**DIRECTIVA NRO. 005-2019-UGD-OTI-UNA**

**NORMAS PARA EL USO DEL SERVICIO DE CORREO ELECTRÓNICO EN LA UNIVERSIDAD NACIONAL DEL ALTIPLANO DE PUNO.**

## 1. FINALIDAD

Normar los procedimientos para el uso del correo electrónico institucional a nivel nacional, para permitir que la comunicación e intercambio de información entre personas y entidades de la administración pública sea ágil y fluida.

## 2. OBJETIVO

2.1. Dar lineamientos para el uso correcto del servicio de correo electrónico oficial de la Universidad.

2.2. Optimizar la comunicación interna y externa a través de un medio electrónico, configurado de acuerdo a los requerimientos de información de la institución.

2.3. Cumplir con la aplicación de las normas para el uso del correo electrónico en el sector público.

## 3. ALCANCE

La presente Directiva es de cumplimiento obligatorio por todo el personal que labora en la Universidad Nacional del Altiplano, Sede Central, sedes descentralizadas y estudiantes de las 35 Escuelas Profesionales.

## 4. BASE LEGAL

- Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27444 - Ley del Procedimiento Administrativo General.
- Ley Nº 28493 - Ley que regula el uso del correo electrónico comercial no solicitado.
- Ley N° 30096 – Ley de Delitos Informáticos.
- Ley N° 27309 - Ley que incorpora los delitos informáticos al Código Penal.
- Ley Nº 27269 - Ley de Firmas y Certificados Digitales.
- Ley Nº 27291 - Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- Resolución Rectoral N° 0112-2018-R-UNA, que aprueba el Reglamento de Organizaciones y Funciones 2018 de la UNA – Puno.
- Decreto Supremo Nº 031-2005-MTC - Reglamento de la Ley Nº 28493 que regula el envío del correo electrónico comercial no solicitado.
- Decreto Supremo Nº 004-2013-PCM - Política Nacional de Modernización de la Gestión Pública.
- Resolución Jefatural Nº 088-2003-INEI - Aprueban Directiva sobre «Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública».

- Decreto Supremo Nº 019-2002-JUS - Reglamento de la Ley de Firmas y Certificados Digitales.

## 5. DISPOSICIONES GENERALES

5.1. El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas, es suministrada únicamente con el propósito de intercambiar información relacionada a la entidad en cumplimiento de la función en la entidad, no es una herramienta de difusión indiscriminada de información, con excepción de las listas de interés establecida por la institución para fines institucionales.

5.2. La Oficina de Tecnología Informática (Unidad de Gobierno Digital) llevará el control sobre el número de cuentas habilitadas con el objetivo de que se realice un uso racional de los recursos informáticos.

5.3. La asignación de cuentas de correo electrónico institucional es para los Docentes, Servidores Administrativos y Estudiantes de la UNA Puno y por excepción para terceros, previa autorización de la autoridad competente, quién deberá justificar y especificar el periodo de vigencia.

5.4. El usuario sólo podrá acceder al correo electrónico institucional mientras esté vinculado con la institución, pudiendo ser Administrativo, Docente o Estudiante.

5.5. Todo usuario que cuente con una cuenta de correo electrónico institucional, está comprometido y obligado a aplicar la presente directiva, y someterse a ellas.

5.6. Los usuarios de las cuentas de correo electrónico son responsables de todas las acciones que realizan con las mismas. Cualquier usuario que deje su cuenta de correo abierta en un lugar público es responsable de todo aquello que se realice desde dicha cuenta.

5.7. Las cuentas de correo electrónico institucional deben ser utilizadas por los usuarios en actividades que estén relacionadas con el cumplimiento de su función en la institución.

5.8. La institución debe garantizar la privacidad de las cuentas de correo electrónico institucional de todos los usuarios.

5.9. La cuenta de correo electrónico asignada a un usuario es personal e intransferible. La Unidad de Gobierno Digital está autorizado de otorgar cuentas de correo electrónico para los proyectos a solicitud de la autoridad competente.

## 6. GLOSARIO DE TÉRMINOS

- **Contraseña:** Combinación de números, letras y signos que deben teclearse para tener acceso a un sistema informático, estación de trabajo, entre otros.

- **Spam:** Son los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviado en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

- **Virus:** pequeño programa escrito intencionalmente para auto instalarse en la computadora de un usuario sin el consentimiento o permiso de éste. Normalmente se comporta como un programa parásito, pues infecta y ataca a los archivos del sistema y puede producir serios daños, pudiendo ocasionar que se borren o destruyan los archivos.

