UNIVERSIDAD DE TARAPACÁ
ARICA - CHILE

APRUEBA PROCEDIMIENTOS ADMINISTRATIVOS COMPLEMENTARIOS A LA POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO Nº 00.900/2025.

Arica, julio 21 de 2025.

Con esta fecha la Rectoría de la Universidad de Tarapacá, ha expedido el siguiente decreto:

VISTO:

Lo dispuesto en el D.F.L. N° 150, de 11 de diciembre de 1981, del ex Ministerio de Educación Pública, D.F.L. N° 16, de 27 de diciembre de 2023, publicado el 11 de julio de 2024, del Ministerio de Educación; Resolución Nº 36 de 2024 de la Contraloría General de la República y sus modificaciones; Resolución Exenta Universitaria CONTRAL. Nº0.01/2002, de enero 14 de 2002, Resolución Exenta Universitaria CONTRAL N°0.01/2025, de marzo 26 de 2025; Carta D.G.D.T. N° 54/2025, de fecha 18 de julio de 2025, Carta VRD. N°110/2025, de fecha 18 de julio de 2025, Carta REC.N°2213/2025, de fecha 21 de julio de 2025; los antecedentes adjuntos y las facultades que me confiere el Decreto N° 113, de 13 de junio de 2022, del Ministerio de Educación.

CONSIDERANDO:

Lo dispuesto en el artículo 2° de la Ley N° 21.094, sobre Universidades Estatales, particularmente en lo referente a la autonomía administrativa, en virtud de la cual se faculta a las Universidades del Estado para estructurar su régimen de gobierno y de funcionamiento interno, de conformidad a sus estatutos y reglamentos universitarios, teniendo como única limitación las disposiciones de esta ley y las demás normas legales que les resulte aplicables.

Que, el 11 de julio de 2024 se publicó en el diario oficial el DFL 16 que Aprueba Estatuto de la Universidad de Tarapacá, adecuado al título II de la Ley N°21.094, sobre Universidades Estatales.

Que, el inciso primero del artículo primero del cuerpo transitorio del citado DFL 16, señala: "El presente Estatuto entrará en vigor en el plazo de doce meses desde la fecha de publicación en el Diario Oficial". A su turno, el artículo segundo transitorio indica: "De la continuidad de servicio. Las unidades académicas y administrativas vigentes mantendrán su composición, dependencia, funciones y características, adecuándose en la medida que se lleven a cabo las modificaciones pertinentes.

Las autoridades y demás cargos nombrados bajo el cuerpo legal anteriormente vigente y que no sean incompatibles con lo establecido en el presente Estatuto, permanecerán en funciones por el tiempo que reste para el cumplimiento de sus respectivos períodos.

Con todo, los reglamentos y demás normativa universitaria actualmente vigente se mantendrán en todo aquello que no resulte incompatible con el presente estatuto".

Que, en atención a la mejora continua sobre la seguridad de la información institucional, la Dirección de Gestión Digital y Transparencia ha solicitado formalizar, mediante decreto, los procedimientos sobre seguridad de la información, los cuales han sido aprobados por el Comité de Seguridad de la Información de la Universidad.

Que, dichos procedimientos complementan las Políticas de Seguridad de la Información y dan respuesta a la auditoría de la Contraloría Regional según Carta DACI N° 82/2023.

Que, conforme a los antecedentes presentados por el Sr. Patricio Zapata Valenzuela, Vicerrector de Desarrollo Estratégico de la Universidad de Tarapacá, mediante carta VRD N°110/2025, de fecha 18 de julio de 2025, y a lo ordenado por el Rector de la Universidad, Dr. Emilio Rodríguez Ponce, a través de carta REC N°2213/2025, de fecha 21 de julio de 2025.

DECRETO:

1.- Apruébase, como instrumentos administrativos de la Universidad de Tarapacá, en calidad de complemento de la Política de Seguridad de la Información, los siguientes documentos:

a) Solicitud de Acceso por VPN y/o Escritorio Remoto, contenido en documento adjunto, compuesto por tres (3) páginas, debidamente rubricadas por el Secretario de la Universidad de Tarapacá.

b) Solicitud de Acceso por VPN Institucional, contenido en documento adjunto, compuesto por tres (3) páginas, debidamente rubricadas por el Secretario de la Universidad de Tarapacá.

c) Procedimiento de Destrucción de la Información, contenido en documento adjunto, compuesto por seis (6) páginas, debidamente rubricadas por el Secretario de la Universidad de Tarapacá.

