene un vínculo institucional con la entidad pública y a quien se le atribuye y vincula objetivamente con los mensajes de correo electrónico enviados, así como con la gestión de la información recibida mediante la cuenta de correo electrónico institucional, en cumplimiento de sus funciones, inclusive tras su cese en la entidad pública respecto de las acciones realizadas durante la vigencia del referido vínculo. Actúa como poseedor de la información institucional de naturaleza pública contenida en la referida cuenta a efectos de lo dispuesto en la normativa de transparencia y acceso a la información pública (en adelante, el titular).

r) **Usuario de una cuenta de correo electrónico institucional:** Es la persona natural a quien se le asigna la gestión operativa del buzón de una cuenta de correo electrónico institucional. Puede o no tener un vínculo institucional con la entidad pública (en adelante, el usuario).

s) **Vínculo institucional:** Relación jurídica, académica, laboral, contractual, de designación oficial o de otra naturaleza autorizada que une a una persona con la UNAP y habilita la titularidad o uso de cuentas institucionales, según corresponda.

VII. RESPONSABILIDADES

Los actores vinculados con el servicio de correo electrónico institucional deben cumplir obligatoriamente las siguientes responsabilidades:

7.1. Responsabilidad de la máxima autoridad administrativa.

a) Garantizar la implementación y cumplimiento de la presente Directiva a nivel institucional.

b) Aprobar y/o modificar el documento normativo institucional para la gestión, operación, supervisión y uso seguro del servicio de correo electrónico institucional, asegurando su alineación con la presente Directiva.

c) Disponer que el servicio de correo electrónico institucional forme parte del SGSI de la entidad pública, garantizando su gestión como un activo digital bajo un enfoque integral basado en riesgos, de conformidad con la normativa vigente en materia de seguridad y confianza digital.

d) Gestionar los recursos necesarios para la implementación, operación y mantenimiento del servicio de correo electrónico institucional.

7.2. Responsabilidad de la Oficina de Tecnologías de la Información como administrador del servicio de correo electrónico institucional

7.2.1. En materia de gestión del servicio de correo electrónico institucional

a) Elaborar y proponer el documento normativo institucional sobre la gestión, operación, seguridad y uso del servicio de correo electrónico institucional conforme con la política de seguridad de la información de la entidad, la presente Directiva y la regulación en materia de gobierno, confianza y transformación digital.

b) Evaluar y determinar el servicio de correo electrónico institucional a utilizar en la entidad, priorizando la disponibilidad y escalabilidad, considerando los niveles de servicio, establecidos en los SLA, ofrecidos por los proveedores o las capacidades técnicas de la infraestructura tecnológica propia. El servicio puede basarse en la adquisición, suscripción o implementación de una solución licenciada o de código abierto.

c) Gestionar la configuración de los permisos y niveles de acceso de los usuarios del servicio de correo electrónico institucional, de acuerdo con sus funciones, cargo, roles y el principio de privilegios mínimos.

d) Implementar mecanismos técnicos de autenticación para las cuentas de correo electrónico institucional funcional con múltiples usuarios que permitan identificar de forma unívoca a la persona natural que realiza cada acción, asegurando la integridad de los registros de auditoría.

e) Brindar el soporte técnico para la provisión segura del servicio de correo electrónico institucional, la atención de incidentes, la creación de las copias de respaldo de la cuenta de correo electrónico institucional, entre otros.

f) Determinar los límites de cantidad y tamaño permitido para los mensajes de correo electrónico enviados y recibidos, así como las cuotas de almacenamiento de las cuentas de correo electrónico institucional, en función de la capacidad de la infraestructura tecnológica y las necesidades de la entidad pública.

g) Gestionar el ciclo de vida de las cuentas de correo electrónico institucional, que comprenda su alta, asignación, modificación, suspensión, baja, entre otros.

h) Ejecutar la baja inmediata o suspensión de las cuentas de correo electrónico nominales por término del vínculo institucional, fallecimiento del titular, mandato judicial o administrativo, o cuando se identifiquen riesgos inminentes a la seguridad digital de la entidad pública.

i) Realizar revisiones anuales de las cuentas de correo electrónico funcionales para verificar su vigencia, la actualización de los responsables titular y usuarios) de su gestión y operación, y la pertinencia de los accesos autorizados.

j) Coordinar con el ODP de la entidad todo aspecto relacionado al tratamiento de datos personales en el servicio de correo electrónico institucional.

k) Capacitar al personal de la entidad pública sobre el uso seguro y ético del servicio de correo electrónico institucional, como mínimo una (1) vez al año o según lo establecido en el plan de desarrollo de personas de la entidad pública.

7.2.2. En materia de seguridad digital

a) Gestionar las políticas de seguridad perimetral del servicio de correo electrónico institucional, incluyendo controles antispam, antimalware, mecanismos de protección orientados a la detección y bloqueo de enlaces maliciosos, análisis de ficheros adjuntos y contenidos potencialmente riesgosos, detección de intentos de suplantación de identidad institucional y de sus usuarios, fraude electrónico y uso indebido de dominios institucionales, identificación de patrones anómalos de comportamiento, incluyendo envíos masivos no habituales, creación de reglas de reenvío no autorizadas, accesos inusuales y otras actividades que puedan evidenciar el compromiso de las cuentas de correo electrónico institucional.

b) Implementar los protocolos de autenticación de correo SPF, DKIM y DMARC para el nombre de dominio institucional, asegurando que la política DMARC progrese de manera obligatoria hacia niveles estrictos de mitigación (quarantine o reject).

c) Monitorear y gestionar la reputación del dominio institucional y de sus direcciones IP en las listas de bloqueo global (blacklists), actuando de manera inmediata frente a reportes de incidentes o falsos positivos para garantizar la correcta entrega de los mensajes y minimizar su filtrado o eliminación por receptores externos.

d) Implementar controles de seguridad de la información en función de la evaluación de riesgos de la entidad, para garantizar la confidencialidad, integridad y disponibilidad del servicio de correo electrónico institucional, en coordinación con el OSCD de la entidad.

e) Utilizar obligatoriamente protocolos seguros de comunicación y cifrado de transporte (como TLS 1.2 o superior) para el acceso y tránsito de los mensajes, restringiendo el uso de suites de cifrado obsoletas o vulnerables,

así como deshabilitar de manera permanente el acceso a través de los protocolos IMAP y POP en sus versiones inseguras, garantizando la integridad y confidencialidad de las comunicaciones desde el origen hasta el servidor de destino.

f) Implementar y administrar mecanismos de cifrado de mensajes a nivel de plataforma (tales como el cifrado automático por reglas de contenido o mediante pasarelas de correo seguro) para proteger comunicaciones con información sensible, confidencial, secreta o reservada; asegurando que el acceso al contenido cifrado sea gestionado de manera centralizada y transparente para el usuario del servicio de correo electrónico institucional.

g) Implementar mecanismos de autenticación de múltiples factores bajo un enfoque de autenticación adaptativa para el acceso al servicio de correo electrónico institucional desde redes externas.

h) Asegurar la disponibilidad y continuidad del servicio de correo electrónico institucional a fin de facilitar el acceso y la conservación de la información de las cuentas de correo electrónico institucional.

i) Crear copias de respaldo de las cuentas de correo electrónico institucional en formatos estándar, abiertos e interoperables, priorizando una periodicidad diaria, y mínima mensual, conforme a las políticas de seguridad de la información de la entidad, en función de las capacidades tecnológicas y presupuestales de la entidad.

j) Establecer y aplicar lineamientos de seguridad para el acceso desde dispositivos móviles al servicio de correo electrónico institucional, incluyendo medidas en caso de pérdida o robo del dispositivo.

k) Establecer límites para el número de destinatarios de mensajes (internos y externos) y la cantidad de mensajes enviados por día, así como restricciones para el envío de correos masivos, a fin de prevenir el uso del servicio de correo electrónico institucional para fines de spam y proteger la reputación del dominio institucional.

l) Implementar y conservar registros de auditoría (logs) que permitan la detección, investigación y respuesta ante incidentes de seguridad digital, debiendo registrarse como mínimo: (i) autenticaciones exitosas y fallidas; (ii) creación o modificación de reglas de reenvío y filtrado; (iii) patrones de envío anómalos o masivos; y (iv) cambios en los privilegios de administración. La conservación de estos registros debe sujetarse a los plazos establecidos por la norma vigente en materia de seguridad digital.

m) Integrar el servicio de correo electrónico institucional a una plataforma de monitoreo para identificar eventos de seguridad, asegurando su registro, categorización y atención oportuna conforme a los protocolos de respuesta a incidentes de seguridad de la entidad pública.

n) Definir, establecer y monitorear los RTO y RPO del servicio de correo electrónico institucional, a fin de garantizar su recuperación y la integridad de los mensajes de correo electrónico ante contingencias o desastres.

o) Mantener un inventario actualizado del dominio y subdominios utilizados en el servicio de correo electrónico institucional, así como de las cuentas de correo electrónico funcionales de la entidad.

p) Aplicar políticas de contraseñas robustas, mecanismos de protección de credenciales y controles que reduzcan el riesgo de compromiso de las cuentas de correo electrónico institucional.

q) Efectuar revisiones periódicas de las cuentas de correo electrónico institucional nominales o funcionales, inactivas, huérfanas o que presenten niveles de riesgo elevados, u otros.

7.3. Responsabilidad del Oficial de Seguridad y Confianza Digital

Además de las funciones y responsabilidades establecidas en la Resolución Rectoral que formaliza su designación, el/la Oficial de Seguridad y Confianza Digital (OSCD) tiene a su cargo las siguientes responsabilidades:

a) Coordinar la identificación y evaluación de los riesgos de seguridad digital asociados al servicio de correo electrónico institucional.

b) Coordinar la implementación de controles de seguridad de la información referentes al servicio de correo electrónico institucional.

c) Coordinar la respuesta ante incidentes de seguridad digital vinculados al servicio de correo electrónico institucional.

d) Supervisar que la configuración y el uso del servicio de correo electrónico institucional cumplan con los estándares y normas de seguridad y confianza digital, realizando revisiones periódicas sobre los niveles de cumplimiento.

e) Coordinar el establecimiento de los lineamientos para el registro y monitoreo de registros de auditoría (logs), así como la revisión periódica de los privilegios y accesos otorgados.

f) Proponer e impulsar la implementación de medidas de prevención contra la fuga de información.

g) Coordinar acciones de capacitación y sensibilización para los usuarios de las cuentas de correo electrónico institucional sobre el uso seguro del correo electrónico y la prevención de riesgos digitales.

h) Validar que la estrategia de continuidad del servicio de correo electrónico institucional esté alineada con los planes de continuidad operativa y de seguridad digital de la entidad.

7.4. Responsabilidad de los titulares de las cuentas de correo electrónico institucional

a) Utilizar su cuenta de correo electrónico institucional para las comunicaciones y coordinaciones en la entidad, hacia y con otras entidades públicas, ciudadanos y personas en general, en el ejercicio de sus funciones.

b) No utilizar el servicio de correo electrónico institucional como sustituto de los canales o sistemas de negocio formalmente establecidos para la tramitación y formalización de actos o decisiones que, por su naturaleza o normativa vigente, deban ser gestionados a través de estos.

c) Asegurar, en coordinación con el administrador del servicio, la disponibilidad de la información de carácter oficial contenida en la cuenta de correo electrónico asignada para su respaldo, especialmente al alcanzar el límite de la cuota de almacenamiento, y al producirse el término o suspensión del vínculo institucional.

d) Realizar la depuración de los mensajes de correo electrónico de naturaleza personal o no oficial, a fin de que la información que la entidad deba conservar corresponda estrictamente a información de carácter oficial producida en cumplimiento de sus funciones, estando prohibido de eliminar o alterarla.

e) Identificar y extraer del buzón de correo electrónico institucional aquellos mensajes de correo electrónico que, por su naturaleza, son parte de una serie documental definida en el PCDA de la entidad pública, para su registro e incorporación en el sistema de negocio correspondiente.

f) El titular o usuario es el único y exclusivo responsable por el sentido y contenido de todos los mensajes emitidos desde su cuenta de correo electrónico institucional, incluyendo aquellos redactados, resumidos o generados, de forma total o parcial, mediante el uso de herramientas de inteligencia artificial.