- **Cuenta de correo electrónico:** servicio que provee un espacio para la recepción, envío y almacenamiento de mensajes. Su utilización puede ser de carácter personal o funcional (cuenta genérica).

- **Correo electrónico institucional:** referido al servicio informático de intercambio de mensajes que la Universidad pone a disposición de las personal que trabajan en la misma, según las normas establecidas para el fin.

- **Cuentas genéricas:** Son cuentas que se utiliza para un propósito funcional común. Así se tiene cuentas genéricas para el servicio de soporte (soporte@unap.edu.pe), que es una cuenta que recibe solicitudes de los diversos usuarios que solicitan soporte técnico.

## 7. DISPOSICIONES ESPECIFICAS

### 7.1. DEL SERVICIO DE CORREO ELECTRÓNICO

7.1.1. La Unidad de Gobierno Digital garantiza la privacidad de las cuentas de correo electrónico institucional del personal de la UNA Puno.

7.1.2. La UGD, como parte del servicio del soporte tecnológico es responsable de brindar asesoría a los usuarios sobre el uso del correo electrónico institucional.

7.1.3. La UGD mantiene actualizado el inventario general de usuario del servicio de correo electrónico.

7.1.4. El envío de correos masivos es una funcionalidad restringida sólo a usuarios autorizados, acorde con sus funciones.

### 7.2. DEL USO DE LA TIPOGRAFIA

7.2.1. Los correos electrónicos institucionales deben estar escritos en las fuentes Tahoma o Arial tamaño 12.

7.2.2. El texto principal debe estar escrito en texto color negro y fondo blanco. Excepcionalmente se puede utilizar los colores (rojo, azul, verde).

7.2.3. No se debe escribir en mayúsculas, ya que puede ser interpretado como ofensa.

7.2.4. Los mensajes enviados no deben tener una imagen de fondo.

## 7.3. DEL BUEN USO DEL CORREO ELECTRÓNICO

7.3.1. Nombre de la Cuenta de Correo Electrónico

El nombre de la cuenta de correo electrónico para cada usuario será otorgado por la Oficina de Tecnologías de Información – Unidad de Gobierno Digital, generado por el Administrador de Correo Electrónico y su definición está conformada por **usuario@unap.edu.pe**, para los servidores administrativos, docentes y para los estudiantes de pregrado y postgrado debe ser **usuario@estudiante.unap.edu.pe**.

- [inicial primer nombre][1er apellido]
- [inicial primer nombre][1er apellido][inicial 2do apellido]
- [inicial primer nombre].[1er apellido]
- [inicial primer nombre].[1er apellido][inicial 2do apellido]

En caso de presentarse homonimia, el administrador de correo electrónico y las personas involucradas coordinarán y acordarán el nombre de la cuenta, tratando de seguir esta regla.

7.3.2. Asignación de contraseña

- Es obligatorio que el usuario una vez que acceda por primera vez al correo electrónico realice el cambio de su contraseña; se sugiere utilizar letras, números, signos de puntuación. La contraseña debe tener como mínimo 8 caracteres alfanuméricos y/o caracteres especiales: $#%&@.

- La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de 3 meses; concluido ese plazo, el sistema, en automático, solicitará el cambio de clave para tener acceso al correo electrónico.

- El usuario no debe anotar en lugar visible o de fácil localización sus contraseñas, debiendo ser estrictamente reservados para su manejo personal.

7.3.3. Sesión del usuario

Cuando un usuario finalice o interrumpa el uso de su estación de trabajo, deberá bloquear el sistema operativo (Windows + L) o cerrar la sesión del correo electrónico para evitar que otra persona utilice su cuenta de correo.

7.3.4. Lectura de correo

Los usuarios que tiene asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico o conectarse al correo electrónico con mayor frecuencia posible para leer sus mensajes.

7.3.5. Mantenimiento de mensajes de correo

- Se debe eliminar permanentemente los mensajes innecesarios.

- Al recibir un mensaje que se considere ofensivo, debe ser reenviado al Administrador de Correo Electrónico de la institución, a fin de que se tomen las acciones pertinentes.

7.3.6. Envío de correo

- Revisar el texto y la lista de destinatarios antes de enviar un mensaje, para corregir errores de ortografía, forma y fondo.

- Utilizar siempre el campo “Asunto”, a fin de resumir el tema del mensaje.

- Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.