2.- Publíquese, en el sistema informático conforme lo señalado en el art. 7 de la Ley N°20.285 de 2008, del Ministerio Secretaria General de la Presidencia, sobre Acceso a la información pública.

Anótese, y remítase a la Contraloría de la Universidad, para su control y registro. Comuníquese una vez tramitado totalmente el acto.

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA

ÁLVARO PALMA QUIROZ
Secretario de la Universidad

UNIVERSIDAD DE TARAPACA RECTOR ARICA

EMILIO RODRÍGUEZ PONCE
Rector

ERP.APQ.yvv

UNIVERSIDAD DE TARAPACA CONTRALORA (S) ARICA

24 JUL 2025

Solicitud de Acceso VPN / Escritorio Remoto

Para cualquier tipo de acceso a plataformas internas, externas o bien desde el exterior de la institución, accediendo remotamente a estos servicios desde un computador dentro de la red de la institución, debe realizar dos pasos fundamentales:

1. Llenar el formulario con toda la información que se solicita.

2. Notificar a la Dirección de Gestión Digital y Transparencia mediante carta o correo udt@gestion.uta.cl respecto de la solicitud ingresada y las razones que motivan su registro.

El ingreso de la solicitud no garantiza ni compromete que se otorgue el acceso mientras no se emita y comunique la aprobación por escrito por la Dirección de Gestión Digital y Transparencia. Toda concesión de acceso se entenderá con límite geográfico nacional. Cualquier otro rango de cobertura deberá ser discutido con el coordinador de área. En el caso de prestadores de servicios a honorarios, se debe contar además con la autorización de su jefe/a director.

1. ANTECEDENTES GENERALES

Correo electrónico

_____

Nombres y apellidos:

_____

RUT/RUN (con puntos, guión y dígito verificador)

_____

Estamento: (si procede)

_____

Unidad/Facultad/Proyecto:

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

APG

_____

Celular: _____

2. DESCRIPCION DEL SERVICIO

Fecha de caducidad del acceso o credencial solicitado (DD/MM/AAAA):

_____

Indique brevemente el motivo que genera esta solicitud:

_____

Tipo de acceso (marque lo que corresponda):

- ☐ SSL/VPN
- ☐ Acceso a sitios externos
- ☐ Escritorio remoto desde internet
- ☐ Apertura de aplicación restringida

Indique las direcciones IP de los dispositivos a los que requiere acceder (si es más de 1, separe con coma):

_____

Indique los servicios que desea habilitar (marque lo que corresponda):

- ☐ SSH
- ☐ HTTP/HTTPS
- ☐ FTP/SFTP/SCP
- ☐ Escritorio remoto (RDP)
- ☐ Aplicación remota (TeamViewer/AnyDesk/VNC/noMachine)

Si en la pregunta anterior no se encontraban los servicios requeridos, indíquelos con nombre y puerto:

_____

Si desea especificar algún detalle adicional, sea breve, claro y técnico:

_____

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

3. CONDICIONES PARA ACCESO AL SERVICIO

☐ Uso Responsable: El acceso a la VPN debe ser utilizado exclusivamente para fines laborales y actividades autorizadas.

☐ Seguridad: Mantener la confidencialidad de las credenciales de acceso y usar contraseñas seguras.

☐ Políticas de la Institución: Cumplir con todas las políticas y normativas de seguridad vigentes.

☐ Monitoreo y Registro: La DGDT puede monitorear y registrar el uso de la VPN.

☐ Protección de Datos: Manejar la información con confidencialidad según las políticas institucionales.

☐ Responsabilidad: El uso de la VPN es personal y el usuario será responsable de cualquier uso indebido.

Declaro que he sido debidamente informado(a) sobre el tratamiento de mis datos personales y, en consecuencia, autorizo su uso conforme a lo dispuesto en la Ley N.° 19.628 sobre Protección de la Vida Privada. Esta autorización se otorga para los fines específicos indicados en este formulario, garantizando el respeto a mis derechos conforme al artículo 19 N.° 4 de la Constitución Política de la República de Chile.

