

**APRUEBA EL REGLAMENTO DE CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL DE LA UNIVERSIDAD ANTOFAGASTA.**

**DECRETO EXENTO Nº 393**

**ANTOFAGASTA, 28 de mayo de 2025.-**

**VISTOS:** Lo dispuesto en los D.F.L. Nºs 11 y 148, ambos de 1981 y D.S. Nº 118, de 2022, del Ministerio de Educación; Ley Nº 21.094, sobre Universidades Estatales.

**CONSIDERANDO:**

1. Que, por oficio DIR INF N°049, de 20 de mayo de 2025, el oficio DIR INF N°047, de 09 de mayo de 2025, ambos de la Dirección de Informática, y el oficio D.J N°323, de 06 de mayo de 2025, de la Dirección Jurídica, solicita oficializar el Reglamento de Cuentas de Correo Electrónico Institucional de la Universidad Antofagasta, el cual cuenta con visto bueno de la Dirección Jurídica.

2. Que, en mérito de lo anterior.

**DECRETO:**

1. **APRUEBASE**, el Reglamento de Cuentas de Correo Electrónico Institucional de la Universidad Antofagasta, cuyo texto es el siguiente:

**REGLAMENTO DE CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL DE LA UNIVERSIDAD DE ANTOFAGASTA**

**I. Disposiciones Generales:**

El siguiente reglamento aplica a todo el personal académico, no académico y alumnos de la Universidad de Antofagasta. Así también, abarca puntos relacionados a exalumnos y exfuncionarios que sigan relacionados a la institución.

1. Definiciones:

**a. Correo electrónico institucional:** Corresponde a todo email de dominio @uantof.cl, @ua.cl o @uamail.cl

**b. Correo electrónico personal:** Corresponde a todo email de alguna persona con vínculo a la Universidad de Antofagasta que no tenga dominio @uantof.cl, @ua.cl o @uamail.cl

**c. Correo electrónico institucional genérico:** Corresponde a un correo electrónico institucional asociado a alguna unidad o cargo de la organización en vez de a un individuo en particular. A pesar de no estar individualizado, de igual forma cuenta con al menos un responsable.

**d. Phishing:** Corresponde a un tipo de ciberataque que utiliza tácticas como hipervínculos falsos para atraer a los destinatarios de correos y hacer que compartan su información personal. Los atacantes suelen hacerse pasar por una entidad o persona de confianza para lograr su cometido.

**e. SPAM:** Se refiere a los mensajes de correo electrónico no solicitados, no deseados o con remitente desconocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades.

**f. OneDrive:** Es un servicio de almacenamiento en la nube de Microsoft que permite guardar, sincronizar y compartir archivos desde cualquier dispositivo con acceso a internet.

**g. SharePoint:** Es una plataforma de colaboración de Microsoft que permite gestionar, almacenar, compartir y organizar documentos y contenido en línea dentro de una empresa o equipo.

## **II. De la creación de correos electrónicos institucionales**

1. La creación de correo de un alumno será realizada bajo el dominio @ua.cl, al momento de validar la matrícula del alumno, la cual será notificada a su correo personal indicado durante el proceso de admisión y matrícula.
2. La creación de correo de personal académico y administrativo será posterior a la firma del nombramiento, contrato de trabajo o convenio de honorario según corresponda y será creada bajo el dominio @uantof.cl.
3. El formato de correo electrónico institucional para todo el personal académico y no académico generalmente será: [nombre].[apellido]@uantof.cl y [nombre].[apellido]@uamail.cl
4. El formato de correo electrónico institucional para alumnos generalmente será: [nombre].[apellido1].[apellido2]@ua.cl
5. Es responsabilidad de jefatura de cada dirección solicitar la creación de correo electrónico institucional al Departamento de Soporte Computacional de la Dirección de Informática, el cual es el encargado de gestionar la creación de este. Para ello, debe proporcionar RUT, nombre completo, cargo que desempeña y unidad a la que pertenece el nuevo usuario de correo electrónico institucional.
6. En el caso que se requiera un correo electrónico institucional genérico para alguna unidad o cargo, este debe ser solicitado al Departamento de Soporte Computacional de la Dirección de Informática por la jefatura de tal unidad con la debida justificación. Además, debe incluir: nombre de la casilla de correo electrónico, nombre que se despliega, tiempo de vigencia y un correo electrónico institucional responsable de la unidad. En este caso, el Departamento de Soporte Computacional enviará un formulario de aceptación de riesgos de uso de una cuenta genérica, la cual debe ser firmada por el responsable de tal correo electrónico institucional.