7.5. Responsabilidad de los usuarios de las cuentas de correo electrónico institucional

a) Resguardar y gestionar las credenciales de acceso a la cuenta de correo electrónico institucional, asegurando su confidencialidad, manteniendo el carácter personal e intransferible de éstas, y aplicando las disposiciones establecidas en el documento normativo institucional sobre la gestión, operación, supervisión y uso seguro del servicio de correo electrónico institucional, asumiendo la responsabilidad por su uso.

b) No utilizar las cuentas de correo electrónico institucional para fines personales o ajenos al ejercicio de sus funciones o actividades, priorizando la protección de la información y evitando el envío de información secreta, reservada o confidencial a personas no autorizadas.

c) Gestionar operativamente el buzón de correo electrónico conforme con el espacio de almacenamiento asignado.

d) Reportar de manera inmediata al CSIRT institucional, o en su defecto al administrador del servicio, y al OSCD, cualquier incidente de seguridad digital o indicio de compromiso de sus credenciales, incluyendo la pérdida o robo de equipos asociados, la suplantación de identidad, la detección de accesos inusuales, intentos de phishing o cualquier otra actividad sospechosa, conforme al procedimiento establecido por la entidad.

e) No eliminar o alterar información de carácter oficial contenida en la cuenta de correo electrónico institucional.

f) Otros que determine la entidad pública.

7.6. Responsabilidad del Comité de Gobierno Digital

Además de las responsabilidades establecidas en la Resolución Rectoral que dispone su conformación, el Comité de Gobierno Digital, integrado por el titular de la entidad o su representante; el/la líder de Gobierno Digital; el/la responsable de la Oficina de Tecnologías de la Información o quien haga sus veces; el/la responsable de la Unidad de Recursos Humanos o quien haga sus veces; el/la responsable de la Secretaría General o quien haga sus veces; el/la oficial de Seguridad de la Información; el/la responsable de la Oficina de Asesoría Jurídica o quien haga sus veces; y el/la responsable de la Oficina de Planeamiento y Presupuesto o quien haga sus veces, tiene las siguientes responsabilidades:

a) Impulsar la alineación de la presente Directiva con las políticas de gobierno, confianza y transformación digital.

b) Evaluar los riesgos institucionales vinculados al servicio y proponer acciones de mejora continua.

c) Coordinar con la OTI y el OSCD la implementación de controles de seguridad, continuidad e interoperabilidad.

d) Supervisar el cumplimiento de los estándares institucionales aplicables al servicio de correo electrónico.

e) Promover la capacitación, sensibilización y cultura de responsabilidad digital en el uso del correo institucional.

7.7. Responsabilidad del Oficial de Datos Personales

Además de las funciones y responsabilidades establecidas en la Resolución Rectoral que formaliza su designación, el/la Oficial de Datos Personales (ODP) tiene a su cargo las siguientes responsabilidades:

a) Orientar a la OTI y a las unidades orgánicas respecto del tratamiento de datos personales realizado mediante el servicio de correo electrónico institucional.

b) Coordinar la atención de riesgos, incidentes o consultas vinculadas a datos personales contenidos en cuentas, mensajes, adjuntos o respaldos.

c) Emitir recomendaciones para asegurar el cumplimiento de la Ley de Protección de Datos Personales y su Reglamento.

d) Participar, cuando corresponda, en la evaluación de acceso, conservación, respaldo, eliminación o transferencia de información que contenga datos personales.

7.8. Responsabilidad de las dependencias y unidades orgánicas

a) Solicitar oportunamente la creación, modificación, renovación, suspensión o baja de cuentas nominales o funcionales bajo su ámbito.
b) Designar titulares institucionales responsables para cuentas funcionales de servicios, sistemas, unidades, proyectos o personas sin vínculo institucional.

c) Verificar la vigencia del vínculo laboral, contractual, académico o funcional de usuarios bajo su dependencia.

d) Garantizar que las cuentas de oficinas, servicios o sistemas se utilicen exclusivamente para fines institucionales.

e) Comunicar a la OTI y al OSCD incidentes, accesos indebidos, usos no autorizados o riesgos vinculados al servicio.

f) Coordinar la entrega, conservación y respaldo de información oficial cuando un titular cesa, cambia de funciones o fallece.

g) Validar anualmente las cuentas funcionales y accesos autorizados bajo su responsabilidad.

7.9. Responsabilidad de las unidades de gestión de personal, abastecimiento y registro académico

a) Proporcionar información actualizada y veraz para la creación, modificación, suspensión y baja de cuentas institucionales.

b) Comunicar en un plazo máximo de 48 horas ingresos, ceses, suspensiones, fallecimientos, cambios de condición, renovaciones o términos contractuales.

c) Mantener consistencia e interoperabilidad con sistemas institucionales de personal, abastecimiento, escalafón y registro académico.

d) Coordinar con la OTI la conservación de respaldos de cuentas de exfuncionarios o exservidores como parte del legajo o vínculo referencial, según corresponda.

e) Informar las fechas de inicio y fin de contratos, órdenes de servicio, modalidades formativas, convenios o autorizaciones que habiliten cuentas temporales.

f) Participar en la depuración de información de cuentas de titulares fallecidos, resguardando la intimidad y datos personales.

7.10. Responsabilidad frente a incidentes y uso indebido

Todo usuario, titular, autoridad o unidad que tome conocimiento de un incidente de seguridad, uso indebido, vulneración, fuga de información o compromiso de credenciales debe comunicarlo de inmediato a la OTI, al OSCD y, cuando corresponda, al CSIRT institucional, siguiendo los canales establecidos.

La atención de incidentes se realizará conforme a procedimientos internos, garantizando trazabilidad, confidencialidad, proporcionalidad y debido proceso.

VIII. DISPOSICIONES GENERALES

8.1. Naturaleza del correo institucional

La cuenta de correo electrónico institucional y la información oficial contenida en ella constituyen activos digitales y herramientas de comunicación y coordinación propiedad de la UNAP. Su asignación constituye una habilitación de uso para fines institucionales y no otorga derecho de propiedad al titular ni al usuario.

La UNAP mantiene la potestad de revocar, suspender, auditar o respaldar las cuentas por necesidades del servicio, término del vínculo institucional, finalización de la causa que motivó su creación o frente a incidentes de seguridad, en cumplimiento de las garantías constitucionales, los procedimientos legales y la normativa de protección de datos personales.

8.2. Carácter oficial de las comunicaciones

Toda comunicación e información institucional vinculada al ejercicio de funciones públicas, actividades académicas, administrativas o de gestión universitaria que se intercambie mediante el correo institucional tiene carácter oficial. Las comunicaciones realizadas con cuentas personales o externas no generan efectos institucionales, salvo autorización expresa y documentada por la autoridad competente.

8.3. Dominio institucional

El servicio de correo electrónico institucional de la UNAP opera bajo el dominio educativo unapiquitos.edu.pe, conforme a la naturaleza de institución educativa pública. La OTI administra los registros DNS y los mecanismos de seguridad del dominio y subdominios autorizados para correo institucional.

Los subdominios específicos derivados del dominio institucional solo podrán utilizarse para cuentas funcionales de sistemas automatizados cuando el volumen estimado de mensajes pueda comprometer la reputación del dominio principal, previa evaluación técnica de la OTI.

8.4. Clasificación y presunción de publicidad de la información

La clasificación de la información contenida en cuentas institucionales se rige por el marco normativo de transparencia, acceso a la información pública y protección de datos

personales. La información oficial contenida en cuentas institucionales se presume pública cuando haya sido creada u obtenida por la UNAP y se encuentre bajo su posesión o control, salvo las excepciones legales de información secreta, reservada, confidencial o protegida por datos personales.

8.5. Mesa de Partes Digital y sistemas de negocio

La cuenta de correo institucional no debe ser utilizada como Mesa de Partes Digital de la UNAP, salvo situación excepcional debidamente justificada y autorizada por la unidad responsable. Los trámites, expedientes, actos administrativos y comunicaciones que deban registrarse en sistemas de negocio o sistemas documentales deberán gestionarse mediante dichos canales.

Cuando la UNAP requiera un canal de recepción documental digital, deberá emplear la Mesa de Partes Digital institucional o las plataformas estatales habilitadas, según corresponda.

8.6. Infraestructura autorizada

El servicio de correo institucional no debe alojarse ni gestionarse en infraestructuras, plataformas o servidores compartidos de web hosting de acceso público masivo. Debe operar sobre infraestructura dedicada, corporativa, gubernamental o provista por un servicio de nube autorizado que garantice seguridad perimetral avanzada, control de acceso, trazabilidad, disponibilidad, respaldo y reputación de las direcciones emisoras.

8.7. Uso obligatorio y responsable

El correo electrónico institucional es el medio oficial y obligatorio para comunicaciones formales de la UNAP, sin perjuicio de otros canales institucionales autorizados. Su uso se rige por los principios de legalidad, responsabilidad digital, seguridad de la información, eficiencia, trazabilidad, protección de datos, conservación documental y buen uso de recursos públicos.

8.8. Sanciones por uso indebido

El incumplimiento de la presente Directiva puede generar suspensión temporal o definitiva de la cuenta, medidas correctivas, responsabilidades administrativas, civiles o penales, y las acciones legales que correspondan, de acuerdo con la gravedad del hecho, el régimen aplicable y el debido proceso.

IX. DISPOSIONES ESPECÍFICAS

9.1. Gestión del servicio y niveles de servicio

La OTI evaluará la solución tecnológica del servicio de correo institucional, sea licenciada, de código abierto, adquirida, suscrita o implementada con infraestructura propia, priorizando disponibilidad, escalabilidad, seguridad, interoperabilidad, continuidad, cumplimiento normativo, reputación del dominio y niveles de servicio. Los SLA del proveedor o de la infraestructura propia deberán ser documentados y monitoreados.

9.2. Creación del Correo Institucional y Asignación.

Las cuentas de correo electrónico institucional pueden ser de dos tipos:

a) **Cuentas nominales:** asignadas de forma personal e intransferible a personas naturales con vínculo institucional vigente. En estas cuentas, el titular y el usuario son la misma persona.

b) **Cuentas funcionales:** destinadas a servicios, sistemas automatizados, unidades orgánicas o personas sin vínculo institucional. Deben contar con titular institucional responsable y usuarios autorizados.

Las cuentas funcionales se clasifican en:

- Para servicios: utilizadas para una función, objetivo, prestación de servicio público, representación de unidad orgánica, oficina, comisión, proyecto, evento o servicio institucional.
- Para sistemas automatizados: utilizadas para envío de mensajes, respuestas automáticas, notificaciones, integración con servicios de software o plataformas institucionales.
- Para personas sin vínculo institucional: utilizadas para consultores, locadores de servicios, personas bajo modalidades formativas o personal externo autorizado. El usuario externo no adquiere titularidad; la titularidad recae en el funcionario o directivo responsable.

El funcionario público, directivo o jefe de unidad orgánica es responsable de solicitar la creación, renovación o baja de cuentas nominales y funcionales correspondientes a su unidad. Toda solicitud debe contener sustento, tipo de cuenta, titular, usuarios autorizados, finalidad, fecha de inicio, fecha de fin cuando corresponda, aceptación de responsabilidades y autorización de la unidad competente.

Las cuentas funcionales para personas sin vínculo institucional tendrán fecha de caducidad automática coincidente con la finalización del servicio, convenio, orden, contrato o actividad que motivó su creación. La OTI podrá generar copia de respaldo de la cuenta, la cual será conservada conforme a la presente Directiva.

La asignación efectiva de cuentas se concreta mediante entrega formal del identificador y credenciales de acceso. La UNAP puede formalizar la aceptación de responsabilidades mediante declaración jurada, acta de entrega o aviso automático de toma de conocimiento en el primer acceso.

a) **Estudiantes.** Todo estudiante se le es asignado automáticamente un correo institucional en el momento que ingresa a estudiar a la universidad. Su acceso al mismo es garantizado mientras sea estudiante de la Universidad.

b) **Egresados.** Todo estudiante egresado de la universidad puede mantener su acceso al correo institucional como manera de promover la formación continua en estudios superiores como talleres y especializaciones que requieren un correo institucional de la universidad de la que se egresó.

c) **Docentes.** Todo docente que se incorpora a la Universidad Nacional de la Amazonía Peruana tiene derecho a un correo electrónico institucional bajo el

dominio unapiquitos.edu.pe. La Oficina de Tecnologías de la Información (OTI) es responsable de la creación y asignación de estas cuentas, una vez que se formaliza el vínculo laboral del docente con la Universidad.
La información oficial sobre la relación de docentes activos es proporcionada por el área de Escalafón, la cual comunica oportunamente a la OTI los datos necesarios para la habilitación del servicio.

d) **Personal administrativo.** Todo personal administrativo tiene acceso a un correo institucional, este se le es asignado al momento que cuenta con un contrato con la Universidad. La información de personal administrativo es proporcionada a la OTI por el área de Escalafón.

