UNIVERSIDAD DE TARAPACA
ARICA - CHILE

PROMULGA ACUERDO N° 2354 DE LA JUNTA DIRECTIVA DE LA UNIVERSIDAD DE TARAPACÁ, APRUEBA LA ACTUALIZACIÓN DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO N° 00.916/2025.

Arica, 24 de julio 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° 16, de 27 de diciembre de 2023, publicado el 11 de julio de 2024, del Ministerio de Educación; D.F.L. N.º 150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública; Resolución N°36, de 23 diciembre de 2024, de la Contraloría General de la República; Resolución Exenta CONTRAL. Nº0.01/2002, de fecha 14 de enero 2002, Resolución Exenta CONTRAL. N°0.01/2025, de fecha 26 de marzo de 2025; Sesión extraordinaria N° 240 de la Junta Directiva, de julio 18 de 2025; Certificado N° 2354 de la Junta Directiva, de julio 18 de 2025; Traslado T/Contral N° 510/2025, de julio 23 de 2025; , los documentos adjuntos y las facultades que me confiere la letra I), punto Nº 3 del artículo 11, del D.F.L. Nº 150, ya citado en relación con el decreto Nº1605/84, de diciembre 14 de 1984; Decreto TRA Nº 335/9/2025, tomado de razón el 06 de mayo de 2024.

CONSIDERANDO:

Que, la Universidad de Tarapacá es una persona jurídica autónoma, descentralizada funcionalmente que cuenta con personalidad jurídica y patrimonio propio. Se relaciona con el Presidente de la República mediante el Ministerio de Educación.

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, en la Sesión extraordinaria N° 240 de la Junta Directiva, de fecha 18 de julio de 2025, a proposición del Rector, Dr. Emilio Rodriguez Ponce, y ante la presentación efectuada por el Director de Gestión Digital y Transparencia, Sr. Mauricio Arriagada Benítez, se presenta la Política General de Seguridad de la Información de la Universidad de Tarapacá.

En mérito del Certificado del Acuerdo N° 2354 de la Junta Directiva, de fecha 18 de julio de 2025, por unanimidad de los directores, se adopta el Acuerdo N° 2354, de "*aprobar la actualización de la Política General de Seguridad de la Información de la Universidad de Tarapacá.*"

Que, mediante Traslado T/Contral N° 510/2025, de julio 23 de 2025, la Contralora (S) de la Universidad, Sra. Paulina Ortuño Fariña, devuelve a la Secretaria de la Universidad, el Decreto Exento N° 00.884/2025, de fecha 18 de julio de 2025, con las observaciones indicadas en el mismo.

DECRETO:

1.- **Promulgase** el Acuerdo N° 2354 de la Junta Directiva de la Universidad de Tarapacá, aprobado en la sesión extraordinaria N° 240, realizada con fecha 18 de julio de 2025, adoptando el siguiente acuerdo:

"ACUERDO N°2354

Por unanimidad de los directores presentes Sres./as; Presidenta Sra. Rosa María Alfaro Torres; Sr. Honorino Córdova Valdés; Sr. Nicolás Fleet Oyarce; Sr. Renato Briceño Espinoza; Sr. Horacio Diaz Rojas, la Junta Directiva, atendida la presentación del Director de Gestión Digital y Transparencia, Sr. Mauricio Arriagada Benítez, y a proposición del Rector de la Universidad, Dr. Emilio Rodríguez Ponce, **ACUERDAN APROBAR LA ACTUALIZACIÓN DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE TARAPACÁ**, expuesto mediante una (1) exposición compuesta por nueve (09) diapositivas y un (1) documento compuesto por cuarenta y uno (41) paginas, rubricadas por el Secretario General de la Universidad de Tarapacá.

1. INTRODUCCIÓN

Los datos y la información, como otros activos de la Universidad de Tarapacá (UTA), son esenciales para la operación y continuidad de los servicios y requiere en consecuencia una protección adecuada, lo cual es especialmente importante en un entorno cada vez más digitalizado y conectado, donde la seguridad y privacidad de la información son cruciales para mantener la confianza pública.
Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor, y variado de amenazas y vulnerabilidades. La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en películas o grabada. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.
La seguridad de la información se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados, revisados y mejorados cuando fuese necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización [1].
En este contexto, se vuelve necesario definir lineamientos claros en materia de seguridad de la información de acuerdo al marco normativo vigente, a saber:

- Constitución Política de Chile / artículo 19/5 de la Constitución Política de Chile consagra la inviolabilidad de las comunicaciones privadas.
- Decreto Supremo 83: Norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma Chilena Oficial NCh-ISO 27002.0f2009, cuya norma indicada está basada en la norma internacional ISO/IEC 27002:2005.
- Ley 19.628: Ley de protección de la vida privada. Ley 19.927: Sobre delitos de pornografía infantil. Ley 17.336: Ley de propiedad intelectual.
- Ley 21.663 Ley Marco de Ciberseguridad.
- Decreto N° 164 (Política Nacional de Ciberseguridad 2023-2028)
- Norma Técnica de Seguridad de la Información y Ciberseguridad (Decreto 7/202
- Ley 20.285 Sobre Acceso a la Información Pública. Ley 21.180 De Transformación Digital del Estado.
- Ley 21.459 Establece normas sobre delitos informáticos.

1.0.1. DECLARACIÓN INSTITUCIONAL

La seguridad de la información es de responsabilidad de todos los organismos de la Universidad, por lo cual es necesaria integrar a todas las unidades administrativas y académicas para garantizar el apoyo manifiesto de las aut3oridades a las iniciativas tecnológicas y de seguridad.
Dicho apoyo permitirá promover e impulsar la implementación de la presente política, la cual estará siempre alineada con la misión y la visión de la Universidad de Tarapacá.
La Universidad de Tarapacá facilitará las herramientas, acceso a servicios y condiciones que permitan ejecutar la labor propia de cada miembro de la comunidad universitaria.

Dichos servicios deben ser utilizados en materias relacionadas directamente con la respectiva función de cada miembro de la comunidad universitaria o con el quehacer propio de la Universidad de Tarapacá.
En este sentido, se establece que los usuarios no podrán hacer uso de los sistemas o herramientas para propósitos personales de carácter comercial, con fines políticos u otro que no tenga relación con el ámbito universitario.

Cada miembro de la comunidad universitaria, tiene la responsabilidad de proteger la información confidencial de la universidad. El uso inapropiado de la información confidencial, expone a la Universidad de Tarapacá a riesgos de seguridad como filtración de información sensible, suplantación de identidad, accesibilidad a los servicios, litigios por aspectos legales, entre otros.

1.0.2. OBJETIVOS

Esta política se enfoca en alcanzar los siguientes objetivos:

1.Proteger eficientemente los activos de la información digitales institucionales asegurando la confiabilidad, integridad, autenticidad y disponibilidad.
2.Establecer la base para la definición de una estructura de procedimientos en materia de seguridad dentro de la Institución.
3.Establecer mecanismos de evaluación considerando encuesta de satisfacción para recabar experiencia usuaria, y de ellas identificar espacios de mejoras implementando una matriz de riesgo la cual deba ser revisado y monitoreada por la Unidad de Auditoría y Control Interno. de evaluación del cumplimiento de la presente política.
4.Establecer mecanismos de difusión de la presente política para el conocimiento de todo el personal perteneciente a la institución.
5.Establecer un proceso de revisión, evaluación y mejora continua de la presente política.