## **III. Del uso de correos electrónicos institucionales.**

1. El correo institucional es una herramienta entregada para funcionarios y alumnos. Cada funcionario será responsable del uso adecuado del correo asignado y dar cumplimiento de lo dispuesto en este reglamento. Esto incluye:
  - a) Utilizar el correo electrónico institucional solo con fines de acuerdo con su función dentro de la institución y con las actividades propias de la universidad. No está permitido utilizar este correo para actividades personales ajenas a la institución.
  - b) Resguardar su clave de acceso. Esta clave es de uso personal e intransferible. Será responsabilidad del funcionario cualquier mal uso de la información o pérdida de la información que pueda producirse por compartir su clave.
  - c) Prohibición de difusión de listas de correos electrónicos institucionales con personas ajenas a la Universidad sin contar la autorización para ello.
  - d) Administrar de manera eficiente el espacio asignado al correo y las aplicaciones que comparten espacio de almacenamiento con este, con el fin de evitar su saturación.
  - e) Incluir identificación adecuada, que incluya nombre completo, cargo, dirección a la que pertenece, institución (en este caso Universidad de Antofagasta), dirección de la institución,

- enlace de la página web institucional, correo electrónico del remitente, logo de la Universidad y logo de acreditación actualizado. Se debe incluir número de anexo en caso de contar con él.
- f) Evitar suscribirse a listas, foros y/o páginas web donde de manera directa o indirecta que faciliten la proliferación de SPAM a los correos electrónicos institucionales.
  - g) Prohibición de envío de correos electrónicos con contenido ilegal por naturaleza, llámase todo el que constituya complicidad con hechos delictivos. Por ejemplo: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, virus o código hostil en general.
  - h) Prohibición del envío mediante correo electrónico de toda cadena de correos, hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "Cartas en Cadena", "Phishing" o enviar correo electrónico solicitando donaciones caritativas, peticiones de claves o cualquier material relacionado.
  - i) Prohibición del envío de un número alto de mensajes por segundo que tenga el objetivo de dificultar o paralizar el servicio de correo electrónico ya sea por saturación de las redes, de la capacidad de CPU del servidor u otro.
  - j) Prohibición de falsificar encabezados de correos electrónicos, utilizar nombres de dominio que sean inválidos o inexistentes, u otras formas engañosas de enviar correo electrónico.

#### **IV. Espacio de almacenamiento asociado a correos electrónicos y aplicaciones institucionales**

1. Para los alumnos con matrícula vigente, se configurará su cuenta de correo institucional con una capacidad máxima de espacio de 5GB y para OneDrive 10 GB, total capacidad 15 GB.
2. Para los alumnos o exalumnos sin matrícula vigente, que sigan vinculados a la Universidad, se configurará su cuenta de correo institucional con una capacidad máxima de espacio de 5GB y para OneDrive 5 GB, total capacidad 10 GB.
3. Para los académicos y funcionarios en general, se configurará su cuenta de correo institucional con una capacidad máxima de espacio 50 GB y para OneDrive 30 GB, total capacidad 80 GB.
4. Para los correos electrónicos institucionales genéricos (congreso.ejemplo), se configurará la cuenta con una capacidad máxima de 20GB y para OneDrive 10 GB, total capacidad 30 GB.
5. Para correos electrónicos institucionales que corresponde a cargos asociados a directivos o secretarios de direcciones o unidades se configurará su cuenta de correo institucional con una capacidad máxima de 50 GB y para OneDrive 30 GB, total capacidad 80 GB.
6. En casos excepcionales y debidamente justificados, personal académico y administrativos podrán solicitar una expansión del límite del espacio de almacenamiento de su cuenta. Estas solicitudes deben realizarse al Departamento de Soporte Computacional de la Dirección de Informática, las cuales serán evaluadas y se podrán determinar los nuevos límites.
7. Personal académico y administrativo que haya culminado su carrera laboral (jubilación), en la Universidad de Antofagasta, podrá mantener su cuenta de correo electrónico institucional con justificación adecuada y por un tiempo definido. Además, se configurará con una capacidad máxima de 5GB y para OneDrive 5 GB, total capacidad 10 GB.

#### **V. De la actualización de información del correo electrónico institucional**

1. Es responsabilidad de cada jefatura de dirección, facultad o unidad solicitar la actualización de información de su personal académico y/o administrativos si se realizan cambios en su cargo o unidad en que desempeña sus funciones cuando éstas ocurran.