FIRMA DEL SOLICITANTE

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Solicitud de Acceso VPN Institucional

Para cualquier tipo de acceso a plataformas internas, externas o bien desde el exterior de la institución debe realizar dos pasos fundamentales:

1. Llenar el formulario con toda la información que se solicita.

2. Notificar a la Dirección de Gestión Digital y Transparencia mediante carta o correo udt@gestion.uta.cl respecto de la solicitud ingresada y las razones que motivan su registro.

El ingreso de la solicitud no garantiza ni compromete que se otorgue el acceso mientras no se emita y comunique la aprobación por escrito por la Dirección de Gestión Digital y Transparencia. Toda concesión de acceso se entenderá con límite geográfico nacional. Cualquier otro rango de cobertura deberá ser discutido con el coordinador de área. En el caso de prestadores de servicios a honorarios, se debe contar además con la autorización de su jefe/a director.

1. ANTECEDENTES GENERALES

Correo electrónico

_____

Nombres y apellidos:

_____

RUT/RUN (con puntos, guión y dígito verificador)

_____

Estamento: (si procede)

_____

Unidad/Facultad/Proyecto:

_____

Celular:

_____

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

2. DESCRIPCION DEL SERVICIO

Fecha de caducidad del acceso o credencial solicitado (DD/MM/AAAA):

_____

Indique brevemente el motivo que genera esta solicitud:

_____

País desde donde requiere contar con acceso:

_____

Marque las opciones que describan mejor su requerimiento

☐ Intranet Institucional

☐ Sistemas Administrativos y Financieros

☐ Sistemas Académicos

☐ Firma de documentos

☐ Firma Gob/Firma Electrónica Avanzada

Si la opciones anteriores no describen el tipo de acceso que necesita, indique aquí brevemente sus requerimientos.

_____

UNIVERSIDAD DE TARAPACA
SECRETARIO
DE LA
UNIVERSIDAD
ARICA - CHILE

3. CONDICIONES PARA ACCESO AL SERVICIO

☐ Uso Responsable: El acceso a la VPN debe ser utilizado exclusivamente para fines laborales y actividades autorizadas.

☐ Seguridad: Mantener la confidencialidad de las credenciales de acceso y usar contraseñas seguras.

☐ Políticas de la Institución: Cumplir con todas las políticas y normativas de seguridad vigentes.

☐ Monitoreo y Registro: La DGDT puede monitorear y registrar el uso de la VPN.

☐ Protección de Datos: Manejar la información con confidencialidad según las políticas institucionales.

☐ Responsabilidad: El uso de la VPN es personal y el usuario será responsable de cualquier uso indebido.

Declaro que he sido debidamente informado(a) sobre el tratamiento de mis datos personales y, en consecuencia, autorizo su uso conforme a lo dispuesto en la Ley N.º 19.628 sobre Protección de la Vida Privada. Esta autorización se otorga para los fines específicos indicados en este formulario, garantizando el respeto a mis derechos conforme al artículo 19 N.º 4 de la Constitución Política de la República de Chile.

FIRMA DEL SOLICITANTE

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

PROCEDIMIENTO DE DESTRUCCIÓN DE LA INFORMACIÓN

1. Propósito:

Este procedimiento tiene como objetivo asegurar que toda la información en la universidad que ha cumplido su ciclo de vida sea destruida de manera segura y en cumplimiento con las normativas de seguridad de la información, protegiendo la confidencialidad de datos sensibles como expedientes académicos, datos de investigación, información financiera, entre otros.

2. Alcance:

Este procedimiento se aplica a todo el personal administrativo, académico, y terceros que manejan información en cualquier formato dentro de la universidad, incluyendo oficinas administrativas, departamentos académicos y centros de investigación.

3. Normativa de referencia:

- Decreto N°83/2005, Ministerio Secretaría General de la Presidencia, norma técnica para Órganos de la Administración del Estado seguridad y confidencialidad de documentos electrónicos, de 03.06.2004, del Ministerio Secretaría General de la Presidencia.
- Norma Chilena NCh ISO/IEC 27002, Seguridad de información, ciberseguridad y protección de la privacidad –controles de seguridad de la información, tercera edición 27.12.2022.
- Decreto N°273/2022, Ministerio del Interior y Seguridad Pública; Subsecretaría del Interior, Establece obligación de reportar incidentes de ciberseguridad.
- DFL 29 Fija Texto Refundido, Coordinado y Sistematizado de la Ley N°18.834, Sobre Estatuto Administrativo.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

- Ley N°19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
- Ley N°19.628, sobre protección de la vida privada.
- Ley N°21.459, que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
- Decreto N°20, Reglamento sobre preservación provisoria de datos informáticos en las investigaciones penales.