9.3. Estructura del Nombre de Usuario e Identificadores.

Los nombres de usuario para los correos institucionales son únicos e irrepetibles, la OTI dispone de reglas específicas para evitar duplicidades y garantizar la correcta identificación de cada cuenta. La estructura del nombre de usuario varía según el rol del miembro de la comunidad universitaria —ya sea estudiante, docente, personal administrativo u otro— con el fin de reflejar adecuadamente su vínculo con la Universidad. A continuación, se detalla la configuración correspondiente para cada caso:

a. Personal Administrativo y Docente

El nombre de usuario institucional asignado al personal administrativo y docente de pregrado se construye siguiendo una estructura estandarizada que facilita la identificación y evita duplicidades. Esta estructura consiste en:

a) Primer nombre, seguido de un punto (.)
b) Primer apellido paterno.
c) Finaliza con el dominio institucional: @unapiquitos.edu.pe.

Ejemplo estándar: juan.villanueva@unapiquitos.edu.pe.

En caso de que el nombre de usuario ya exista, se añade como medida adicional las cuatro primeras letras del apellido materno para garantizar la unicidad:

Ejemplo con duplicado: juan.villanuevarosa@unapiquitos.edu.pe
Caso excepcional, si persiste la duplicidad:

- Se recomienda añadir un número correlativo al final del apellido materno: Ejemplo: juan.villanuevarosa1@unapiquitos.edu.pe, juan.villanuevarosa2@unapiquitos.edu.pe

Esta convención permite mantener coherencia en la asignación de cuentas y facilita la administración del sistema por parte de la Oficina de Tecnologías de la Información (OTI).

b. Locadores, consultores y personal externo

El nombre de usuario del locador institucional asignado como personal administrativo y/o docente, tendrá una estructura estandarizada que facilita la identificación y evita duplicados. Esta estructura consiste en:

a) Nombre Predefinido: locador
b) Número correlativo: 01, 02, 03, ...
c) Siglas de la dependencia a la que pertenece.
d) Finaliza con el dominio institucional: @unapiquitos.edu.pe

- Ejemplo estándar: locador01.oti@unapiquitos.edu.pe
- Ejemplo: convenio.ifd01@unapiquitos.edu.pe
- Ejemplo: externo.proyecto01@unapiquitos.edu.pe

c. Estudiantes y Egresados de Pregrado

El nombre de usuario para los estudiantes y egresados de pregrado se compone del código universitario del estudiante, seguido del dominio @unapiquitos.edu.pe . El código universitario es único para cada estudiante, por lo que no existen casos de duplicidad. El estudiante puede tener un correo institucional para cada carrera que estudia por el mismo hecho que el código universitario es irrepetible.

<codigo universitario>@unapiquitos.edu.pe

Ejemplo: 2102563@unapiquitos.edu.pe

d. Oficinas, dependencias, servicios y sistemas

La Universidad cuenta con muchas oficinas y dependencias, tanto administrativas como de las mismas facultades.

- **Decanato de facultades**
  El nombre de usuario se compondrá de la palabra decanato seguida de un punto y las siglas de la facultad, seguido del dominio @unapiquitos.edu.pe .

  decanato.<siglas de la facultad>@unapiquitos.edu.pe
  Ejemplo: decanato.fisi@unapiquitos.edu.pe

- **Unidades de Investigación de facultades**
  El nombre de usuario se compondrá de la abreviatura *dui* seguida de un punto y de la palabra más usada para describir a una facultad (p. ej., *sistemas* para la Facultad de Sistemas e Informática, *educacion* para la Facultad de Ciencias de la Educación y Humanidades, etc.).

  dui.<facultad>@unapiquitos.edu.pe
  Ejemplo: dui.sistemas@unapiquitos.edu.pe

- **Direcciones de escuela de facultades**
  El nombre de usuario se compondrá de la abreviatura *des* seguida de un punto y de la palabra más usada para describir a una facultad.

  des.<facultad>@unapiquitos.edu.pe
  Ejemplo: des.sistemas@unapiquitos.edu.pe

e. Mesa de partes

Se aplica tanto para las facultades como oficinas administrativas. El nombre de usuario se compondrá de las abreviaturas *mp* seguido de un punto y de las siglas de la oficina o facultad.

mp.<abreviatura de facultad u oficina>@unapiquitos.edu.pe
Ejemplo: mp.fisi@unapiquitos.edu.pe , mp.ogc@unapiquitos.edu.pe

f. Oficinas y Unidades

Si el nombre de la oficina/unidad se compone de una o dos palabras (p. ej. Oficina de Imagen Institucional, Oficina de Admisión, Oficina de Abastecimiento), el nombre de usuario se compondrá de la primera palabra del nombre de la oficina (admisión, abastecimiento, imagen) seguido del dominio @unapiquitos.edu.pe

<primera palabra del nombre de la oficina>@unapiquitos.edu.pe
Ejemplo: admision@unapiquitos.edu.pe

En el caso de que la oficina/unidad tenga un nombre extenso, el nombre de usuario se compondrá de las siglas de la oficina/unidad seguido del dominio @unapiquitos.edu.pe . Si se trata de una oficina/unidad de una facultad, el nombre de usuario se compondrá de las siglas de la oficina/unidad, seguido de un punto y de las siglas de la facultad seguido del dominio @unapiquitos.edu.pe .

<siglas de la oficina>@unapiquitos.edu.pe
Ejemplo: usa.dbu@unapiquitos.edu.pe

g. Sistemas automatizados

Ejemplo: notificaciones.siga@unapiquitos.edu.pe

h. Personal de organizaciones externas

Personas ajenas a la universidad pertenecientes a organizaciones externas que se encuentren colaborando con la universidad, pueden solicitar un correo institucional. Este correo tiene una validez de forma temporal mientras el convenio/colaboración dure con la organización externa. Se pueden aplicar excepciones que modifiquen la temporalidad del correo, dependiendo de la situación.

El nombre de usuario se compondrá de las siglas del nombre de la organización/convenio, seguido de un punto y del primer nombre y apellido del personal. Si existe un usuario ya con ese nombre, se agregarán las cuatro primeras letras del apellido materno del personal.

<siglas de la organización>.<primer nombre del trabajador><primer apellido del trabajador>@unapiquitos.edu.pe
Ejemplo. ifd.carlosgonzales@unapiquitos.edu.pe

9.4. Las Contraseña, MFA y credenciales

Al momento de la creación de la cuenta, la OTI asigna una contraseña temporal al usuario que permite el acceso inicial al servicio. Esta contraseña debe ser cambiada de forma obligatoria tras el primer inicio de sesión. Esta contraseña debe ser modificada obligatoriamente en el primer inicio de sesión, como medida de seguridad básica.

Queda prohibido compartir contraseñas, códigos de segundo factor, tokens, sesiones o cualquier mecanismo de autenticación.

Las contraseñas deberán cumplir, como mínimo, con longitud de ocho caracteres, combinación de letras mayúsculas y minúsculas, números y símbolos, evitando datos personales evidentes. La OTI podrá elevar estos requisitos de acuerdo con la evaluación de riesgos y recomendaciones del OSCD.

El cambio de contraseña se realizará cuando exista indicio de compromiso, a solicitud del titular, por política institucional o como mínimo cada tres meses, salvo que se adopten mecanismos equivalentes de autenticación adaptativa y MFA validados por la OTI y el OSCD.

La MFA será obligatoria para administradores, titulares y usuarios con acceso a información crítica, cuentas funcionales sensibles, accesos desde redes externas y, progresivamente, para todos los usuarios del servicio.
En caso de olvido o pérdida de la contraseña, el usuario podrá solicitar su restablecimiento a través de los canales oficiales de la OTI (WhatsApp institucional o correo electrónico de soporte). Para validar su identidad como titular legítimo de la cuenta, deberá proporcionar la siguiente información:

a. Nombre completo.
b. Número de DNI o código universitario.
c. Información adicional según el perfil:
    - Estudiantes: nombre de la carrera profesional.
    - Docentes: facultad a la que pertenecen.
    - Personal administrativo o externo: nombre de la unidad u organización.

Una vez validada la identidad, la OTI procederá con el restablecimiento de la contraseña y notificará al usuario por el mismo canal de contacto.

Mientras el usuario tenga acceso al servicio podrá modificar la contraseña de su usuario la veces que lo considere necesario, a través de la configuración de su cuenta.

La OTI recomienda el uso de contraseñas seguras, que sean difíciles de adivinar por terceros malintencionados, pero fáciles de recordar para el usuario. Una contraseña segura debe cumplir con los siguientes criterios:

1. Incluir letras mayúsculas y minúsculas
2. mínimo 8 caracteres
3. Incorporar números y símbolos especiales
4. Evitar el uso de datos personales evidentes (fechas de nacimiento, nombres propios, etc.)

Una estrategia útil consiste en elegir una palabra significativa para el usuario y combinarla con caracteres especiales y números para fortalecerla.

Por motivos de seguridad, se establece como requisito mínimo el cambio de contraseña cada tres meses.

9.5. Soporte en el Manejo y Acceso.

La OTI cuenta con canales de soporte al usuario, que son un número de WhatsApp, el cual es el 975 770 258, y un correo de soporte: soporte@unapiquitos.edu.pe , al que cualquier usuario puede comunicarse para solicitar ayuda en el manejo del correo institucional. La OTI puede dar respuesta hasta en un máximo de tres días mediante el canal del correo.

Los canales mencionados también pueden emplearse para solicitar apoyo en el restablecimiento de la contraseña para acceder al servicio. El usuario debe identificarse para poder ser atendido:

a. **Estudiantes o egresados:** indicando su nombre completo o código universitario.
b. **Personal administrativo y/o docentes:** indicando su nombre completo o DNI.

Los correos reportados a la OTI se registrarán en el sistema de gestión de incidentes con la finalidad de llevar un control, hacer seguimiento y generar reportes.

9.6. Uso incorrecto del correo electrónico institucional

Se consideran uso inadecuado o mal uso de la cuenta de correo electrónico institucional y, por lo tanto, está prohibido para su titular o usuario, las siguientes acciones:

9.6.1. Del mal uso de la cuenta de correo electrónico institucional

a. Compartir, facilitar, ceder u ofrecer la cuenta, buzón o credenciales de acceso (tales como contraseñas, códigos de segundo factor, entre otros) del correo electrónico institucional a terceras personas.

b. Utilizar la cuenta de correo electrónico institucional para fines personales, fraudulentos, comerciales, publicitarios, lucrativos u otros ajenos a la función pública y/u objetivos de la institución.

c. Utilizar identidades ficticias o cuentas pertenecientes a otros titulares para el envío de mensajes, así como manipular las cabeceras del mensaje para ocultar o modificar la identidad del remitente.

d. Utilizar cualquier otra cuenta de correo electrónico institucional que no sea la asignada formalmente al titular o usuario.

9.6.2. Del contenido de los mensajes y la conducta ética

a. Enviar o redistribuir mensajes de correo electrónico con contenidos impropios, obscenos, que atenten contra el honor, la reputación de las personas, las buenas costumbres o que contengan rumores, chismes y bromas que puedan afectar el clima institucional u ofender o avergonzar a terceros.

b. Intimidar, insultar, hostilizar o acosar a otros usuarios, titulares o ciudadanos.

c. Realizar propaganda política o distribuir material de actividades partidarias de elecciones externas ajenas a los fines de la entidad.

d. Enviar o redistribuir ficheros (música, videos, software) que violen la normativa vigente sobre derechos de autor o compartir claves ilegales de software.

9.6.3. De la seguridad digital

a. Enviar o redistribuir información confidencial, secreta, reservada o cualquier documento institucional a destinatarios no autorizados, ajenos a la entidad o con fines ajenos a su función, salvo autorización expresa.

b. Distribuir de manera intencionada spam, malware, virus, esquemas de enriquecimiento piramidal (hoax) o participar en cualquier fase de ataques de phishing o estafas.

c. Utilizar la cuenta de correo electrónico institucional para registrarse en redes sociales, sitios de compras, plataformas de apuestas, foros de entretenimiento o cualquier plataforma digital no relacionada con la función pública o de terceros no autorizada por la entidad.

d. Exceder los límites de frecuencia, cantidad y tamaño establecidos por el administrador del servicio para el envío de mensajes (incluyendo sus ficheros adjuntos), de forma que se sature o ponga en riesgo la operatividad de la infraestructura tecnológica institucional; así como, el uso de servicios de transferencia de ficheros no autorizados.

e. Interactuar de manera negligente con ficheros adjuntos o enlaces sospechosos que puedan facilitar ataques de phishing o comprometer la seguridad de la red institucional.