#### **VI. De la deshabilitación y cierre del correo electrónico institucional de funcionarios académicos y no académicos**

1. Las cuentas de correo electrónico institucional que hayan sido asignadas a personal académico y personal no académico que ya no tienen vínculo con la Universidad serán objeto de eliminación en 90 días posterior a su desvinculación. Se podrán evaluar casos de extensión previa solicitud de su jefatura.

2. Cualquier cuenta de correo electrónico que sea responsabilidad de un individuo con una investigación en curso, debe ser informada por la unidad o dirección correspondiente y no se podrá deshabilitar ni eliminar hasta que la investigación culmine.

## **VII. Deshabilitación y eliminación del correo electrónico institucional de alumnos y exalumnos.**

1. Esta medida no aplica para alumnos con retiro temporal, egresados y pérdida de calidad de egresado.
2. Las cuentas de correo electrónico institucional de exalumnos, sin considerar alumnos egresados o titulados, serán objeto de eliminación por abandono después de un periodo de 2 años.
3. El Departamento de Soporte Computacional enviará 2 avisos a una cuenta de correo electrónico institucional objeto de eliminación, indicando que, transcurridos 30 días corridos posterior al aviso, la cuenta será deshabilitada.
4. El responsable de un correo electrónico institucional que haya sido deshabilitada podrá solicitar su habilitación temporal a través de su exjefe de carrera. La solicitud deberá dirigirse al Departamento de Soporte Computacional y se aprobará únicamente con el propósito de recuperar la información almacenada en la cuenta.
5. El Departamento de Soporte Computacional eliminará una cuenta de correo electrónico institucional, transcurridos 15 días posterior a su deshabilitación.
6. Si un correo institucional de alumno ha sido eliminado debido a los plazos establecidos, se podrá crear un nuevo correo únicamente si es solicitado por la dirección, el jefe de carrera o el decano. Este correo será de uso exclusivo para la gestión de trámites como títulos, certificados entre otros, y estará disponible solo por un tiempo limitado, según el trámite a realizar.
7. En caso de defunción de un alumno, se mantendrá el correo activo por 1 año antes de su eliminación.
8. Cualquier cuenta de correo electrónico que sea responsabilidad de un individuo con una investigación en curso, debe ser informada por la unidad o dirección correspondiente y no se podrá suspender ni eliminar hasta que la investigación culmine.

## **VIII. Uso de la plataforma SharePoint**

Microsoft SharePoint es una plataforma utilizada en entornos académicos para la gestión documental, colaboración y almacenamiento de información institucional. Sin embargo, su uso debe estar regulado para garantizar una administración eficiente de los recursos digitales y evitar problemas asociados a la proliferación descontrolada de sitios y el consumo excesivo de almacenamiento. A continuación, se establecen las directrices generales para su uso en la Universidad de Antofagasta.

### **1. Creación y Administración de Sitios de SharePoint**

- a) La creación de sitios en Microsoft SharePoint estará restringida a funcionarios y académicos y no académicos con necesidades institucionales debidamente justificadas.
- b) Los estudiantes y exalumnos no tendrán permisos para crear nuevos sitios, aunque podrán ser agregados como colaboradores a sitios ya existentes, bajo la autorización de un responsable del sitio.
- c) La solicitud de creación de un sitio debe realizarse a través de la Dirección de Informática, indicando el propósito del sitio, los responsables y el período estimado de uso.
- d) Cada unidad académica y administrativa será responsable de la administración y mantenimiento de los sitios que cree, asegurando el cumplimiento de las normativas institucionales.
- e) Se recomienda organizar los sitios en colecciones estructuradas y limitar la creación de subsitios para evitar la sobrecarga y garantizar una gestión eficiente de la plataforma, considerando que el sitio raíz será siempre administrado por la Dirección de Informática.

## **2. Políticas de Almacenamiento en SharePoint**

- a) Cada sitio de SharePoint contará con un límite de almacenamiento predeterminado de 500 GB, sujeto a revisión y ampliación en casos justificados, previa evaluación por el Departamento de Soporte Computacional.
- b) En el caso de sitios de carácter temporal (como proyectos o eventos específicos), el almacenamiento podrá ser asignado de manera provisional, con una revisión posterior para su continuidad o eliminación.
- c) Los responsables de cada sitio deberán gestionar el espacio de almacenamiento de manera eficiente, eliminando documentos obsoletos y evitando la acumulación innecesaria de archivos.
- d) Los sitios que superen el almacenamiento estarán sujetos a una evaluación por parte del Departamento de Soporte Computacional para determinar si es necesario mover los datos a una base de datos.