1.0.3. ALCANCE DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente política tiene un alcance integral que abarca todos los ámbitos relevantes de la seguridad de la información dentro de la Institución. Esto incluye la protección de activos digitales tales como datos personales [2] [3][4] y los derechos que pueden ejercer titulares sobre datos personales, documentos electrónicos, sistemas de información, infraestructuras tecnológicas y redes de comunicación.
Además, la implementación de esta política se extenderá a todas las áreas y procesos que impliquen el tratamiento de información, incluyendo los sistemas de almacenamiento, transmisión y procesamiento de datos, garantizando que estos estén protegidos contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad [5].
En caso de requerirse excepciones o ajustes a esta política, estos deberán ser evaluados y autorizados formalmente por el comité de seguridad de la información.

2.MARCO GENERAL DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A través de la presente política de Seguridad Informática, y por medio del Comité de Seguridad de la información (CSI), la Universidad de Tarapacá declara su voluntad de alinearse con la estrategia nacional de ciberseguridad cuyo propósito es el fortalecimiento de la estructura de gestión de seguridad de la información en la Red de Instituciones Públicas y Privadas y del ecosistema de instituciones científicas y de educación superior.

El propósito de esta política es instaurar un ciclo de mejoramiento continuo en el tiempo que permita alcanzar niveles adecuados de seguridad de los activos de la información relevantes de la Institución que permitan la adecuada gestión y continuidad de sus procesos.
Se entenderá como niveles adecuados de seguridad de los activos de información a los mecanismos que permitan proveer lo siguiente:

1. Confidencialidad: que la información esté debidamente protegida permitiendo el acceso solo a las personas autorizadas.
2. Integridad: que la información sea correcta y que pueda ser preservada en ese estado en el tiempo.
3. Autenticidad: que permita validar su origen.
4. Disponibilidad: que la información sea accesible por todos los sujetos facultados para acceder a ella.

2.0.1. ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Los roles y responsabilidades en materia de seguridad de la información, que cumplen con las directrices establecidas en la presente política general, son los siguientes:

- Comité de seguridad de la información (CSI)
- Oficial de seguridad de la información (OSI)
- Propietario de la información (PI)
- Usuario de la información (UI)

La seguridad informática deberá ser responsabilidad de toda la Institución compartida por todas las Autoridades universitarias, académicos y personal de gestión de la Universidad. Para ello el Comité de seguridad de la información (CSI) deberá coordinar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. Además, se incorpora un Oficial de Seguridad de la Información (OSI), quien cumplirá la función de impulsar la implementación de la presente Política.
Se deberá conformar un Comité de Seguridad de la Información integrado por Directivos pertinentes en la gestión de información, el cual, una vez conformado, deberá proponer un Oficial de Seguridad de la Información (OSI) el que será nombrado por el Rector para cumplir con las funciones operativas y representante institucional sobre los aspectos de seguridad de la información.

En la siguientes 2.1 se muestran los roles y responsabilidades:

Roles	Responsabilidades
1) Autoridades Universitarias	Las autoridades y jefaturas deberán supervisar que el personal de su dependencia cumpla con la presente política.
2) Comité de Seguridad de la Información (CSI)	a) Responsable del ciclo de vida de la política de seguridad informática. b) Velar por la implementación de los controles de seguridad en la plataforma tecnológica. c) Evaluar en forma anual el funcionamiento y cumplimiento de la política de seguridad a través de la matriz de riesgo como el mecanismo de control de daños.
3) Oficial de Seguridad de la Información (OSI)	a) Proponer al comité, desarrollar y actualizar las políticas de seguridad de la institución. b) Coordinar la correcta aplicación de la política velando por la implementación y evaluación. c) Coordinar la respuesta y tratamiento de incidentes de seguridad vinculados a los activos de la información institucionales. d) Mantener informado al Comité de Seguridad de la Información acerca del estado de cumplimiento y evaluación de la política de seguridad informática vigente. e) Mantener actualizado el registro de activos de la información digital. f) Promover acciones tendientes a la difusión y sensibilización respecto a la seguridad de la información a los funcionarios.
4) Director(a) de Gestión de Personas y Bienestar	Incorporar la aplicación y seguimiento de la política de seguridad en un plan de capacitación institucional al ingreso a la Institución. Velar por la inducción del personal en materias de seguridad de la información.
5) Director(a) de Gestión Digital y Transparencia	a) Apoyar en el plan de capacitación institucional.

Tabla 2.1. Roles y responsabilidades de la Política de Seguridad de la Información

3.POLÍTICAS

3.1. POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

3.1.1. GESTIÓN DE LA SEGURIDAD DE LA LAN

Para reducir los riesgos de seguridad de la red local (LAN) de la institución la Dirección de Gestión Digital y Transparencia en coordinación con la Dirección de Servicios y Logística realizarán los siguientes controles:

- Monitoreo periódico del estado de la LAN: Se deberá contar con equipamiento de red para monitorear de tráfico local entre las distintas reparticiones de la institución que permita la detección directa o indirecta de incidentes de seguridad o que afecten al rendimiento de la misma.
- Aislamiento del origen de incidencia: Si se detecta algún equipo conectado a la red local que provoque algún incidente de seguridad o afecte seriamente la disponibilidad y rendimiento de ella, se procederá a desconectar de la red a dicho equipo y notificará al respectivo administrador o encargado para su resolución.
- Segmentación de la LAN: La red local deberá estar segmentada en VLANs correspondiente a cada repartición, sector o edificio para reducir la propagación de tráfico de tipo broadcast y además permitir identificar y aislar los orígenes de tráfico. Adicionalmente cada repartición deberá contar con un registro de direcciones IP asociadas a cada equipo conectado a la red cableada.

3.1.2. ENLACES EXTERNOS

Para reducir el riesgo de incidentes de seguridad originados desde el exterior de la red local de la institución o la propagación de incidentes, desde el interior se contará con las siguientes medidas en coordinación con la Dirección de Gestión Digital y Transparencia y la Dirección de Servicios y Logística:

- Monitoreo periódico de los enlaces externos: Se deberá contar con equipamiento de red que permita medir el rendimiento, uso e incidentes de seguridad.
- Bloqueo de acceso: A todo equipo interno que se detecte que origine incidentes de seguridad hacia el exterior, le será bloqueado el acceso desde y hacia Internet y el encargado será notificado. Esta medida permanecerá hasta que el encargado informe que la situación haya sido remediada.
- Monitoreo del bloqueo: Todo origen externo que se detecte como fuente de incidentes de seguridad hacia la red institucional será bloqueado hasta que se pueda constatar que la actividad haya cesado.

3.1.3. APERTURAS DE PUERTOS DE RED

Para reducir el riesgo de acceso remoto a cualquier equipo interno de la red institucional se aplicarán las siguientes medidas:

- La Dirección de Gestión Digital y Transparencia mantendrá filtrado el acceso desde el exterior a todos los equipos que pertenezcan a la red institucional.
- La apertura del acceso a un equipo desde el exterior deberá solicitarse a través de un formulario electrónico indicando la dirección IP, puerto o servicio y responsable del equipo o encargado.
- La seguridad del servicio expuesto será de exclusiva responsabilidad del responsable del equipo o encargado y se regirá bajo las medidas indicadas anteriormente. Sin perjuicio de lo anterior se podrá asesorar y/o apoyar en la aplicación de medidas que permitan reducir los riesgos de seguridad del servicio respectivo.

3.1.4. SEGURIDAD DE COMPUTADORES DE ESCRITORIO Y/O LAPTOP

El responsable de la seguridad de la información de los equipos asignados al personal perteneciente a la institución será en primera instancia el usuario del equipo. Para ello deberá cumplir con las siguientes medidas:

- Deberá contar con una clave de ingreso que cumpla con los requerimientos mínimos de complejidad análogos a los utilizados para la cuenta UTA.
- Si se requiere dejar el equipo desatendido deberá bloquearse en forma inmediata. El desbloqueo deberá realizarse por medio de una clave con las mismas características del punto anterior.
- Deberá contar con el sistema operativo institucional licenciado con parches actualizados.
- Deberá contar con el software de seguridad (antivirus) institucional. De contar con otro software este deberá estar debidamente licenciado institucionalmente y actualizado.
- Todo programa computacional instalado deberá estar debidamente licenciado.
- Para resguardar la disponibilidad e integridad de la información, se deberá mantener respaldos en los espacios de almacenamientos que disponga la Institución.