9.2.4. Del uso en la comisión de delitos

Almacenar, enviar o recibir material relacionado con la explotación sexual, pornografía, apología al terrorismo, delitos informáticos, estafas o cualquier otra actividad tipificada como delito.

Toda comunicación realizada por este medio tiene carácter confidencial, por lo que el usuario debe configurar en los ajustes de su correo, el siguiente aviso de confidencialidad para que sea insertado de forma automática en todo correo que envíe:

"Aviso de confidencialidad": Esta transmisión de correo electrónico, y cualquier documento, archivo o mensaje de correo electrónico anterior adjunto a ella, pueden contener información confidencial y / o privilegiada y pueden estar legalmente protegidos contra la divulgación. Cualquier revisión, uso, divulgación o distribución no autorizada está estrictamente prohibida. Si usted no es el

destinatario previsto, o una persona responsable de entregarlo al destinatario previsto, comuníquese con el remitente por correo electrónico de respuesta y destruya todas las copias del mensaje original, incluidos los archivos adjuntos."

El usuario no puede delegar el uso de su cuenta de correo a un tercero. La delegación se produce cuando el propietario de una cuenta de correo electrónico (el "delegador") concede permisos a otro usuario ("el delegado") para acceder al correo electrónico, el calendario y/o los contactos del propietario. La delegación no está permitida compartiendo contraseñas o iniciando sesión en la cuenta para que la use el delegado: el delegado debe usar su propia cuenta.

9.7. Suspensión, restricción y cese del uso del servicio.

El servicio de correo institucional brindado por la universidad a sus miembros puede cesar de manera voluntaria, por finalización del vínculo laboral entre el trabajador y la Universidad, o por el incumplimiento de alguna normativa del buen uso del servicio.

a) La forma voluntaria puede darse cuando el usuario, de forma explícita, comunica su intención de dejar de usar el servicio.

b) Por el no uso de la cuenta en un tiempo aproximado de 3 años a más.

c) La finalización o rompimiento del vínculo laboral entre el trabajador y la universidad significa la detención inmediata en el acceso al servicio, impidiendo el acceso al correo institucional de forma inmediata, salvo excepciones aplicables.

d) Incumplir alguna regla sobre el buen uso del correo institucional deriva en la suspensión inmediata del acceso para el usuario al servicio, impidiéndole usar el mismo de forma determinada o indeterminada de tiempo.

9.8. Asignación y gestión de cuotas de almacenamiento del correo electrónico institucional.

a) Google ya no ofrece almacenamiento ilimitado y gratuito en Google Workspace for Education; desde 2022–2023 se estableció limite. Debido a las restricciones de Google, la Universidad debe asignar cuotas de almacenamiento a los Gmail institucionales de la UNAP.

b) El uso de almacenamiento del correo electrónico institucional se limita a almacenar y compartir exclusivamente documentos académicos y administrativos de los miembros de la comunidad universitaria.

c) Al compartir archivos vía correo electrónico institucional deberá cumplir estrictamente con las políticas de seguridad, confidencialidad y propiedad intelectual establecidas en la universidad.

d) El espacio o cuotas de almacenamiento en el correo electrónico institucional a los diferentes usuarios de la comunidad universitaria se estable según la siguiente tabla.

CATEGORIA	CANTIDAD
Docente	300 GB
Docente cesado	250 GB
Estudiantes	250 GB
Estudiantes Egresados	100 GB
Administrativos	250 GB
Oficinas	250 GB

e) Los estudiantes egresados de pregrado y posgrado tendrán un plazo de 30 días posterior a la finalización de sus estudios para poder descargar la información de su correo institucional para la reasignación de la cuota de acuerdo con la tabla anterior. Pasado los 30 días según políticas de Google eliminará de manera aleatoria correos, archivos en drive, imágenes, etc. para la reasignación de la cuota.

f) Sea el caso de que OTI detecte que el límite de almacenamiento establecido fue superado se tomarán las siguientes medidas:

- Se notificará al usuario vía email sobre la superación de límite de almacenamiento en su cuenta, solicitándole que reduzca el el volumen de datos almacenados en un plazo de 5 (cinco) días calendarios. Transcurrido el plazo se procederá a verificar si se ha cumplido con la solicitud, si el usuario cumple con lo solicitado se cierra el proceso.

- En caso de que, el usuario haga caso omiso del correo electrónico o de forma excepcional no haya leído los mensajes, se procederá a llamar vía teléfono móvil al usuario para reiterarle la solicitud y explicarle las consecuencias del no cumplimiento; tendrá 3 (tres) días calendario después del reiterativo para cumplir con la solicitud. Transcurrido el plazo se procederá a verificar si se ha cumplido con la solicitud, si el usuario cumple con lo solicitado se cierra el proceso. Caso contrario se procederá a enviar un nuevo email a su correo electrónico institucional o Alternativa.

- En caso de que el usuario no cumpla con lo solicitado vía correo electrónico o llamada telefónica, se procederá a bloquear la cuenta de correo electrónico de forma definitiva hasta que el usuario se comunique por llamada telefónica o de manera presencial, comprometiéndose a reducir el almacenamiento en un plazo máximo de 2 (días) calendarios.

- En consecuencia, si el usuario no cumplió son lo solicitado o el compromiso asumido por el mismo se procederá a eliminar la información de la cuenta de forma unilateral por parte del administrador de Correos de la OTI, sin opción a recuperar dicha información.

9.9. Firma estandarizada en el correo electrónico institucional.

9.9.1. Toda comunicación enviada desde una cuenta de correo electrónico institucional, sea nominal o funcional, debe contar obligatoriamente con una firma estandarizada al final del cuerpo del mensaje cuando se trate de comunicaciones dirigidas a destinatarios externos, ya sea que se realice por medio de un navegador web, aplicaciones de escritorio o dispositivos móviles.

Para el caso de comunicaciones internas la firma estandarizada es opcional.

9.9.2. La firma estandarizada de un mensaje de correo electrónico de una cuenta de correo electrónico nominal debe incluir como mínimo los siguientes datos:

a) Nombre completo del usuario con vínculo institucional de la cuenta de correo electrónico institucional.
b) Cargo, posición o rol.
c) Nombre de la unidad de organización.
d) Nombre de la entidad pública.
e) Número de teléfono y anexo (en caso corresponda).
f) Dirección de la entidad pública.
g) Enlace a la sede digital de la entidad.
h) Logotipo de la entidad.
i) Aviso de confidencialidad institucional.

Ejemplo:
Juan Jocoso Japlindo
Jefe de la Unidad de ...
(63) 111-222
Calle San Marcos N° 185, distrito San Juan Bautista
https://enlinea.unapiquitos.edu.pe

9.9.3. La firma estandarizada de un mensaje de correo electrónico de una cuenta de correo electrónico funcional debe incluir como mínimo los siguientes datos:

a) Nombre o denominación del servicio público, unidad orgánica o sistema automatizado.
b) Nombre de la entidad pública.
c) Dirección de la entidad pública.
d) Enlace a la sede digital de la entidad.
e) Logotipo de la entidad.
f) Aviso de confidencialidad institucional.

Ejemplo:
Juan Jocoso Japlindo
Universidad Nacional de la Amazonía Peruna
Calle San Marcos N° 185, distrito San Juan Bautista
https://enlinea.unapiquitos.edu.pe

9.9.4. La firma estandarizada de un mensaje de correo electrónico establecida en los numerales precedentes constituye una firma electrónica simple, de conformidad con lo dispuesto en el literal a) del artículo 1A del Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM.

9.10. Seguridad de la Información

Los usuarios están obligados a:

- Proteger sus credenciales de acceso.
- Utilizar contraseñas seguras y mecanismos de autenticación establecidos.
- Cerrar sesión en equipos compartidos.
- Reportar inmediatamente incidentes de seguridad, accesos no autorizados o correos sospechosos.

La Universidad implementará controles técnicos y administrativos para garantizar la confidencialidad, integridad y disponibilidad del servicio.

9.11. Vigencia de la cuenta de correo electrónico institucional.

a) **Inicio de vigencia**

La cuenta de correo institucional tendrá vigencia desde el momento de su creación y entrega al titular y/o usuario, garantizando acceso inmediato a los servicios digitales de la universidad.

b) **Docentes y personal administrativo**

Las cuentas permanecerán activas mientras dure el vínculo laboral o contractual con la universidad.

Una vez culminado dicho vínculo, la cuenta será suspendida o restringida en un plazo máximo de quince (15) días hábiles, previa coordinación con la unidad competente para asegurar la entrega, respaldo y conservación de información oficial.

c) **Estudiantes de pregrado y posgrado**

La cuenta se mantiene activa durante toda la etapa académica.

Al egresar, se otorgará un plazo de treinta (30) días calendario para que el usuario identifique, descargue o transfiera información personal o no oficial, sin eliminar ni alterar información oficial que deba conservarse.

Posteriormente, la cuota de almacenamiento podrá ser reducida y la cuenta podrá ser suspendida, conservando la información oficial conforme a la normativa aplicable.

d) **Egresados**

Podrán conservar acceso limitado a su cuenta institucional como parte de la red de egresados, con una cuota reducida de almacenamiento (ejemplo: 100 GB).

e) **Cuentas temporales (locadores, contratados, servicios específicos)**
La vigencia de estas cuentas estará sujeta al período del contrato o servicio. Al culminar el contrato, orden de servicio, convenio o actividad que motivó su creación, la cuenta será suspendida o dada de baja automáticamente, salvo renovación expresa y sustentada por la unidad responsable.

f) **Cuentas inactivas**
Las cuentas que no registren actividad durante tres (3) años consecutivos serán suspendidas por quince (15) días y posteriormente dadas de baja, previa verificación de información oficial y respaldo cuando corresponda.

g) **Oficinas y servicios institucionales**
Las cuentas asignadas a oficinas o servicios permanecerán activas mientras exista la unidad orgánica o el servicio.

En caso de reorganización institucional, la OTI deberá actualizar o dar de baja dichas cuentas haciendo de conocimiento a la Alta dirección.

h) **Notificación y transparencia**
Todo proceso de suspensión, restricción, baja o eliminación de cuentas deberá ser notificado previamente al usuario o a la unidad responsable, cuando corresponda, y registrado por la OTI, preservando la confidencialidad, protección de datos personales y seguridad de la información.

9.12. Registros de auditoría y monitoreo

La OTI implementará y conservará registros de auditoría del servicio de correo institucional para detección, investigación y respuesta ante incidentes. Como mínimo, se registrarán autenticaciones exitosas y fallidas, creación o modificación de reglas de reenvío y filtrado, patrones de envío anómalos o masivos, cambios de privilegios administrativos, altas, bajas, suspensiones, restablecimientos de contraseña y modificaciones de cuentas funcionales.

Los logs se conservarán conforme a la normativa vigente en seguridad digital, políticas del SGSI, disponibilidad tecnológica y requerimientos legales. El acceso a logs estará restringido al personal autorizado, dejando trazabilidad de consulta, extracción o análisis.

9.13. Continuidad, respaldos, RTO y RPO

La OTI garantizará la disponibilidad y continuidad del servicio de correo institucional conforme al Plan de Continuidad Operativa, Plan de Recuperación ante Desastres y SGSI de la UNAP. Los RTO y RPO serán definidos, aprobados, monitoreados y revisados periódicamente, considerando criticidad, capacidades tecnológicas y SLA aplicables.

Los respaldos de cuentas institucionales se generarán en formatos estándar, abiertos e interoperables cuando sea técnicamente viable. La periodicidad prioritaria será diaria y, como mínimo, mensual, en función de capacidades institucionales. La OTI realizará

pruebas periódicas de restauración, verificando integridad, confidencialidad y disponibilidad.

9.14. Acceso desde dispositivos móviles

El acceso desde dispositivos móviles debe realizarse con MFA, bloqueo de pantalla, sistema operativo actualizado, aplicaciones oficiales o autorizadas y protección contra pérdida o robo. En caso de pérdida, robo o sospecha de compromiso de un dispositivo vinculado al correo institucional, el usuario debe reportar inmediatamente a la OTI para revocar sesiones, cambiar credenciales, retirar dispositivos confiables y aplicar borrado remoto cuando sea posible y legalmente procedente.

9.15. Acceso a información pública contenida en cuentas institucionales

El titular de la cuenta es poseedor de la información contenida en ella y, ante una solicitud de acceso a información pública, debe determinar la naturaleza pública de la información oficial de su cuenta nominal y, de ser el caso, de las cuentas funcionales asignadas, evaluando excepciones de transparencia y protección de datos personales, y gestionando su entrega al funcionario responsable de atender la solicitud.