## **3. Administración de Accesos y Permisos**

- a) El acceso a los sitios de SharePoint será determinado por la Dirección de Informática, quien deberá asignar permisos conforme a las necesidades operativas y los principios de seguridad de la información bajo la responsabilidad del usuario solicitante.
- b) La gestión de permisos deberá garantizar que solo los usuarios autorizados puedan visualizar, modificar o compartir documentos dentro de cada sitio.
- c) Se deberá evitar la asignación de permisos globales de edición o administración a grupos amplios, priorizando el acceso restringido y supervisado.

## **4. Eliminación y Mantenimiento de Sitios de SharePoint**

- a) Los sitios de SharePoint que no presenten actividad por un período de **12 meses** podrán ser identificados como inactivos y sujetos a revisión para su eliminación por Departamento de Soporte Computacional.
- b) Antes de proceder a la eliminación de un sitio, se enviará una notificación a los responsables, otorgando un período de **30 días** para justificar su continuidad o realizar el respaldo de la información almacenada.
- c) En caso de que un sitio deba ser eliminado, el usuario responsable es quien llevara a cabo el procedimiento correspondiente, asegurando la correcta migración o eliminación de los datos según corresponda al cual se le otorgara un soporte por parte del Departamento de Soporte Computacional.
- d) Los sitios de carácter temporal tendrán una fecha de expiración definida desde su creación, debiendo ser renovados o eliminados al término del período estipulado.

## **5. Responsabilidades y Cumplimiento**

- a) Todo usuario de SharePoint deberá utilizar la plataforma conforme a los fines institucionales y académicos de la Universidad, respetando las normativas de seguridad y gestión documental.
- b) El incumplimiento de estas directrices podrá derivar en restricciones de acceso, eliminación de permisos o sanciones conforme a las normativas vigentes de la Universidad.
- c) Cualquier situación no contemplada en este reglamento será evaluada por el Departamento de Soporte Computacional en conjunto con la Dirección de Informática, conforme a la normativa institucional aplicable.

## **IX. Otras situaciones**

1.- Cuando se lleve a cabo la reducción del espacio de almacenamiento en OneDrive para las cuentas institucionales, por motivos previamente informados, se notificará a los usuarios en dos ocasiones por

correo electrónico, con el objetivo de que puedan respaldar su información antes de que sea eliminada por la plataforma.

2.- Otras situaciones no previstas en este documento serán resueltas por o en conjunto con el Departamento de Soporte Computacional y la Dirección de Informática en conformidad con normas y reglamentación vigente de la Universidad.

**ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.**

**FERNANDO  
FERNANDEZ  
DE LA CERDA**

Firmado digitalmente  
por FERNANDO  
FERNANDEZ DE LA  
CERDA  
Fecha: 2025.05.28  
15:38:39 -04'00'

**FERNANDO FERNÁNDEZ DE LA CERDA  
SECRETARIO GENERAL**

**MARCOS  
ANTONIO  
CIKUTOVIC  
SALAS**

Firmado digitalmente  
por MARCOS ANTONIO  
CIKUTOVIC SALAS  
Fecha: 2025.05.28  
12:47:54 -04'00'

**MARCOS CIKUTOVIC SALAS  
RECTOR**

MCS/FFDLC/MDS/CRC

Distribución:

Secretaría General (SGD 1901)

Rectoría

Contraloría Universitaria

Dirección Jurídica

Vicerrectoría Académica

Vicerrectoría Económica

Vicerrectoría de Investigación, Innovación y Postgrado

Dirección de Gestión y Análisis Institucional

Dirección de Vinculación con el Medio y Extensión

Dirección de Gestión Docente

Dirección de Desarrollo Curricular

Dirección de Registro Curricular

Dirección de Proyectos de Desarrollo Institucional

Servicio de Biblioteca y Recursos de apoyo de Aprendizaje

Dirección de Desarrollo Estudiantil

Servicio Bienestar Estudiantil

Facultades

Dirección de Economía y Finanzas

Departamento de Finanzas

Unidad de Remuneraciones

Dirección de Matricula y Cobranzas

Dirección de Personal y Administración de Campus

Depto. Desarrollo de las Personas

Depto. de Administración de Recursos Humanos

Departamento de Abastecimiento

Dirección de Informática

Dirección Escuela de Postgrado

Dirección de Gestión de la Investigación

Sistema de Educación a Distancia  
Centros  
CITEVA  
Institutos  
Oficina de Santiago  
Departamento de Comunicaciones  
Relaciones Públicas  
Jefe de Gabinete de Rectoría  
Oficina de Partes  
Oficina de Títulos y Grados  
F.E.U.A.  
BOE-UA