3.1.5. SEGURIDAD DE OTROS EQUIPOS

El responsable de la seguridad de la información de otros equipos tales como servidores, estaciones de trabajo, IoT (Internet de la Cosas) será de exclusiva responsabilidad del usuario o administrador de estos, debiendo aplicar las mismas medidas o equivalentes a los señalados en el punto anterior según sea el caso. Las Dirección de Gestión Digital y Transparencia y la Dirección de Servicios y Logística brindarán apoyo en la habilitación de

los accesos mediante solicitud de formulario, siendo el solicitante el responsable de la administración.
La implementación de servicios y servidores deberán ser informados a las direcciones de Gestión Digital y Transparencia, y Servicios y Logística con anterioridad.

3.1.6. SEGURIDAD DE LA INFRAESTRUCTURA DE SISTEMAS DE SERVIDORES

Todo equipamiento que intervenga en el funcionamiento de sistemas críticos deberá seguir la siguiente política:

- Deberá contar con contrato de mantención o garantía vigente, si aplica, de manera que minimizar la pérdida de información o interrupción del servicio por fallas físicas.
- Deberá contar con elementos de alta disponibilidad (HA), tales como:
    - Fuentes de poder redundantes
    - Arreglos de discos locales Hot Swap
    - Ventiladores internos redundantes
- Deberá contar con sistemas de respaldo cuyo retención y frecuencia serán determinadas según la criticidad y naturaleza de la información. Estos respaldos deberán tener un plan de revisión periódico para asegurar la recuperación de la información cuando sea necesario.

3.2. POLÍTICA DE SEGURIDAD FÍSICA

El objetivo de esta política es establecer las directrices y medidas necesarias para proteger los activos físicos, infraestructuras y recursos de la Institución contra amenazas físicas que puedan comprometer su integridad, disponibilidad y funcionamiento. Esta política busca reducir los riesgos de daños, pérdidas, robos, accesos no autorizados, y cualquier otra acción que pueda afectar negativamente la operatividad de la organización y la seguridad de su información y activos.

3.2.1. SEGURIDAD DEL EDIFICIO

Se deberá contar con los resguardos necesarios para minimizar el acceso no autorizado a sus dependencias y en particular a la Sala de Servidores. Será la Dirección de Servicios y Logística encargada de velar por las medidas de protección y vigilancia del inmueble, en particular durante horarios no hábiles, para cumplir con lo anterior.

3.2.2. ACCESO A SALA DE SERVIDORES

El acceso al recinto donde se encuentran alojados los activos de la información más relevantes de la institución, la sala de servidores será restringido solo al personal autorizado. Para ello la sala deberá contar con los siguientes controles:

Control de acceso por medio de credencial autorizado en el sistema.
Puerta de ingreso, ventana y sala reforzado para minimizar el riesgo de ingreso en forma forzosa.
Ante la necesidad de hacer ingreso a personas no autorizado, ya sea personal técnico interno o externo a la institución, deberá ser acompañado y supervisado por personal previamente autorizado quedando registro de éste.
Ingresos por personal no técnico, ya sea interno o externo, deberán ser evaluados por el encargado de la sala de servidores y aplicarán las mismas medidas del punto anterior.

3.2.3. SUMINISTRO ELÉCTRICO

La sala de servidores deberá estar protegido contra posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

El cableado eléctrico, tablero y enchufes deberán evitar puntos únicos de falla en la distribución de energía al interior de la sala.
Contar con un suministro de energía ininterrumpido (UPS) para asegurar el funcionamiento continuo del equipamiento que sustenta las operaciones críticas de la institución. Este deberá contar con características que reduzcan los puntos únicos de falla, tablero de bypass para efectuar mantenimiento sin interrumpir el servicio y contrato de mantención vigente y permanente.
Disponer de un generador de respaldo ante una falla prolongada en el suministro de energía. Deberá contar con un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado de tiempo.
El encendido del generador deberá ser automático y en un tiempo significativamente menor a la autonomía de la UPS. Para ello se requerirá de un tablero de transferencia automático.
Para asegurar lo anterior se deberán realizar pruebas de encendido permanente, inspección regular y/o mantención preventiva y correctiva desde la Dirección de Servicios y Logística.
Sin perjuicio de lo anterior se deberá elaborar un plan de contingencia para aquellos casos en que no se pueda dar continuidad al suministro eléctrico, ya sea por causas de la naturaleza, humanas, o para tareas de mantención del cableado eléctrico interno o equipos involucrados.

3.2.4. SISTEMA DE CLIMATIZACIÓN

La sala de servidores deberá contar con un sistema de climatización para asegurar la temperatura de la sala entre los 18° y 24° grados Celsius sin gradientes superiores a 2° por hora y una humedad relativa entre los entre un 40 % y un 60 %. El sistema deberá mantener su funcionamiento ante una interrupción prolongada del suministro eléctrico. Además, deberá ser tolerante a fallas para permitir la continuidad de operación.

3.3. POLÍTICA DE CONTROL DE ACCESO DIGITAL

El objetivo de esta política es asegurar que el acceso a la información esté limitado solo a usuarios autorizados y a los niveles necesarios para cumplir con sus funciones.

3.3.1. GESTIÓN DE IDENTIDAD

Toda persona que cuente con un vínculo con la institución, ya sea alumno de pre o postgrado, funcionario, etc. deberá contar con credenciales de acceso Institucional, el cual permitirá identificar a la persona mediante la combinación de un usuario y contraseña u otro factor de autenticación adicional dependiendo de la criticidad del acceso.

3.3.2. CREDENCIALES DE ACCESO INSTITUCIONAL

La Dirección de Gestión Digital y Transparencia será la encargada de generar las credenciales de acceso Institucional a Sistemas Informáticos, la cual será el mecanismo principal de autenticación y acceso a todos los servicios y sistemas institucionales. Además, deberá proveer un mecanismo de asignación de roles asociadas a las credenciales para autorizar el acceso a los diferentes sistemas.

3.3.3. CONTRASEÑAS A SISTEMAS INFORMÁTICOS INSTITUCIONALES

Considerando que las contraseñas son el elemento principal para la autenticación de usuarios se regirán por la siguiente política:

El resguardo de la contraseña es de exclusiva responsabilidad del usuario. Para ello deberá seguir las siguientes indicaciones:

- Mantener las contraseñas en secreto.
- Cambiar la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Los usuarios y contraseñas son intransferibles.

3.3.4 ACCESO A APLICACIONES INSTITUCIONALES

El acceso a las aplicaciones corporativas de tipo Cliente Servidor se permitirá bajo las siguientes condiciones:

- El usuario deberá estar conectado a la red local de la UTA, ya sea en forma cableada o WiFi corporativa, donde se implementarán un segundo factor de autenticación.
- La autenticación del usuario será mediante credencial de acceso Institucional.
- Ante la necesidad de conectarse desde fuera de la red UTA deberá utilizar la VPN-SSL institucional previa autorización de su jefatura directa.

- El usuario deberá contar con la autorización previa, según los privilegios solicitados en concordancia con el rol y tarea a efectuar.