Cuando la solicitud se refiera a cuentas de exfuncionarios o exservidores, la unidad donde ejercieron funciones será poseedora de la información y responsable de evaluar su accesibilidad o inaccesibilidad, con apoyo técnico de la OTI. En caso de unidades extinguidas, fusionadas o modificadas, la evaluación corresponderá a la unidad sucesora o a la que determine la UNAP conforme a su normativa interna.

La OTI brindará facilidades técnicas para acceso, extracción, respaldo y trazabilidad, sin alterar la información original y respetando confidencialidad, protección de datos personales y cadena de custodia cuando corresponda.

9.16. Conservación de información oficial

Durante la vigencia del vínculo institucional, el administrador del servicio conservará la información oficial contenida en cuentas institucionales mediante mecanismos centralizados de respaldo, asegurando disponibilidad, confidencialidad e integridad. El titular o usuario tiene prohibido eliminar o alterar información oficial.

Al término del vínculo institucional, el titular debe depurar información personal o no oficial, entregar la información oficial generada en ejercicio de sus funciones y suscribir una declaración jurada en la que manifieste que la información entregada comprende la totalidad de la información oficial y que la depuración se limitó a información personal o no oficial. La suscripción no exime de responsabilidad por omisiones, alteraciones o eliminaciones indebidas.

La OTI creará la copia de respaldo correspondiente y la información oficial será conservada como parte del legajo o mediante vínculo referencial, durante el periodo establecido por la normativa de legajos, transparencia, archivos o gestión documental aplicable, en coordinación con la unidad de recursos humanos o la unidad competente.

En caso de fallecimiento del titular, la unidad donde ejerció funciones será responsable de entregar la información oficial contenida en la cuenta, coordinando con la OTI la creación de respaldo y con recursos humanos su conservación. La depuración se

realizará con participación de recursos humanos para proteger la intimidad y datos personales del fallecido.
Los mensajes oficiales que formen parte de series documentales definidas en el PCDA deben identificarse, extraerse, registrarse e incorporarse al sistema de negocio o sistema documental correspondiente. Su periodo de conservación será el mismo de la serie documental aplicable. Los documentos preliminares o borradores que no tengan carácter oficial deben ser identificados y excluidos conforme a la normativa de archivos.

9.17. Fiscalización y Control del Correo Institucional.

a) **Supervisión de la Oficina de Tecnologías de la Información (OTI)**
La OTI es responsable de auditar periódicamente las cuentas de correo institucional, verificando el cumplimiento de la presente directiva y de las disposiciones legales y normativas internas.

b) **Autorización de envíos masivos**
Todo envío masivo de correos electrónicos deberá ser previamente autorizado por la OTI y ejecutado únicamente por el Administrador de Correo o personal designado.

Se prohíbe el uso de listas de distribución para fines ajenos a la universidad.

c) **Registro de actividades**
El Administrador de Correo deberá mantener un registro actualizado de la creación, modificación, suspensión y eliminación de cuentas de correo institucional.

Dichos registros estarán disponibles para auditorías internas y externas.

d) **Control de seguridad y contraseñas**
Se fiscalizará el cumplimiento de la política de contraseñas seguras (mínimo 8 caracteres, combinación de letras, números y símbolos).

Los usuarios deberán cambiar su contraseña cuando exista indicio de compromiso, por requerimiento de seguridad o como mínimo cada tres (3) meses, salvo que se adopten mecanismos equivalentes de autenticación adaptativa y MFA validados por la OTI y el OSCD.

La autenticación multifactor será obligatoria para administradores, titulares y usuarios con acceso a información crítica, cuentas funcionales sensibles y accesos desde redes externas, y será implementada progresivamente para todos los usuarios.

e) **Monitoreo de cuentas inactivas**
La OTI realizará controles semestrales para identificar cuentas inactivas.

Las cuentas sin actividad durante tres (3) años serán suspendidas y posteriormente dadas de baja, previa evaluación de la información oficial que deba conservarse.

f) **Auditoría de almacenamiento en la nube**
Se fiscalizará el uso del almacenamiento en Drive, asegurando que se respete la cuota asignada por tipo de usuario.

Se prohíbe almacenar archivos personales ajenos a la gestión académica o administrativa.

g) **Control frente a abuso del correo electrónico**
Se tipifican como infracciones: spam, difusión de contenido ofensivo, phishing, envío masivo no autorizado, uso indebido de listas de distribución.

La OTI podrá suspender temporalmente la cuenta mientras se investiga la infracción.

h) **Sistema de gestión de incidentes**
La universidad implementará un sistema para registrar y dar seguimiento a incidentes relacionados con el correo institucional (ej. accesos indebidos, recepción de correos ofensivos).

Los usuarios deberán ser notificados del estado de sus reportes en un plazo máximo de 24 horas.

i) **Transparencia y rendición de cuentas**
Los resultados de auditorías y controles serán informados a la Alta Dirección de manera consolidada y con las restricciones necesarias para proteger datos personales, información confidencial, seguridad digital y detalles técnicos sensibles. La difusión de información se realizará únicamente cuando corresponda, conforme al marco de transparencia y acceso a la información pública.

II. DISPOSICIONES COMPLEMENTARIAS

Primera. Supervisión y control del servicio

La Universidad, a través del órgano competente en tecnologías de la información, podrá realizar acciones de supervisión, monitoreo y control del servicio de correo electrónico institucional, con la finalidad de garantizar su uso adecuado, la continuidad del servicio y la protección de la información institucional.

El servicio de correo institucional deberá utilizar protocolos y mecanismos de acceso seguros, tales como SMTP, IMAP o POP cuando se encuentren habilitados, mediante conexiones cifradas SSL/TLS o estándares equivalentes, autenticación institucional y controles definidos por la OTI. La habilitación de protocolos de acceso estará sujeta a evaluación de seguridad y necesidad operativa.

Dichas acciones se efectuarán respetando el principio de legalidad, el debido proceso y la normativa vigente sobre protección de datos personales.

Segunda. Auditoría de cuentas institucionales

Las acciones de monitoreo, revisión de metadatos, logs y cumplimiento podrán realizarse de manera periódica para fines de seguridad, continuidad y control. El acceso al contenido de mensajes o buzones solo procederá cuando existan indicios razonables, incidentes de seguridad, requerimiento de autoridad competente o necesidad institucional debidamente sustentada, respetando legalidad, proporcionalidad, trazabilidad y protección de datos personales.

Toda auditoría que implique acceso al contenido del buzón deberá contar con autorización expresa de la máxima autoridad administrativa o de quien haga sus veces, salvo mandato de autoridad competente, dejando constancia documentada de las acciones realizadas.

Tercera. Gestión de incidentes y correos indebidos

Los incidentes relacionados con el servicio de correo electrónico institucional, tales como accesos no autorizados, correos ofensivos, spam, suplantación de identidad o vulneraciones de seguridad, deberán ser reportados de manera inmediata a la unidad responsable del servicio.

La atención de dichos incidentes se realizará conforme a los procedimientos internos de gestión de incidentes de seguridad de la información, garantizando la trazabilidad, confidencialidad y oportunidad de respuesta.

Cuarta. Medidas correctivas y responsabilidades

El incumplimiento de las disposiciones establecidas en la presente Directiva dará lugar a la aplicación de medidas correctivas, administrativas o disciplinarias, de acuerdo con el régimen normativo aplicable, sin perjuicio de las responsabilidades civiles o penales que correspondan.

Las medidas adoptadas deberán ser proporcionales, debidamente motivadas y registradas.

Quinta. Revisión anual de cuentas funcionales

La OTI, en coordinación con las unidades responsables, realizará al menos una revisión anual de cuentas funcionales para verificar vigencia, titularidad, usuarios autorizados, finalidad, accesos y necesidad de continuidad.

Sexta. Cuentas vinculadas a Mesa de Partes o recepción documental

Las cuentas que por denominación o uso se vinculen a recepción de documentos no sustituyen la Mesa de Partes Digital. Solo podrán emplearse de forma excepcional, temporal y documentada cuando exista justificación de la unidad responsable y autorización competente.

Séptima. Actualización normativa

La presente Directiva podrá ser actualizada o modificada cuando se produzcan cambios en la normativa vigente, en la infraestructura tecnológica institucional o en las políticas de gobierno digital, previa evaluación técnica y legal correspondiente.

Octava. Interpretación y casos no previstos

Los casos no previstos serán evaluados por la OTI en coordinación con la Oficina de Asesoría Jurídica, OSCD, ODP, Comité de Gobierno Digital u órgano competente. La interpretación de la Resolución N° 001-2026-PCM/SGTD y de la Directiva N° 001-2026-PCM/SGTD corresponde a la SGTD de la PCM en el marco de su rectoría.

ANEXO 1: SOLICITUD DE CREACION DE CUENTA NOMINAL PARA PERSONAL ADMINISTRATIVO Y DOCENTES

N°	Nombres y Apellidos	DNI	Celular	Correo Personal	Dependencia	Cargo	Condición de contrato*	Fecha de Inicio	Fecha de Fin**

Nota*: En caso la condición sea locación de servicios u otra modalidad temporal, indicar el número de orden de servicio, contrato, convenio o documento habilitante y la fecha de fin. La unidad solicitante debe adjuntar sustento de vínculo institucional y autorización de la jefatura correspondiente.

Declaración: La unidad solicitante confirma que la cuenta nominal será utilizada exclusivamente para fines institucionales y que el usuario recibirá las credenciales de forma personal e intransferible.

Firma de la unidad solicitante: _____ Firma OTI: _____

ANEXO 2: SOLICITUD DE CREACIÓN, MODIFICACIÓN O RENOVACIÓN DE CUENTA FUNCIONAL

N.°	Tipo de cuenta funcional	Titular institucional responsable	DNI	Unidad	Correo alternativo	Identificador propuesto	Finalidad / descripción	Usuarios autorizados	Fecha inicio	Fecha fin

Tipos de cuenta funcional: servicio, sistema automatizado, unidad orgánica, proyecto, evento, convenio o persona sin vínculo institucional. El identificador propuesto no debe contener nombres ni apellidos de personas naturales.

La unidad solicitante declara que ha designado titular institucional responsable, usuarios autorizados, finalidad, fecha de caducidad cuando corresponda y aceptación de responsabilidades por el uso del activo digital.

Firma del titular institucional: _____ Firma OTI: _____

ANEXO 3: SOLICITUD DE SUSPENSIÓN, BAJA O ELIMINACIÓN DE CUENTA INSTITUCIONAL

Fecha: _____

Dependencia: _____

Nombres y apellidos del jefe de área:

_____

Cargo: _____

Cuenta institucional a suspender o dar de baja:

_____

Tipo de cuenta: nominal / funcional / sistema automatizado:

_____

Titular institucional responsable: _____

Usuario o usuarios autorizados: _____

Motivo de la baja o suspensión: _____

Fecha efectiva de baja o suspensión:

_____

Categoría	Marcar (X)
Docente	
Estudiante	
Egresado	
Administrativo	
Locador / externo	
Oficina / servicio	
Sistema automatizado	

Documentos adjuntos: comunicación de cese, término contractual, resolución, informe técnico, acta de entrega de cargo, declaración jurada, solicitud de respaldo u otro sustento.

La OTI verificará la existencia de información oficial y realizará el respaldo correspondiente antes de la eliminación definitiva de la cuenta.