- Evitar el uso de la opción de confirmación de entrega, a menos que sea un mensaje muy importante.

- Evitar el envío de mensajes a listas globales, a menos que sea un asunto oficial que involucre a la institución.

- Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar los lineamientos y recomendaciones para dicho tipo de documentos, tales como: Saludo formal, nombrar al destinatario por su nombre, evitar tutear, escribir puntualmente, al final del correo agradecer por la atención prestada.

- Evite enviar mensajes a personas que no conoce, a menos que sea por un asunto oficial que los involucre.

7.3.7. Reenvío de mensajes

- Para el reenvío de mensajes, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe.

- Previo al reenvío de un correo institucional a entes diferentes a los que se encuentran interviniendo en la comunicación, el usuario

debe asegurarse de que se ha realizado la validación de pertinencia de dicha acción, manteniéndose así la confidencialidad de la información.

7.3.8. Vigencia de las cuentas de correo electrónico

- Las cuentas de correo electrónico que no se usen durante un periodo continuo de 3 meses serán desactivadas, sin ningún tipo de notificación.

- Posteriormente la UGD remitirá a la Oficina de Recursos Humanos, los correos electrónicos desactivados o en desuso, para que determine las acciones necesarias.

7.3.9. Firma de correo electrónico

- Todos los correos institucionales deben tener definida la autofirma del remitente, para efectos de una fácil identificación del usuario dentro de la institución.

- La autofirma debe ser breve e informativa, no debiendo ocupar más de cinco (05) líneas, la cual deberá contener la siguiente información: logo de la institución, nombres y apellidos, cargo, oficina o unidad orgánica, número de teléfono / anexo.

- No incluir la dirección de correo en la autofirma, porque está ya fue incluida de manera automática en parte superior del mensaje.

- No debe abreviar el nombre de su dependencia ni omitir partes del mismo.

- Para mayor seguridad, incluya en la configuración de su firma de correo el siguiente párrafo que advierte que los contenidos que se incluyan en sus correos solo podrán ser utilizados por los destinatarios de los mismos. El siguiente texto debe pegarlo después de los datos de su firma, en la fuente Tahoma o Arial, tamaño 8 color gris.

  *La información contenida en este correo electrónico y en todos sus archivos anexos es confidencial y privilegiada. Este correo electrónico establece una comunicación entre un emisor y uno o varios receptores autorizados. La información y documentos anexos se encuentran amparados por el derecho fundamental al secreto y la inviolabilidad de las comunicaciones. Si usted ha obtenido el correo electrónico sin autorización, o de forma casual o involuntaria, la información contenida en él, además de no tener ningún efecto legal, no puede ser difundida, almacenada, copiada, divulgada o distribuida, por no existir consentimiento. Si lo hace, es posible que esté afectando derechos protegidos por la Constitución y las leyes, que impliquen responsabilidad sancionable o punible. Tampoco existe consentimiento para divulgar, almacenar o recopilar datos personales contenidos en el correo*

*electrónico, por no ser tal su finalidad. La información contenida en el correo electrónico no refleja necesariamente la posición oficial de la Universidad Nacional del Altiplano - Puno. El correo electrónico contiene comunicaciones o archivos que pueden o no generar estado, en la medida que reúnan los requisitos de eficacia, consentimiento y validez requeridos, y hayan sido remitidos en el alcance de la autorización recibida como usuario y usted sea un receptor autorizado. Por seguridad a su información, redes y sistemas someta este correo electrónico y sus anexos al control antivirus y los demás controles que correspondan. Está prohibido cualquier uso inadecuado de esta información, así como la generación de copias de este mensaje. Evite imprimir el correo, como medida de Ecoeficiencia, y a fin de preservar nuestros recursos naturales.*

## 7.4. DEL MAL USO DEL CORREO ELECTRÓNICO

7.4.1. Se considera falta grave facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas, los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucional y cuentas privadas ofrecidas por otros proveedores de servicios en Internet. Es falta grave el intentar apoderarse de claves de acceso de otros usuarios y acceder, modificar los mensajes de un usuario que no le corresponde.

7.4.2. Se considera como mal uso del correo electrónico institucional las siguientes actividades:

- Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la institución.

- Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.

- Distribuir mensajes con contenidos impropios y/o lesivos a la moral.

- Falsificar las cuentas de correo electrónico.

- Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de internet.

En caso del mal uso del servicio de correo electrónico o la detección de irregularidades contra lo establecido por la institución, la Oficina de Tecnologías de Información – Unidad de Gobierno Digital tomará las medidas pertinentes, con el respectivo informe a Secretaría General, Oficina de Recursos Humanos.