3.3.5. ACCESO A LA BASE DE DATOS INSTITUCIONAL

La Base de Datos (BD) Corporativa contiene los principales activos de información de la institución. Por lo anterior el acceso a ella será restringido por medio de las siguientes medidas:

- El acceso a la BD solo se podrá realizar por medio de las aplicaciones administrativas desarrolladas por la Institución.
- Solo el personal autorizado según sus respectivos roles tendrá acceso a la BD por medio de las aplicaciones administrativas y se autenticará utilizando su credencial de acceso remoto.
- El acceso a la BD por medio de las aplicaciones administrativas deberá originarse solo desde equipos conectados a la red de la institución. No se permiten accesos remotos a menos que estos se realicen por medio de la VPN institucional y autorizados previamente por la jefatura correspondiente.
- El acceso a la BD desde otras aplicaciones deberá realizarse por medio de servidores de aplicaciones que cuenten con control de acceso.
- Aplicaciones desarrolladas por externos a la Dirección de Gestión Digital y Transparencia que requieran acceso a la BD deberán ser realizadas por medio de un API que provea control de acceso, autenticación y control de carga.
- Cualquier tipo de acceso a la BD deberá ser autorizada y coordinada con los propietarios de la información.

3.4. POLÍTICAS DE SEGURIDAD EN EL DESARROLLO DE SISTEMAS

La seguridad de la información en los sistemas desarrollados por la institución deberá ser incorporado desde el diseño y considerando los principales riesgos a los cuales pueda verse expuesto los activos de información relevantes. Se entenderá como activos de información relevantes todos aquellos que intervengan directamente en los procesos misionales de la institución. Para ello se establece la siguiente política:

- Se deberá contar con tres ambientes para el desarrollo de sistemas: Desarrollo, Testing (QA) y Producción.
- Los ambientes de Desarrollo y Testing debieran estar separados del ambiente de producción, ya sea en instancias físicas o virtuales.
- Para el ambiente de Desarrollo no se deberá utilizar datos de producción para pruebas internas.
- En aquellos sistemas donde es necesario almacenar contraseñas estas deberán ser cifradas mediante algoritmos criptográficos que aseguren la confidencialidad de la información.

- Toda información considerada sensible que viaje por la red deberá realizase utilizando protocolos que aseguren la integridad y confidencialidad, tales como SSL, HTTPS, etc.

3.5. POLÍTICAS DE SEGURIDAD DE LAS PERSONAS

Esta política tiene como objetivos asegurar el uso de la interacción de usuarios con los sistemas de información.

3.5.1. COMPETENCIAS MÍNIMAS

Los usuarios deberán contar con competencias mínimas sobre el uso de las tecnologías de información y de seguridad que deben ser comprobadas y validadas por sus respectivas jefaturas.

3.5.2. DURANTE LA CONTRATACIÓN DE PERSONAL

Todo personal contratado por la institución deberá conocer la presente política y aceptarla como parte del proceso de contratación. Su registro e ingreso en el Sistema de Personal automáticamente lo facultará para contar con las credenciales de acceso Institucional.

3.5.3. DURANTE LA DESVINCULACIÓN DE PERSONAL

La Dirección de Gestión de Personas y Bienestar deberá informar periódicamente a la Dirección de Gestión Digital y Transparencia el personal desvinculado de la institución de manera de proceder a bloquear el acceso a los respectivos sistemas según los roles asignados. Las excepciones para mantener credenciales de acceso Institucional, en particular para el uso del correo electrónico (jubilados, profesores eméritos, etc.) deberán ser solicitados a la Dirección de Gestión de Personas y Bienestar.

3.5.4. TRABAJO A DISTANCIA

El personal de la institución que solicite a la modalidad de trabajo a distancia y que requiera hacer uso de los sistemas de información deberá cumplir con lo siguiente:

- El dispositivo a utilizar deberá contar con un software de seguridad que prevenga incidentes asociados a Malware y otros.
- Se deberá evitar el uso de equipos con cuentas compartidas o de uso público.
- Para tomar el control remoto de algún dispositivo ubicado en la red de la UTA deberá utilizar la VPN y contar con las autorizaciones respectivas de su jefatura directa.
- Será de responsabilidad del usuario velar por la seguridad de la conexión remota.

3.6. POLÍTICAS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN ANTE DESASTRES

El objetivo de esta política es asegurar la disponibilidad y recuperación de datos en caso de incidentes de pérdida de información.

3.6.1. REALIZACIÓN DE COPIAS DE SEGURIDAD

Se deben realizar copias de seguridad periódicas de toda la información crítica. La frecuencia dependerá de la importancia de los datos y en un proceso que permita dar continuidad al servicio informático Institucional.

3.6.2. ALMACENAMIENTO DE COPIAS DE SEGURIDAD

Las copias deben almacenarse en un lugar seguro, idealmente en un sitio remoto y con acceso restringido.

3.6.3. PRUEBAS DE RECUPERACIÓN

Las copias de seguridad deben probarse regularmente para verificar su integridad y efectividad en la recuperación de información.

3.6.4. PLAN DE CONTINUIDAD DE NEGOCIO

La universidad debe contar con un plan de continuidad para garantizar la operación en caso de incidentes graves, incluyendo desastres naturales.

3.7. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de esta política es detectar, gestionar y responder a incidentes de seguridad de la información para minimizar el impacto en la universidad.

3.7.1. DETECCIÓN Y NOTIFICACIÓN DE INCIDENTES

Todo miembro de la universidad debe reportar cualquier incidente de seguridad a la brevedad.

3.7.2. PLAN DE RESPUESTA A INCIDENTES

Se debe implementar un plan para contener, erradicar y recuperar sistemas comprometidos, además de analizar las causas para prevenir futuros incidentes.

3.7.3. DOCUMENTACIÓN Y LECCIONES APRENDIDAS

Cada incidente debe documentarse y revisarse para mejorar los procesos de seguridad en la universidad.

3.8. POLÍTICA DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN

El objetivo de esta política es proteger los activos de información mediante un adecuado control y clasificación de la información.

3.8.1. INVENTARIO DE ACTIVOS

Todos los activos de información (hardware, software, datos y documentos) deben ser registrados y etiquetados en un inventario detallado.

3.8.2. CLASIFICACIÓN DE LA INFORMACIÓN

La información debe clasificarse en función de su sensibilidad (confidencial, interna, pública, restringida, sensible, estadística o crítica) y aplicarse controles de seguridad acordes a cada nivel.

3.8.3. RESPONSABILIDAD DE ACTIVOS

Cada activo debe tener un responsable designado encargado de su protección y de aplicar las políticas de seguridad correspondientes.

3.8.4. POLÍTICA DE USO ACEPTABLE

Los activos de la universidad deben usarse únicamente para actividades relacionadas con las funciones de la institución. El uso indebido está prohibido.

3.9. POLÍTICA DE CONSERVACIÓN Y DESTRUCCIÓN DE INFORMACIÓN

El objetivo es establecer los lineamientos para la conservación, almacenamiento y destrucción segura de la información generada y/o custodiada por la Universidad de Tarapacá, en cumplimiento de la normativa vigente en materia de educación superior, protección de datos personales, transformación digital y gestión documental. Esta política también se alinea con los principios establecidos en la Ley N.º 21.180 sobre Transformación Digital del Estado, la Ley N.º 19.799 sobre Firma Electrónica, la Ley N.º 21.459 sobre Protección de Datos Personales en el Tratamiento Automatizado, y la Resolución Exenta N.º 173 del Ministerio de las Culturas, las Artes y el Patrimonio.

3.9.1. CONSERVACIÓN DE LA INFORMACIÓN

La información académica, administrativa y financiera será conservada por los plazos establecidos en la normativa sectorial o en los planes de archivo institucionales. Los datos personales serán conservados solo por el tiempo necesario para cumplir con la finalidad para la cual fueron recolectados, salvo obligación legal de conservación. En el caso de documentación digital, se aplicarán los principios establecidos en la Ley N.º 18.845, asegurando la integridad, autenticidad y disponibilidad de los documentos electrónicos.