Firma unidad solicitante: _____ Firma OTI: _____

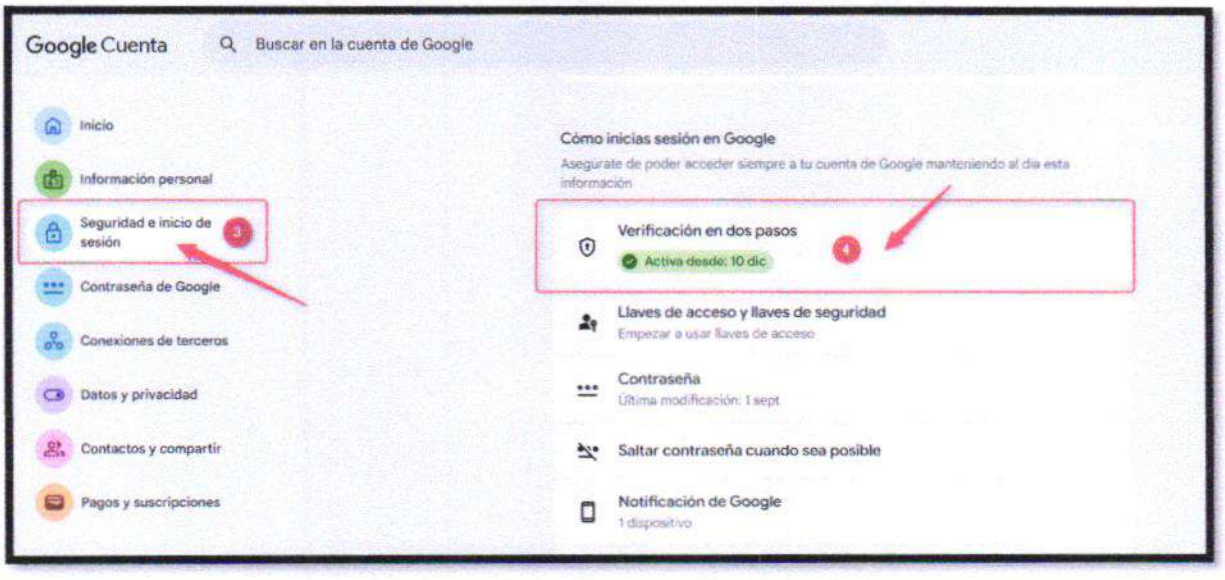
ANEXO 4: GUÍA PARA ACTIVAR LA AUTENTICACIÓN DE MÚLTIPLES FACTORES EN LA CUENTA INSTITUCIONAL (GMAIL)

En esta guía se da a conocer para establecer un nivel alto de seguridad para cuenta de correo institucional y evitar uso de credenciales sin autorización del propio usuario de la cuenta. Teniendo en cuenta reglas básicas para nuestra ciberseguridad.

a) Acceda a su cuenta institucional en una computadora y/o laptop de su confianza.
b) Luego en la parte superior derecha (1) haga click para abrir en panel de perfil de usuario.
c) Seleccione la opción GESTIONAR TU CUENTA DE GOOGLE (2).

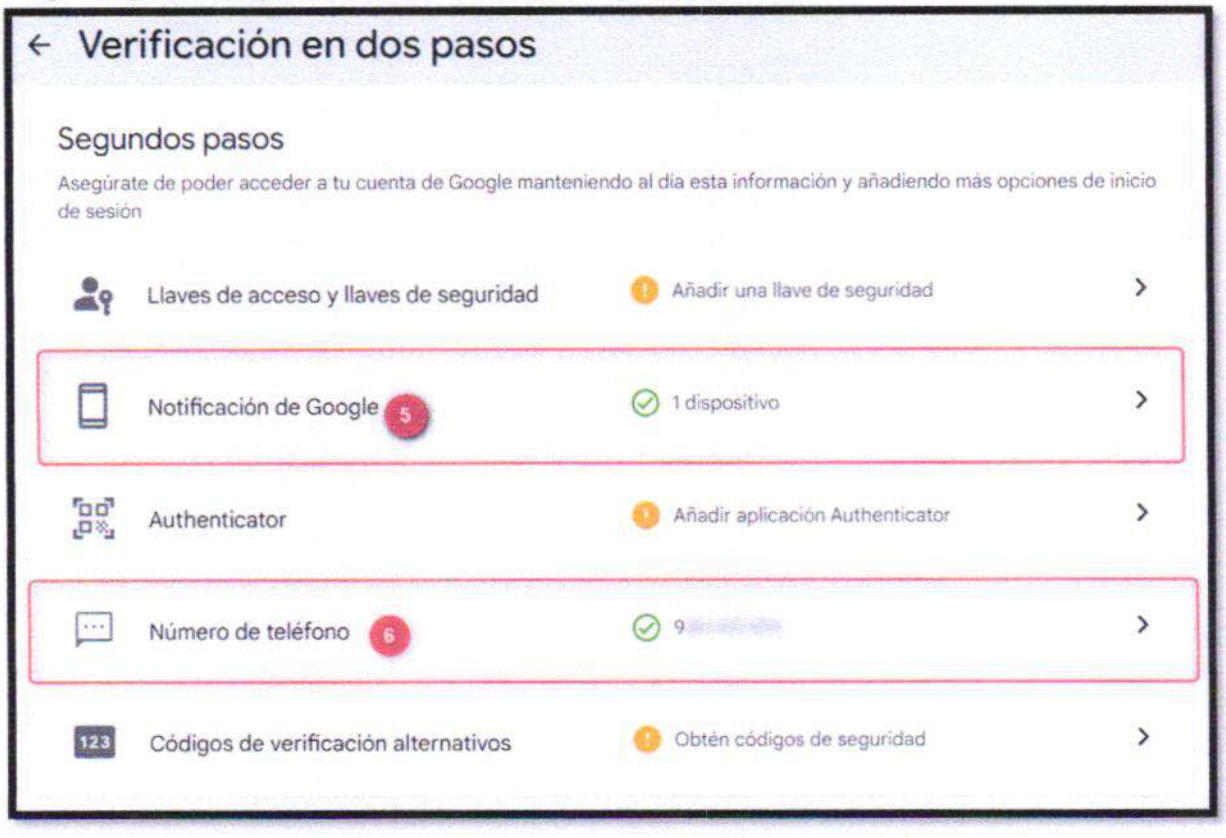


d) Se abrirá una nueva pestaña en el navegador y en la lista de opciones del lado izquierdo seleccionar la opción **Seguridad e Inicio de Sesión (3).**
e) Luego en vista de la página deslizar hacia abajo hasta encontrar el apartado de COMO INICIAS SESION EN GOOGLE, seleccionar la opción **Verificación en dos pasos (4).**



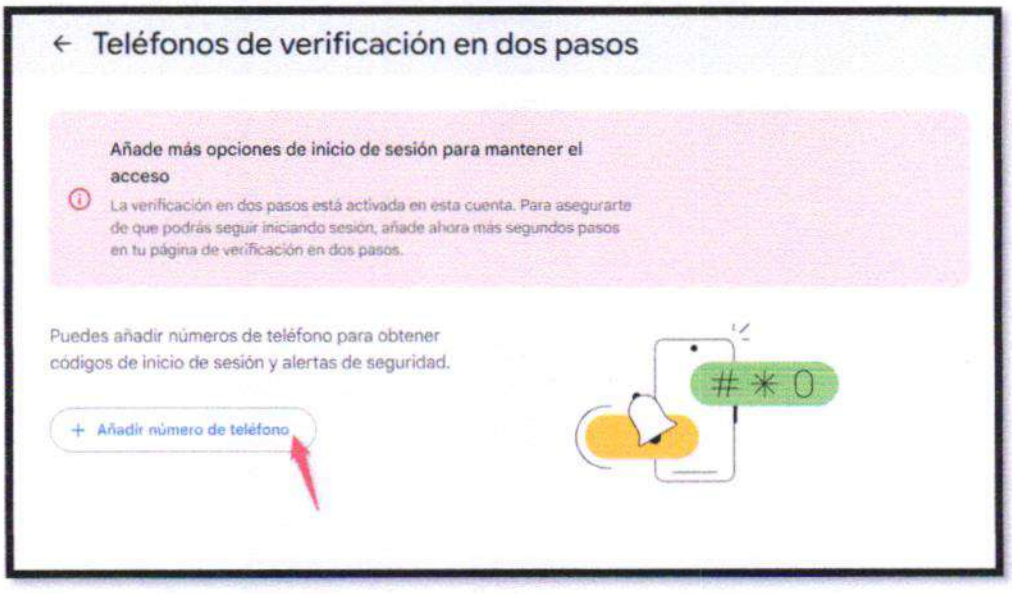
f) Cargará la página de verificación de usuario y será necesario ingresar contraseña de la cuenta institucional.

g) Luego cargará la página de Verificación en dos pasos.

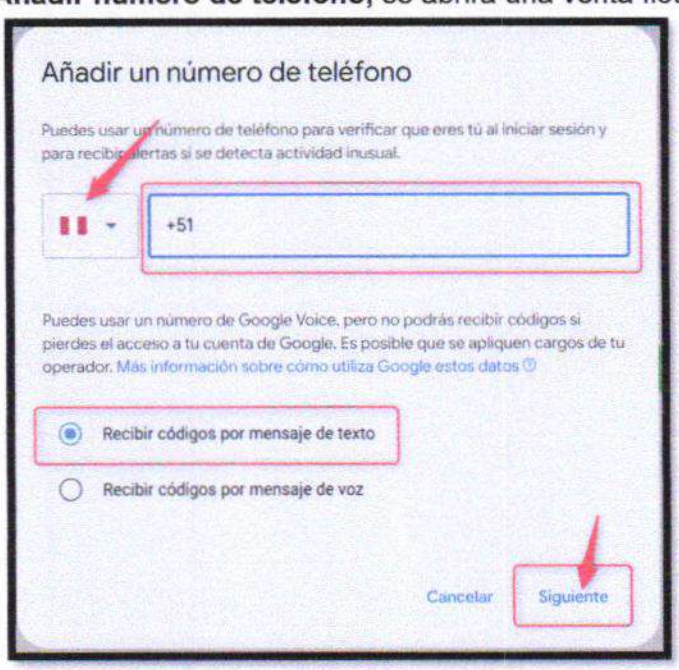


h) Para la activación de **Notificación de Google (5),** será necesario iniciar sesión con la cuenta institucional en un teléfono móvil de uso institucional o personal, una vez iniciado aparecerá en el apartado mencionado.

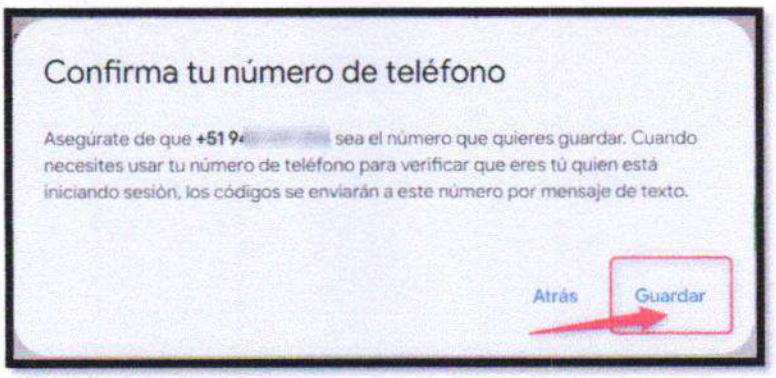
i) **Número de teléfono (6),** hacer click en la opción para agregar el o los número telefónicos que estarán vinculadas a la cuenta institucional.



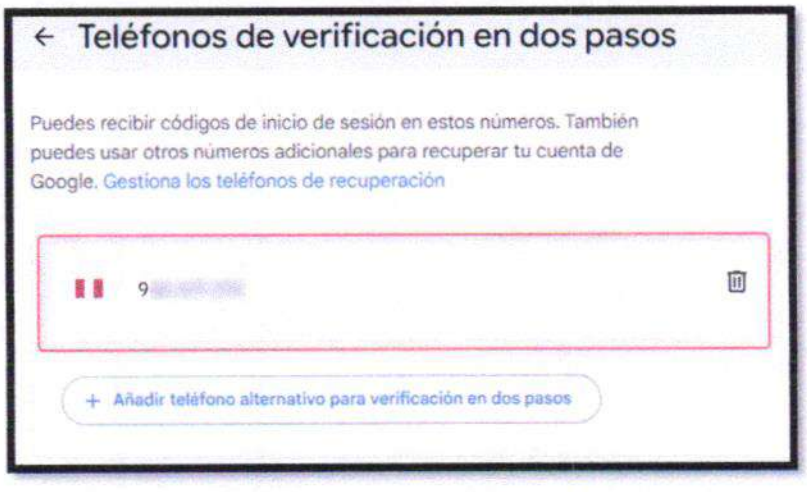
j) Hacer click en **Añadir número de teléfono,** se abrirá una venta flotante.