7.4.3. Enviar mensajes anónimos, con seudónimos, o que consignen títulos, cargos o funciones no oficiales o falsas.

7.4.4. Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengas el objetivo de paralizar el servicio por saturación de las

líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.

7.4.5. Suscripción indiscriminada a listas de correo. Es una versión de “mail bombing”, en que los ataquen no vienen de una sola dirección, sino de varias, los cuales son mucho más difíciles de encontrar.

7.4.6. Difundir mensajes masivos con contenido político, campañas de publicidad electoral, proselitismo y otros relacionados con procesos electorales.

7.4.7. Enviar correo electrónico con publicidad no autorizada en forma masiva, o cualquier otro tipo de correo no solicitado (spam).

7.4.8. Difundir información confidencial o reservada dentro y/o fuera de la UNA a destinatarios no autorizados.

7.4.9. Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos, injuriosos, cadena de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Institución.

## 7.5. DE LA VALIDEZ OFICIAL DEL CORREO ELECTRÓNICO

7.5.1. La Universidad Nacional del Altiplano, incorpora dentro de sus documentos oficiales el correo electrónico, en tal sentido tiene validez oficial para las gestiones internas de la Institución.

7.5.2. Para el intercambio de información entre instituciones públicas, se deberá disponer a la utilización de correo electrónico seguro, para lo que se podrá utilizar la firma y certificados digitales u otro medio de seguridad y verificación.

7.5.3. Los mensajes de correo electrónico y sus archivos adjuntos, tendrán validez legal si están firmados digitalmente, bajo el marco de la Ley N° 27269, “Ley de Firmas y Certificados Digitales” y de su Reglamento aprobado mediante Decreto Supremo N° 019-2002-JUS.

## 7.6. DE LA SEGURIDAD DE CORREO ELECTRÓNICO

7.6.1. El servicio de correo electrónico provisto por la empresa Google, posee un antivirus interno, el cual detecta si los archivos adjuntos en un mensaje contienen virus y si fuera necesario su exterminación.

7.6.2. Si el mensaje enviado contiene virus o troyano, debe eliminarse inmediatamente. Así mismo se deberá informar, al administrador de correo, el nombre del remitente y que su mensaje contenía virus.

7.6.3. En resguardo del correo electrónico los usuarios están prohibidos de:

- Enviar archivos con extensión: exe, cmd, bat, pif, scr, vbs y similares, debido a que estos tipos de archivos pueden ser utilizados para la propagación de virus y software malicioso en general.

7.6.4. El usuario debe dar aviso de inmediato a la UGD, sobre cualquier fallo de seguridad en su cuenta de correo electrónico, como el uso no autorizado de la cuenta por terceros, pérdida de contraseña u otros.

7.6.5. La UGD debe comunicar de manera oportuna a los usuarios la suspensión del servicio de correo electrónico cuando de modo programado, se vea en la obligación de hacerlo por cuestiones técnicas o de mantenimiento.

## 8. RESPONSABILIDADES

8.1. Los órganos y el personal de la UNA involucrados en la presente Directiva son responsables de velar por el debido, oportuno y estricto cumplimiento de sus disposiciones.

8.2. La Unidad de Gobierno Digital es responsable de que el personal de la institución cumpla con lo dispuesto en la presente directiva.

## 9. DISPOSICIONES COMPLEMENTARIAS

9.1. Las notificaciones institucionales pueden efectuarse mediante correo electrónico, el numeral 20.1.2 de la Ley N° 27444, Ley del Procedimiento Administrativo General.

9.2. Si se recibe algo cuestionable o ilegal, comunicar a la Oficina de Tecnologías de Información para que se tomen las acciones del caso.

9.3. La Oficina de Recursos Humanos deberá comunicar a la Oficina de Tecnologías de Información – Unidad de Gobierno Digital, la relación de trabajadores que hayan ingresado a laborar y de ser factible la(s) lista(s) a la(s) cuales se deben incorporar. Asimismo, deberá comunicar la relación de aquellos que han dejado de laborar, para proceder a la activación o desactivación de las cuentas de correo respectivas.

## 10. SANCIONES

El incumplimiento a las normas contenidas en la presente Directiva, será considerado como falta y sujeto a sanción de acuerdo a la normatividad vigente.

## 11. ANEXOS

a) Anexo 1. Solicitud para el acceso al Correo electrónico Institucional.