3.9.2. DESTRUCCIÓN DE LA INFORMACIÓN

La destrucción de documentos físicos o digitales que contengan datos personales o información sensible deberá realizarse mediante métodos seguros e irreversibles (trituración, borrado seguro, destrucción física de soportes). Todo proceso de eliminación deberá ser documentado, incluyendo fecha, responsable, método utilizado y tipo de información destruida.
La eliminación de documentos originales microcopiados o digitalizados se regirá por el marco normativos de Ley 19.628 de Protección de la Vida Privada que establece los principios y normas para el tratamiento de datos personales, incluyendo la obligación de las universidades de proteger la información que manejany Ley 21.719 de Protección de Datos Personales introduce nuevas regulaciones y desafíos para la protección de datos personales en Chile, incluyendo las universidades.

3.10. POLÍTICA DE PROTECCIÓN CONTRA MALWARE

El objetivo de esta política es proteger los sistemas de la Universidad contra software malicioso que pueda afectar la integridad y disponibilidad de la información.

3.10.1. INSTALACIÓN Y ACTUALIZACIÓN DE SOFTWARE ANTIMALWARE

Todos los equipos institucionales conectados a la red universitaria deben contar con software antimalware actualizado que incluya protección contra virus, spyware, ransomware, entre otros a cargo de la Dirección de Servicios y Logística.

3.10.2. CAPACITACIÓN Y CONCIENTIZACIÓN

Se deben realizar campañas informativas a través de distintos medios de comunicación sobre los riesgos del malware y las prácticas para evitarlos, como no abrir correos sospechosos ni descargar archivos de fuentes desconocidas.

3.10.3. MONITOREO Y RESPUESTA A INCIDENTES

La Dirección de Gestión Digital y Transparencia debe monitorear continuamente la red para identificar y mitigar posibles amenazas. Además, debe contar con un plan de respuesta a incidentes específico para actividad sospechosa.

3.11. POLÍTICA DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

El objetivo de esta política es establecer las directrices y normas para el uso adecuado del correo electrónico institucional, con el fin de proteger la seguridad, integridad y reputación de la Institución. Se espera que el correo institucional sea utilizado de manera responsable,

ética y en línea con los valores de la universidad, asegurando que apoye las actividades académicas, administrativas e investigativas de la institución.
La política aplica a todos los miembros de la comunidad universitaria, incluidos funcionarios académicos, funcionarios de gestión, estudiantes, y cualquier otra persona o entidad que tenga acceso a una cuenta de correo electrónico proporcionada por la universidad.

3.11.1. USO ACEPTABLE

- El correo electrónico institucional debe usarse exclusivamente para actividades relacionadas con la labor académica, administrativa y de investigación de la universidad.
- Se prohíbe el uso del correo institucional para fines personales, comerciales o actividades que no estén alineadas con los intereses y objetivos de la universidad.
- Los correos deben ser utilizados de acuerdo con las políticas de confidencialidad y privacidad de la institución, asegurando el correcto tratamiento de la información sensible o confidencial.

3.11.2. CONFIDENCIALIDAD Y SEGURIDAD

- Los usuarios deben proteger sus credenciales de acceso (por ejemplo usuario y contraseña) y no compartirlas con terceros. La universidad no se hace responsable de los daños derivados del uso indebido de las credenciales de acceso.
- No está permitido enviar información confidencial, privada o sensible sin las debidas medidas de seguridad (como cifrado o acceso restringido).
- En caso de pérdida o compromiso de la cuenta, y que no pueda ser recuperado por el/la usuario/a, el usuario debe notificarlo de inmediato a la Dirección de Gestión Digital y Transparencia para tomar las medidas correctivas necesarias.

3.11.3. CONTENIDO DE LOS MENSAJES

- Se espera que el contenido de los correos sea respetuoso. Queda estrictamente prohibido el envío de mensajes ofensivos, discriminatorios, difamatorios, que inciten al odio, o que infrinjan derechos de terceros.
- No está permitido el uso del correo institucional para el envío de correos en masa no autorizados (SPAM) o mensajes de cadena.

3.11.4. RESPONSABILIDAD DE LOS MENSAJES

- Los usuarios son responsables de la información que envían a través del correo institucional. La universidad no se hace responsable de las opiniones o afirmaciones personales expresadas en los correos enviados desde cuentas institucionales

3.11.5. ALMACENAMIENTO Y GESTIÓN DE CUENTAS

- La capacidad de almacenamiento del correo institucional es limitada. Los usuarios deben hacer un uso razonable del espacio y eliminar correos que no sean necesarios para el desempeño de sus funciones, siempre que sea posible de acuerdo a la norma [4].
- Las cuentas de correo institucional (académicos y gestión) serán desactivadas y eliminadas cuando el usuario ya no pertenezca a la comunidad universitaria. Se crearán mecanismos para establecer este proceso a través de la Vicerrectoría de Administración y Finanzas, dependiendo de los casos que se presenten.
- En el caso de alumnos, se les mantendrá la cuenta con el propósito de tener contacto con egresados de la Institución, la cual tendrá reducción de espacio para una mejor administración de los recursos Institucionales.
- Los dominios de los correos electrónicos institucionales serán establecidos por el comité ad-hoc creado para este propósito.
- Para prestadores de servicio (contrato a honorarios):

    - Se le asignará un correo electrónico con dominio a ser definido por comité designado para tal propósito.
    - El correo electrónico permanecerá activo sólo durante el período que dure el contrato de honorario.

4. MECANISMOS DE DIFUSIÓN

La presente política debe ser conocida por todos/as los/as funcionarios/as de la Universidad de Tarapacá, para ello es necesario contar con una difusión a través de la Intranet y en el sitio web oficial de la UTA para las partes interesadas externas. La difusión de esta política debe ir acompañada, siempre que sea posible, de capacitaciones continuas. Asimismo, se implementará un programa de inducción para los/as funcionarios/as que se incorporen a la Universidad de Tarapacá, con el objetivo que toda dotación se sensibilice en uso y protección de los activos de la información como parte del quehacer institucional y del desarrollo de las personas.

5. PERÍODO DE REVISIÓN

La revisión y mantención de la presente política será realizada por el Oficial de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad y la máxima autoridad universitaria.
La presente política deberá ser revisada y aprobada por el Comité de Seguridad, de acuerdo a las necesidades de la Universidad una vez al año contados desde su publicación. Sin embargo, esta política podrá ser revisada y actualizada antes de cumplirse este periodo según requerimiento de alguno de sus miembros o por alguna circunstancia coyuntural que lo requiera, que afecten la adecuada protección de la información, considerando como tales entre otros, cambios a nivel estructural de la Universidad, en la misión, objetivos

estratégicos, productos estratégicos, personal y/o cambios tecnológicos que impacten la seguridad de la información, entre otros. Hechos los cambios y aprobación, el Oficial de seguridad de la Información deberá difundir la nueva versión.

6. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de la presente política dará lugar a las medidas disciplinarias establecidas en el Estatuto Administrativo, así como en las ordenanzas académicas y estudiantiles, en virtud de las infracciones a los deberes establecidos en dichas normativas. Lo anterior es sin perjuicio de la aplicación de los protocolos institucionales vinculados a la Ley N.° 21.369, la Ley Karin u otras normativas equivalentes que resulten pertinentes, cuando corresponda. Asimismo, las personas contratadas como prestadores de servicios a honorarios deberán considerar como infracción a los deberes establecidos en sus respectivos contratos el incumplimiento de la presente política, lo que dará lugar a las sanciones contempladas en dichos contratos.

7. GLOSARIO DE TÉRMINOS

Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.
Activo de Información: Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.
Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado o afectado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.
Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.
Cliente Servidor: Modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.
Confidencialidad: Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.
Control de Seguridad: Conjunto de estándares, buenas prácticas y normativas que permiten administrar los riesgos en las tecnologías de la información.