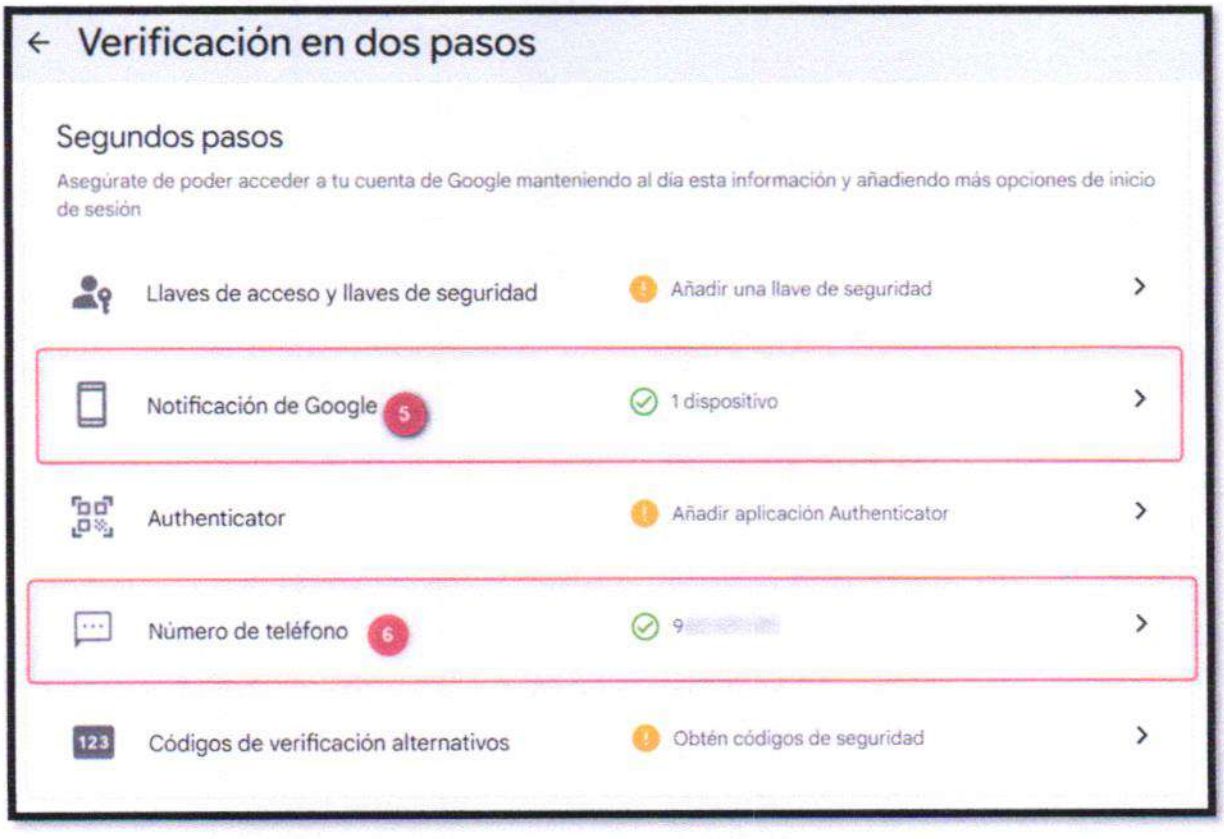
k) Seleccionar el país PERÚ y escribir el número telefónico de uso institucional o personal el cual estará vinculado al correo institucional, verificar que la opción **Recibir códigos por mensaje de texto** este seleccionado. Hacer click en **SIGUIENTE.**



l) Inmediatamente aparecerá otra venta para confirmar los datos ingresados esta correctos y proceder a **guardar**.



m) Una vez guardado el número registrado estará disponible en la vista.



n) De esta manera tendremos activado la autenticación en dos pasos. Deberán tener check de color verde las dos opciones configuradas anteriormente.

ANEXO 5: MATRIZ RACI DEL CICLO DE VIDA DE CUENTAS INSTITUCIONALES

R = Responsable, A = Aprobador, C = Consultado, I = Informado.

Actividad	Unidad orgánica	OTI	OSCD	ODP	RR. HH. / Registro / Abastecimiento	Titular / usuario
Solicitud de creación de cuenta nominal	R/A	C/I	I	C cuando trate datos personales	C/I	I
Solicitud de cuenta funcional	R/A	C/I	C	C cuando trate datos personales	C si corresponde	I
Creación técnica de cuenta	C	R/A	I	I	I	I
Entrega de credenciales y aceptación de responsabilidades	C	R	I	I	I	R
Revisión anual de cuentas funcionales	R/C	R/A	C	C	I	C
Suspensión por cese o término de vínculo	R/C	R/A	I	C si corresponde	R/C	I
Respaldo de información oficial	C/R	R/A	C	C	C	R
Atención de incidentes de seguridad	I	R	R/C	C si hay datos personales	I	R/I
Baja definitiva de cuenta	C/R	R/A	I	C si corresponde	C	I

ANEXO 6: FLUJOGRAMA TEXTUAL DE CREACIÓN Y BAJA DE CUENTAS

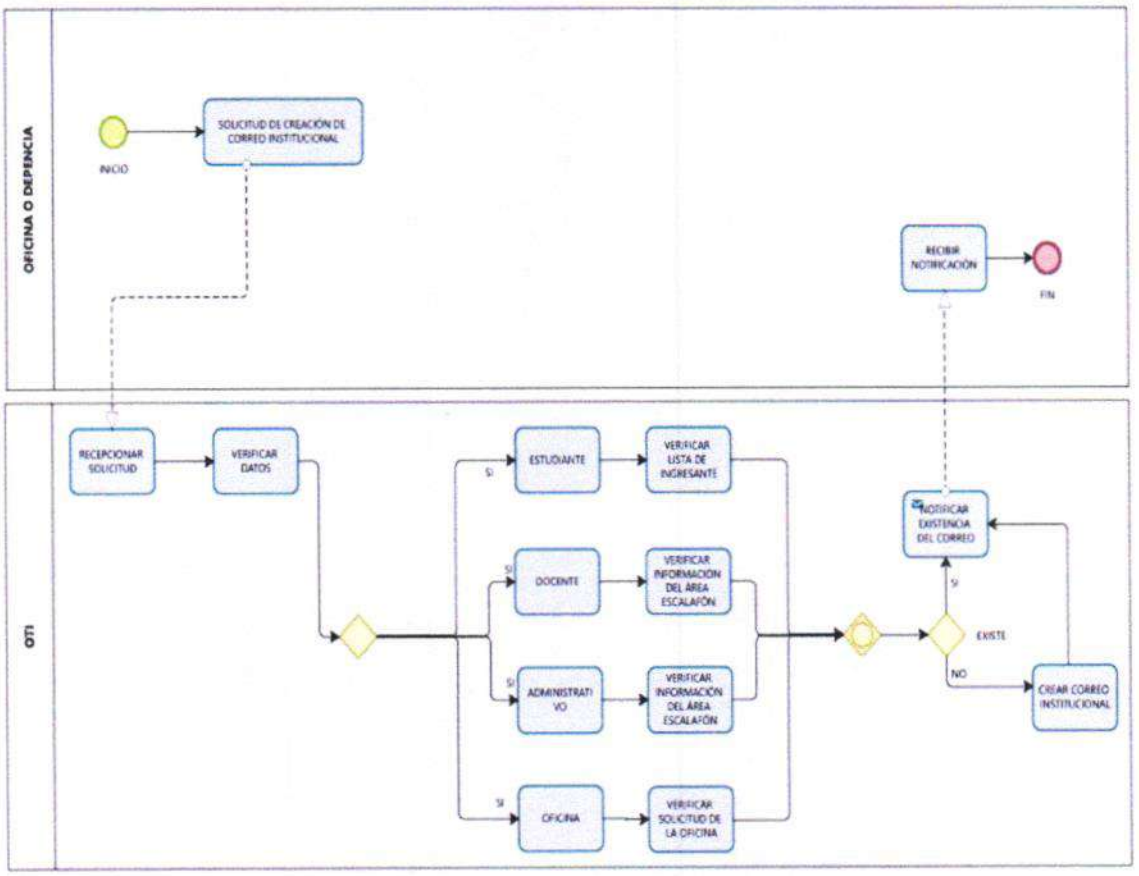
Proceso de creación de cuenta:

1. La unidad orgánica identifica la necesidad y define tipo de cuenta.
2. La unidad orgánica valida titular, usuario, finalidad, fecha de inicio y fecha de fin cuando corresponda.
3. La unidad orgánica remite solicitud formal a la OTI con documentos sustentatorios.
4. La OTI verifica datos, disponibilidad de identificador, cumplimiento de reglas y riesgos.
5. La OTI crea la cuenta, configura seguridad, cuota, permisos, MFA y registros.
6. La OTI entrega credenciales de forma segura y registra aceptación de responsabilidades.
7. El titular o usuario confirma acceso y activa MFA.

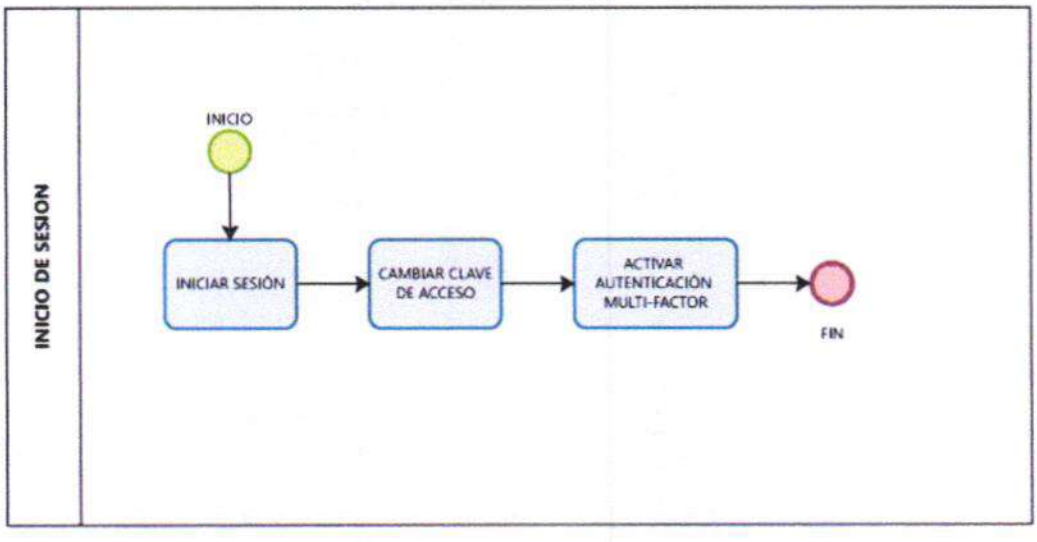
Proceso de baja o suspensión de cuenta:

1. La unidad orgánica o unidad de personal comunica cese, término de vínculo, fallecimiento, vencimiento, incidente o causal de baja.
2. La OTI suspende o restringe acceso cuando corresponda para preservar seguridad.
3. El titular o unidad responsable identifica y entrega información oficial; depura información personal o no oficial.
4. La OTI crea copia de respaldo en formato estándar, abierto e interoperable cuando sea viable.
5. La información oficial se conserva en legajo, sistema documental o repositorio autorizado.
6. La OTI ejecuta baja definitiva y actualiza el inventario de cuentas.