4. Definiciones:

- Información confidencial universitaria: Datos cuya divulgación puede comprometer la seguridad o integridad de los estudiantes, profesores, empleados, investigaciones, o la misma universidad. Ejemplos incluyen datos personales, calificaciones, investigaciones en curso, planes estratégicos, entre otros.

- Destrucción de información: Proceso irreversible de eliminación de información universitaria para prevenir el acceso no autorizado o recuperación posterior.

- Formato físico: Documentos en papel, medios de almacenamiento magnético o dispositivos físicos.

- Formato digital: Información almacenada en discos duros, servidores, unidades USB, entre otros medios electrónicos.

5. Responsabilidades:

- Dirección de Gestión Digital y Transparencia: Supervisar la correcta aplicación de este procedimiento en relación con los sistemas de información.

- Oficial de Seguridad de la Información de la Universidad: Responsable de la vigilancia general del proceso de destrucción.

- Propietarios de la información: Cada departamento o unidad académica es responsable de identificar la información que debe ser destruida.

- Usuarios autorizados: Asegurarse de seguir los procedimientos apropiados para eliminar la información bajo su control.

6. Clasificación de la Información:

Antes de proceder a la destrucción, cada unidad debe tener correctamente clasificada la información, por ejemplo:

- Expedientes estudiantiles.
- Información financiera.
- Datos de investigación.
- Documentos administrativos y académicos.

La autorización para la destrucción debe ser obtenida del propietario de la información (como el departamento responsable o el investigador principal).

APG

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

7. Métodos de Destrucción:

7.1 Información en formato físico: Esto aplica siempre que se haya realizado previamente respaldo digital de la información.

- Documentos en papel: Utilizar destructoras de papel de corte cruzado para la eliminación de expedientes académicos, datos personales de estudiantes y documentos financieros. Para cantidades grandes, se podrían contratar servicios externos certificados.

- Dispositivos físicos (discos, cintas, etc.): Utilizar métodos como desmagnetización o trituración de discos duros de equipos informáticos de laboratorios o servidores antiguos de la universidad.

- Medios ópticos (CDs/DVDs): Destrucción física o incineración en instalaciones seguras.

7.2 Información en formato digital:

Software especializado: Uso de herramientas de borrado seguro para sobrescribir múltiples veces la información almacenada en los sistemas de la universidad.
Eliminación criptográfica: Si los datos se encuentran cifrados, la eliminación de las claves de cifrado puede considerarse una destrucción efectiva.

7.3 Información almacenada en la nube:

Eliminación en servicios de terceros: Solicitar formalmente la destrucción segura de datos a los proveedores de servicios en la nube utilizados por la universidad y obtener un certificado de destrucción.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO
DE LA
UNIVERSIDAD
ARICA - CHILE

8. Registro y Evidencias:

Cada unidad debe mantener un registro detallado de todas las acciones de destrucción de información mediante plataforma disponibilizada por la institución. El registro debe incluir:

- Descripción de la información destruida.
- Fecha de destrucción.
- Método de destrucción utilizado.
- Nombre del responsable de la destrucción.
- Autorización para la destrucción (si corresponde).
- Certificados de destrucción de servicios externos (si aplica).

9. Auditoría y Verificación:

Este procedimiento será revisado anualmente, o con una periodicidad menor si así se requiere, por el Comité de Seguridad de la Información, con el fin de realizar actualizaciones, modificaciones u otras gestiones pertinentes.

Asimismo, su aplicación y registro podrán ser incorporados en el Plan Anual de Auditorías Institucionales, a requerimiento del Rector o Rectora o de los órganos colegiados superiores, con el objetivo de verificar su implementación y cumplimiento adecuado.

10. Excepciones:

Cualquier excepción a este procedimiento debe ser aprobada por el Oficial de Seguridad de la Información y estar debidamente documentada.

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

11. Difusión:

Todo el personal, incluyendo administrativos, docentes e investigadores, debe recibir capacitación regular sobre la importancia de la correcta destrucción de información y las responsabilidades que conlleva.

12. Revisión y Mejora Continua:

Este procedimiento será revisado anualmente o cuando surjan cambios en las normativas o tecnologías. La universidad deberá adaptar el procedimiento conforme a los avances tecnológicos y nuevas regulaciones para asegurar su vigencia.