Disponibilidad: Atributo de los activos y activos de información, relativo a su accesibilidad y utilización a requerimiento de una entidad o proceso autorizado.
Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
Estación de Trabajo: Equipo computacional conectado a una red de computadores que facilita a los usuarios el acceso a los servidores y periféricos de la red.
Evaluación de Riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la institución) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.
Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.
Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.
Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.
Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.
Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.
Programa malicioso (malware): Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora. También se denominan malware.
Red local: En términos de informática, una red local o LAN (del inglés Local Area Network) es un conjunto de dispositivos (como computadores, impresoras, servidores, teléfonos, etc.) interconectados entre sí dentro de un área geográfica limitada, como una casa, oficina, edificio o campus
Reglamento: Decreto supremo Nº 4, de 2020, del Ministerio Secretaría General de la Presidencia, que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley Nº 21.180 sobre Transformación Digital del Estado.
Restricción del acceso: Acción consistente en la delimitación de acceso de los funcionarios, estudiantes o terceras partes a determinados recursos físicos o lógicos.
Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Servidor: Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.

Sistema informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.

Sistema de comunicaciones electrónicas: Se refiere a todo medio o dispositivos que permite comunicarse. Entiéndase: correo electrónico, mensajería instantánea (por ejemplo WhatsApp, Instagram, Discord, WeChat, Facebook Messenger, Line, Viber, Snapchat, Skype u otros), Teleconferencia (por ejemplo Skype, Zoom, Microsoft Team, Webex, Jitsi u otros), Telefonía fija y móvil, u otros.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

Trabajo a distancia: aquel en el que el trabajador o funcionario presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

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

ALVARO PALMA QUIROZ
Secretario General de la Universidad

JORGE BERNAL PERALTA
Rector (S) de la Universidad

UNIVERSIDAD DE TARAPACA CONTRALORIA ARICA

24 JUL 2025

JBP. APQ. lza.

UNIVERSIDAD DE TARAPACÁ
ARICA – CHILE

CERTIFICADO DE ACUERDO
JUNTA DIRECTIVA

Que, el ministro de fe que suscribe da fe que en sesión extraordinaria N°240, de fecha 18 de julio de 2025, la Junta Directiva de la Universidad de Tarapacá, adopta el siguiente acuerdo:

"ACUERDO N°2354

Por unanimidad de los directores presentes Sres./as; Presidenta Sra. Rosa María Alfaro Torres; Sr. Honorino Córdova Valdés; Sr. Nicolás Fleet Oyarce; Sr. Renato Briceño Espinoza; Sr. Horacio Diaz Rojas, la Junta Directiva, atendida la presentación del Director de Gestión Digital y Transparencia, Sr. Mauricio Arriagada Benítez, y a proposición del Rector de la Universidad, Dr. Emilio Rodríguez Ponce, **ACUERDAN APROBAR LA ACTUALIZACIÓN DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE TARAPACÁ,** expuesto mediante una (1) exposición compuesta por nueve (09) diapositivas y un (1) documento compuesto por cuarenta y uno (41) paginas, rubricadas por el Secretario General de la Universidad de Tarapacá."

DOY FE

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

ÁLVARO PALMA QUIROZ
SECRETARIO GENERAL DE LA UNIVERSIDAD

UNIVERSIDAD DE TARAPACÁ
Universidad del Estado

DGDT
Dirección de Gestión
Digital y Transparencia

Política General de Seguridad de la Información de la Universidad de Tarapacá

Firmado por:
Mauricio Javier Arriagada Benítez
Director de Dirección de Gestión
Digital y Transparencia
Fecha: 18-07-2025 15:06 CLT
Universidad de Tarapacá

Elaborado por: Dirección de Gestión Digital y Transparencia

Arica, 18 de julio de 2025

GPCP GPMH OASO JAZO

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

Índice general

1 Introducción 2

2 Marco General de las Políticas de Seguridad de la Información 6

3 Políticas 10

3.1 Política de Gestión de Comunicaciones y Operaciones 10

3.2 Política de Seguridad Física 13

3.3 Política de Control de Acceso Digital 16

3.4 Políticas de Seguridad en el Desarrollo de Sistemas 18

3.5 Políticas de Seguridad de las Personas 19

3.6 Políticas de Copias de Seguridad y Recuperación Ante Desastres 20

3.7 Política de Gestión de Incidentes de Seguridad de la Información 21

3.8 Política de Gestión de Activos de la Información 22

3.9 Política de Conservación y Destrucción de Información 23

3.10 Política de Protección Contra Malware 24

3.11 Política de Uso del Correo Electrónico Institucional 25

4 Mecanismos de Difusión 28

5 Período de Revisión 29

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

6 Incumplimiento y Sanciones 30

7 Glosario de Términos 31

8 Términos Abreviados 35

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO
ARICA - CHILE

Índice de tablas

2.1 Roles y responsabilidades de la Política de Seguridad de la Información 9

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO
DE LA
UNIVERSIDAD
ARICA - CHILE

Versión de Cambios

Versión	Fecha	Descripción del Cambio	Autor
1.0	31/07/2021	Políticas iniciales	Oscar Sagardia
1.1	10/07/2025	Actualización revisado por Comité de Seguridad de la Información	Mauricio Arriagada

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO
DE LA
UNIVERSIDAD

1. Introducción

Los datos y la información, como otros activos de la Universidad de Tarapacá (UTA), son esenciales para la operación y continuidad de los servicios y requiere en consecuencia una protección adecuada, lo cual es especialmente importante en un entorno cada vez más digitalizado y conectado, donde la seguridad y privacidad de la información son cruciales para mantener la confianza pública.

Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor, y variado de amenazas y vulnerabilidades. La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en películas o grabada. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados, revisados y mejorados cuando fuese necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización [1].

En este contexto, se vuelve necesario definir lineamientos claros en materia de seguridad de la información de acuerdo al marco normativo vigente, a saber:

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

- Constitución Política de Chile / artículo 19/5 de la Constitución Política de Chile consagra la inviolabilidad de las comunicaciones privadas.
- Decreto Supremo 83: Norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Norma Chilena Oficial NCh-ISO 27002.0f2009, cuya norma indicada está basada en la norma internacional ISO/IEC 27002:2005.
- Ley 19.628: Ley de protección de la vida privada.
- Ley 19.927: Sobre delitos de pornografía infantil.
- Ley 17.336: Ley de propiedad intelectual.
- Ley 21.663 Ley Marco de Ciberseguridad.
- Decreto N° 164 (Política Nacional de Ciberseguridad 2023-2028)
- Norma Técnica de Seguridad de la Información y Ciberseguridad (Decreto 7/202
- Ley 20.285 Sobre Acceso a la Información Pública.
- Ley 21.180 De Transformación Digital del Estado.
- Ley 21.459 Establece normas sobre delitos informáticos.

1.0.1. Declaración Institucional

La seguridad de la información es de responsabilidad de todos los organismos de la Universidad, por lo cual es necesaria integrar a todas las unidades administrativas y académicas para garantizar el apoyo manifiesto de las autoridades a las iniciativas tecnológicas y de seguridad.

Dicho apoyo permitirá promover e impulsar la implementación de la presente política, la cual estará siempre alineada con la misión y la visión de la Universidad de Tarapacá.

La Universidad de Tarapacá facilitará las herramientas, acceso a servicios y condiciones que permitan ejecutar la labor propia de cada miembro de la comunidad universitaria.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD

Dichos servicios deben ser utilizados en materias relacionadas directamente con la respectiva función de cada miembro de la comunidad universitaria o con el quehacer propio de la Universidad de Tarapacá.