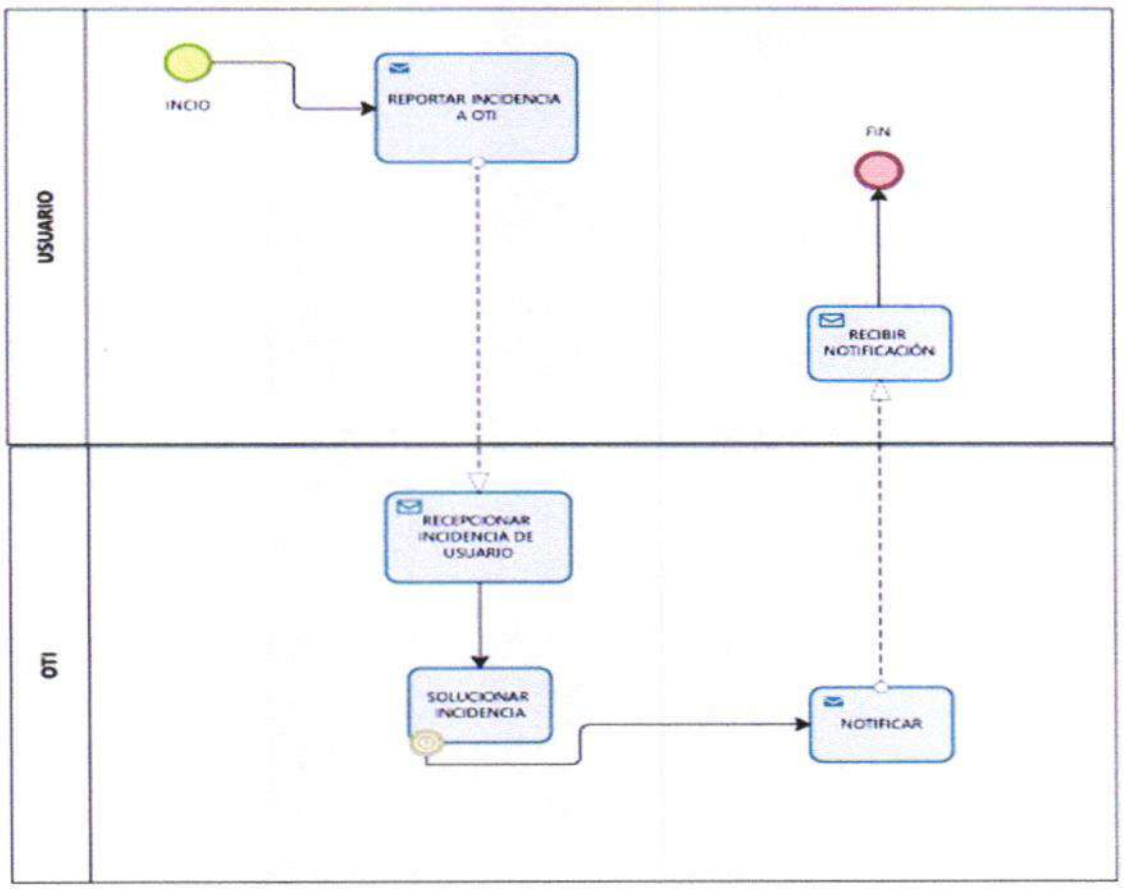
ANEXO 7: DIAGRAMA DE FUJO DE CREACIÓN DE USUARIO



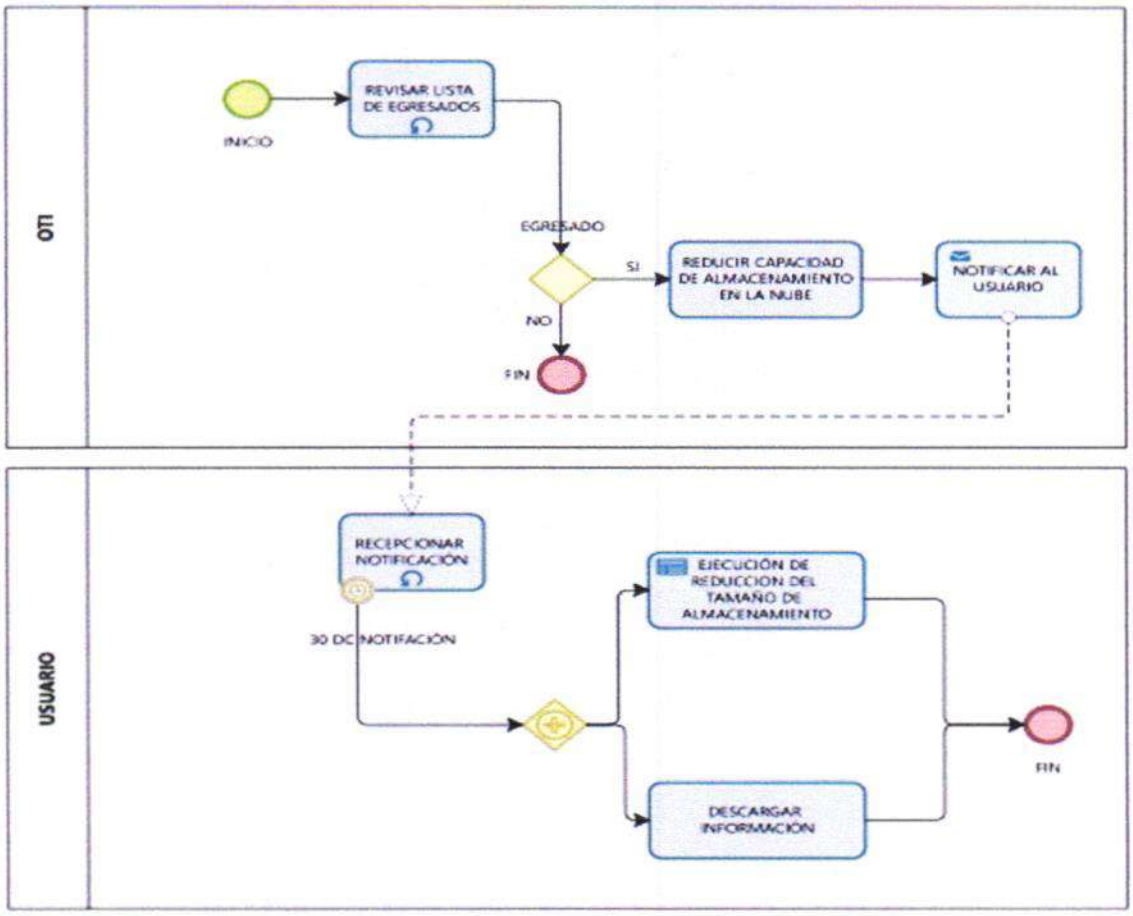
ANEXO 8: DIAGRAMA DE FUJO DE INICIO DE SESIÓN, CAMBIO DE CLAVE Y ACTIVACIÓN DE AUTENTICACIÓN MULTI-FACTOR.



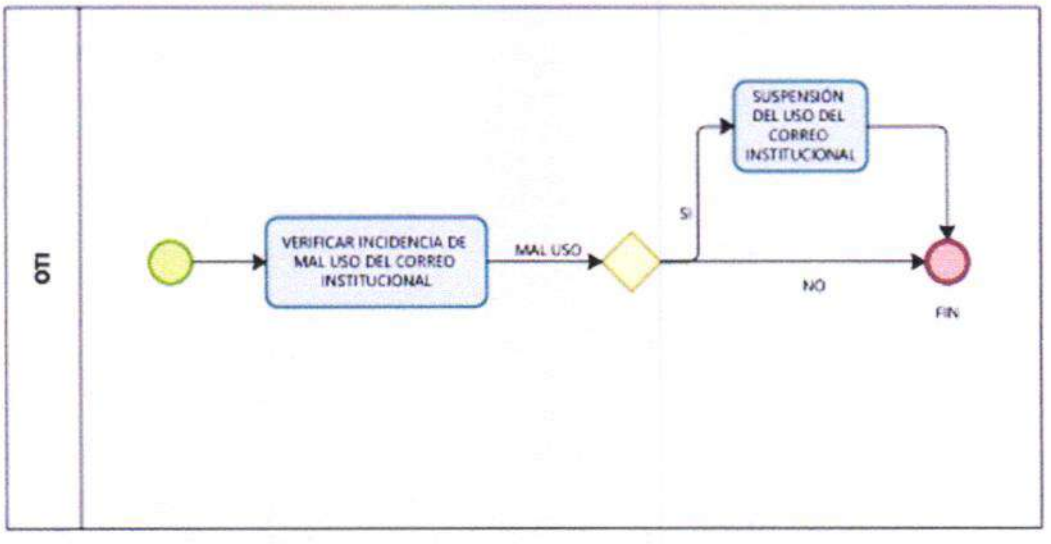
ANEXO 9: DIAGRAMA DE FUJO DE REPORTE DE INCIDENCIAS



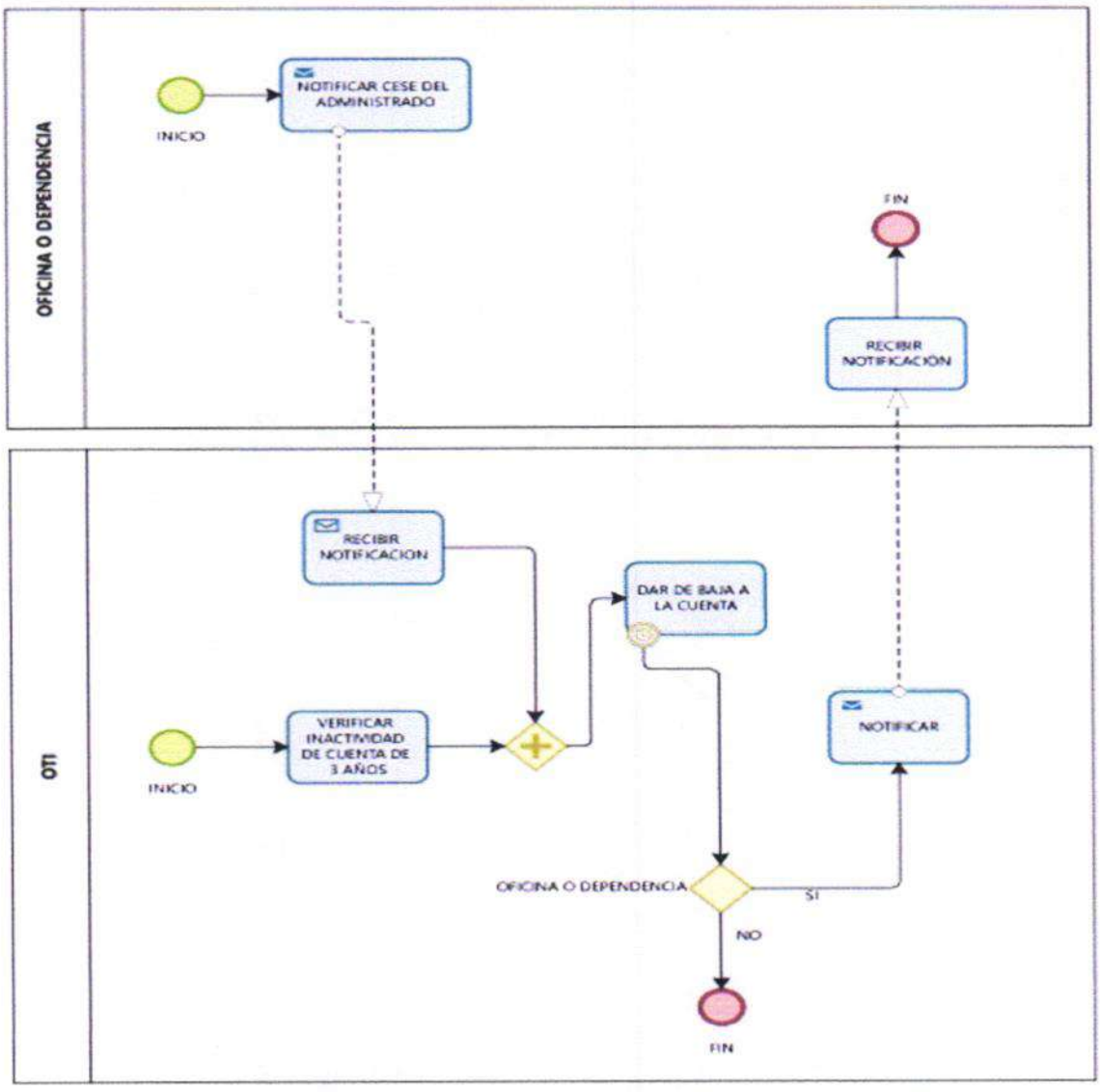
ANEXO 10: DIAGRAMA DE FUJO DE REDUCCIÓN DE TAMAÑO DE ALMACENAMIENTO EN LA NUBE



ANEXO 11: DIAGRAMA DE FUJO DE SUSPENSIÓN DE CUENTA



ANEXO 12: DIAGRAMA DE FUJO DEL CESE E INACTIVIDAD DEL USUARIO



ANEXO 13: DECLARACIÓN JURADA DE ENTREGA DE INFORMACIÓN OFICIAL

Nombres y apellidos del titular: _____

DNI: _____

Cargo / rol: _____

Unidad orgánica: _____

Cuenta nominal: _____

Cuentas funcionales asignadas: _____

Fecha de término de vínculo: _____

Responsable receptor de la información oficial: _____

Medio o repositorio de entrega: _____

Código de respaldo generado por OTI: _____

Declaro bajo juramento que la información entregada contiene la totalidad de la información de carácter oficial generada, recibida o gestionada en el ejercicio de mis funciones mediante la cuenta institucional indicada. Asimismo, declaro que la depuración realizada se limitó a información personal o no oficial, sin eliminar ni alterar información oficial.

La presente declaración no exime de responsabilidad por omisiones, alteraciones, eliminaciones indebidas o incumplimientos normativos detectados posteriormente.

Firma del titular: _____ Firma del receptor: _____ Firma OTI: _____

ANEXO 14: INVENTARIO Y REVISIÓN ANUAL DE CUENTAS FUNCIONALES

N.°	Cuenta funcional	Tipo	Finalidad	Titular institucional	Usuarios autorizados	Unidad responsable	Fecha inicio	Fecha fin	Última revisión	Estado / acción

La revisión anual debe verificar vigencia de la cuenta, actualización del titular institucional, usuarios autorizados, pertinencia de accesos, necesidad de continuidad, fecha de caducidad, registros de auditoría y cumplimiento de la prohibición de identificadores con nombres o apellidos de personas naturales.

Firma unidad responsable: _____ Firma OTI: _____