En este sentido, se establece que los usuarios no podrán hacer uso de los sistemas o herramientas para propósitos personales de carácter comercial, con fines políticos u otro que no tenga relación con el ámbito universitario.

Cada miembro de la comunidad universitaria, tiene la responsabilidad de proteger la información confidencial de la universidad. El uso inapropiado de la información confidencial, expone a la Universidad de Tarapacá a riesgos de seguridad como filtración de información sensible, suplantación de identidad, accesibilidad a los servicios, litigios por aspectos legales, entre otros.

1.0.2. Objetivos

Esta política se enfoca en alcanzar los siguientes objetivos:

1. Proteger eficientemente los activos de la información digitales institucionales asegurando la confiabilidad, integridad, autenticidad y disponibilidad.
2. Establecer la base para la definición de una estructura de procedimientos en materia de seguridad dentro de la Institución.
3. Establecer mecanismos de evaluación considerando encuesta de satisfacción para recabar experiencia usuaria, y de ellas identificar espacios de mejoras implementando una matriz de riesgo la cual deba ser revisado y monitoreada por la Unidad de Auditoría y Control Interno. de evaluación del cumplimiento de la presente política.
4. Establecer mecanismos de difusión de la presente política para el conocimiento de todo el personal perteneciente a la institución.
5. Establecer un proceso de revisión, evaluación y mejora continua de la presente política.

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

1.0.3. Alcance de la Política General de Seguridad de la Información

La presente política tiene un alcance integral que abarca todos los ámbitos relevantes de la seguridad de la información dentro de la Institución. Esto incluye la protección de activos digitales tales como datos personales [2] [3][4] y los derechos que pueden ejercer titulares sobre datos personales, documentos electrónicos, sistemas de información, infraestructuras tecnológicas y redes de comunicación.

Además, la implementación de esta política se extenderá a todas las áreas y procesos que impliquen el tratamiento de información, incluyendo los sistemas de almacenamiento, transmisión y procesamiento de datos, garantizando que estos estén protegidos contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad [5].

En caso de requerirse excepciones o ajustes a esta política, estos deberán ser evaluados y autorizados formalmente por el comité de seguridad de la información.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO
DE LA
ARICA - CHILE

2. Marco General de las Políticas de Seguridad de la Información

A través de la presente política de Seguridad Informática, y por medio del Comité de Seguridad de la información (CSI), la Universidad de Tarapacá declara su voluntad de alinearse con la estrategia nacional de ciberseguridad cuyo propósito es el fortalecimiento de la estructura de gestión de seguridad de la información en la Red de Instituciones Públicas y Privadas y del ecosistema de instituciones científicas y de educación superior.

El propósito de esta política es instaurar un ciclo de mejoramiento continuo en el tiempo que permita alcanzar niveles adecuados de seguridad de los activos de la información relevantes de la Institución que permitan la adecuada gestión y continuidad de sus procesos.

Se entenderá como niveles adecuados de seguridad de los activos de información a los mecanismos que permitan proveer lo siguiente:

1. **Confidencialidad**: que la información esté debidamente protegida permitiendo el acceso solo a las personas autorizadas.
2. **Integridad**: que la información sea correcta y que pueda ser preservada en ese estado en el tiempo.
3. **Autenticidad**: que permita validar su origen.
4. **Disponibilidad**: que la información sea accesible por todos los sujetos facultados para acceder a ella.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL ARICA - CHILE

2.0.1. Roles y Responsabilidades en Seguridad de la Información

Los roles y responsabilidades en materia de seguridad de la información, que cumplen con las directrices establecidas en la presente política general, son los siguientes:

- Comité de seguridad de la información (CSI)
- Oficial de seguridad de la información (OSI)
- Propietario de la información (PI)
- Usuario de la información (UI)

La seguridad informática deberá ser responsabilidad de toda la Institución compartida por todas las Autoridades universitarias, académicos y personal de gestión de la Universidad. Para ello el Comité de seguridad de la información (CSI) deberá coordinar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. Además, se incorpora un Oficial de Seguridad de la Información (OSI), quien cumplirá la función de impulsar la implementación de la presente Política.

Se deberá conformar un Comité de Seguridad de la Informacion integrado por Directivos pertinentes en la gestión de información, el cual, una vez conformado, deberá proponer un Oficial de Seguridad de la Información (OSI) el que será nombrado por el Rector para cumplir con las funciones operativas y representante institucional sobre los aspectos de seguridad de la información.

En la siguientes 2.1 se muestran los roles y responsabilidades:

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD

Roles	Responsabilidades
1) Autoridades Universitarias	Las autoridades y jefaturas deberán supervisar que el personal de su dependencia cumpla con la presente política.
2) Comité de Seguridad de la Información (CSI)	a) Responsable del ciclo de vida de la política de seguridad informática. b) Velar por la implementación de los controles de seguridad en la plataforma tecnológica. c) Evaluar en forma anual el funcionamiento y cumplimiento de la política de seguridad a través de la matriz de riesgo como el mecanismo de control de daños.
3) Oficial de Seguridad de la Información (OSI)	a) Proponer al comité, desarrollar y actualizar las políticas de seguridad de la institución. b) Coordinar la correcta aplicación de la política velando por la implementación y evaluación. c) Coordinar la respuesta y tratamiento de incidentes de seguridad vinculados a los activos de la información institucionales. d) Mantener informado al Comité de Seguridad de la Información acerca del estado de cumplimiento y evaluación de la política de seguridad informática vigente. e) Mantener actualizado el registro de activos de la información digital. f) Promover acciones tendientes a la difusión y sensibilización respecto a la seguridad de la información a los funcionarios.
4) Director(a) de Gestión de Personas y Bienestar	a) Incorporar la aplicación y seguimiento de la política de seguridad en un plan de capacitación institucional al ingreso a la Institución. b) Velar por la inducción del personal en materias de seguridad de la información.
5) Director(a) de Gestión Digital y Transparencia	a) Apoyar en el plan de capacitación institucional.

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL ARICA - CHILE

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

6) Usuarios(as)	a) Conocer y cumplir la política de seguridad informática. b) Reportar cualquier incidente de seguridad que tengan conocimiento.

Tabla 2.1. Roles y responsabilidades de la Política de Seguridad de la Información

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO
DE LA
UNIVERSIDAD
CHILE

3. Políticas

3.1. Política de Gestión de Comunicaciones y Operaciones

3.1.1. Gestión de la seguridad de la LAN

Para reducir los riesgos de seguridad de la red local (LAN) de la institución la Dirección de Gestión Digital y Transparencia en coordinación con la Dirección de Servicios y Logística realizarán los siguientes controles:

- **Monitoreo periódico del estado de la LAN**: Se deberá contar con equipamiento de red para monitorear de tráfico local entre las distintas reparticiones de la institución que permita la detección directa o indirecta de incidentes de seguridad o que afecten al rendimiento de la misma.
- **Aislamiento del origen de incidencia**: Si se detecta algún equipo conectado a la red local que provoque algún incidente de seguridad o afecte seriamente la disponibilidad y rendimiento de ella, se procederá a desconectar de la red a dicho equipo y notificará al respectivo administrador o encargado para su resolución.
- **Segmentación de la LAN**: La red local deberá estar segmentada en VLANs correspondiente a cada repartición, sector o edificio para reducir la propagación de tráfico de tipo broadcast y además permitir identificar y aislar los orígenes de tráfico. Adicionalmente cada repartición deberá contar con un registro de direcciones IP asociadas a cada equipo conectado a la red cableada.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD

3.1.2. Enlaces Externos

Para reducir el riesgo de incidentes de seguridad originados desde el exterior de la red local de la institución o la propagación de incidentes, desde el interior se contará con las siguientes medidas en coordinación con la Dirección de Gestión Digital y Transparencia y la Dirección de Servicios y Logística:

- **Monitoreo periódico de los enlaces externos**: Se deberá contar con equipamiento de red que permita medir el rendimiento, uso e incidentes de seguridad.
- **Bloqueo de acceso**: A todo equipo interno que se detecte que origine incidentes de seguridad hacia el exterior, le será bloqueado el acceso desde y hacia Internet y el encargado será notificado. Esta medida permanecerá hasta que el encargado informe que la situación haya sido remediada.
- **Monitoreo del bloqueo**: Todo origen externo que se detecte como fuente de incidentes de seguridad hacia la red institucional será bloqueado hasta que se pueda constatar que la actividad haya cesado.

3.1.3. Aperturas de Puertos de Red

Para reducir el riesgo de acceso remoto a cualquier equipo interno de la red institucional se aplicarán las siguientes medidas:

- La Dirección de Gestión Digital y Transparencia mantendrá filtrado el acceso desde el exterior a todos los equipos que pertenezcan a la red institucional.
- La apertura del acceso a un equipo desde el exterior deberá solicitarse a través de un formulario electrónico indicando la dirección IP, puerto o servicio y responsable del equipo o encargado.
- La seguridad del servicio expuesto será de exclusiva responsabilidad del responsable del equipo o encargado y se regirá bajo las medidas

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL UNIVERSIDAD ARICA - CHILE

indicadas anteriormente. Sin perjuicio de lo anterior se podrá asesorar y/o apoyar en la aplicación de medidas que permitan reducir los riesgos de seguridad del servicio respectivo.

3.1.4. Seguridad de computadores de escritorio y/o laptop

El responsable de la seguridad de la información de los equipos asignados al personal perteneciente a la institución será en primera instancia el usuario del equipo. Para ello deberá cumplir con las siguientes medidas:

- Deberá contar con una clave de ingreso que cumpla con los requerimientos mínimos de complejidad análogos a los utilizados para la cuenta UTA.
- Si se requiere dejar el equipo desatendido deberá bloquearse en forma inmediata. El desbloqueo deberá realizarse por medio de una clave con las mismas características del punto anterior.
- Deberá contar con el sistema operativo institucional licenciado con parches actualizados.
- Deberá contar con el software de seguridad (antivirus) institucional. De contar con otro software este deberá estar debidamente licenciado institucionalmente y actualizado.
- Todo programa computacional instalado deberá estar debidamente licenciado.
- Para resguardar la disponibilidad e integridad de la información, se deberá mantener respaldos en los espacios de almacenamientos que disponga la Institución.

3.1.5. Seguridad de otros equipos

El responsable de la seguridad de la información de otros equipos tales como servidores, estaciones de trabajo, IoT (Internet de la Cosas) será de exclusiva responsabilidad del usuario o administrador de estos, debiendo aplicar las

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

mismas medidas o equivalentes a los señalados en el punto anterior según sea el caso. Las Dirección de Gestión Digital y Transparencia y la Dirección de Servicios y Logística brindarán apoyo en la habilitación de los accesos mediante solicitud de formulario, siendo el solicitante el responsable de la administración.

La implementación de servicios y servidores deberán ser informados a las direcciones de Gestión Digital y Transparencia, y Servicios y Logística con anterioridad.

3.1.6. Seguridad de la Infraestructura de Sistemas de Servidores

Todo equipamiento que intervenga en el funcionamiento de sistemas críticos deberá seguir la siguiente política:

- Deberá contar con contrato de mantención o garantía vigente, si aplica, de manera que minimizar la pérdida de información o interrupción del servicio por fallas físicas.
- Deberá contar con elementos de alta disponibilidad (HA), tales como:
  - Fuentes de poder redundantes
  - Arreglos de discos locales Hot Swap
  - Ventiladores internos redundantes
- Deberá contar con sistemas de respaldo cuyo retención y frecuencia serán determinadas según la criticidad y naturaleza de la información. Estos respaldos deberán tener un plan de revisión periódico para asegurar la recuperación de la información cuando sea necesario.

3.2. Política de Seguridad Física

El objetivo de esta política es establecer las directrices y medidas necesarias para proteger los activos físicos, infraestructuras y recursos de la Institución contra amenazas físicas que puedan comprometer su integridad,

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE
APS

disponibilidad y funcionamiento. Esta política busca reducir los riesgos de daños, pérdidas, robos, accesos no autorizados, y cualquier otra acción que pueda afectar negativamente la operatividad de la organización y la seguridad de su información y activos.

3.2.1. Seguridad del edificio

Se deberá contar con los resguardos necesarios para minimizar el acceso no autorizado a sus dependencias y en particular a la Sala de Servidores. Será la Dirección de Servicios y Logística encargada de velar por las medidas de protección y vigilancia del inmueble, en particular durante horarios no hábiles, para cumplir con lo anterior.

3.2.2. Acceso a Sala de Servidores

El acceso al recinto donde se encuentran alojados los activos de la información más relevantes de la institución, la sala de servidores, será restringido solo al personal autorizado. Para ello la sala deberá contar con los siguientes controles:

- Control de acceso por medio de credencial autorizado en el sistema.
- Puerta de ingreso, ventana y sala reforzado para minimizar el riesgo de ingreso en forma forzosa.
- Ante la necesidad de hacer ingreso a personas no autorizado, ya sea personal técnico interno o externo a la institución, deberá ser acompañado y supervisado por personal previamente autorizado quedando registro de éste.
- Ingresos por personal no técnico, ya sea interno o externo, deberán ser evaluados por el encargado de la sala de servidores y aplicarán las mismas medidas del punto anterior.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

3.2.3. Suministro eléctrico

La sala de servidores deberá estar protegido contra posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- El cableado eléctrico, tablero y enchufes deberán evitar puntos únicos de falla en la distribución de energía al interior de la sala.
- Contar con un suministro de energía ininterrumpido (UPS) para asegurar el funcionamiento continuo del equipamiento que sustenta las operaciones críticas de la institución. Este deberá contar con características que reduzcan los puntos únicos de falla, tablero de bypass para efectuar mantenimiento sin interrumpir el servicio y contrato de mantención vigente y permanente.
- Disponer de un generador de respaldo ante una falla prolongada en el suministro de energía. Deberá contar con un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado de tiempo.
- El encendido del generador deberá ser automático y en un tiempo significativamente menor a la autonomía de la UPS. Para ello se requerirá de un tablero de transferencia automático. Para asegurar lo anterior se deberán realizar pruebas de encendido permanente, inspección regular y/o mantención preventiva y correctiva desde la Direccion de Servicios y Logística.
- Sin perjuicio de lo anterior se deberá elaborar un plan de contingencia para aquellos casos en que no se pueda dar continuidad al suministro eléctrico, ya sea por causas de la naturaleza, humanas, o para tareas de mantención del cableado eléctrico interno o equipos involucrados.

3.2.4. Sistema de climatización

La sala de servidores deberá contar con un sistema de climatización para asegurar la temperatura de la sala entre los 18° y 24° grados Celsius sin

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

gradientes superiores a 2° por hora y una humedad relativa entre los entre un 40 % y un 60 %. El sistema deberá mantener su funcionamiento ante una interrupción prolongada del suministro eléctrico. Además, deberá ser tolerante a fallas para permitir la continuidad de operación.

3.3. Política de Control de Acceso Digital

El objetivo de esta política es asegurar que el acceso a la información esté limitado solo a usuarios autorizados y a los niveles necesarios para cumplir con sus funciones.

3.3.1. Gestión de Identidad

Toda persona que cuente con un vínculo con la institución, ya sea alumno de pre o postgrado, funcionario, etc. deberá contar con credenciales de acceso Institucional, el cual permitirá identificar a la persona mediante la combinación de un usuario y contraseña u otro factor de autenticación adicional dependiendo de la criticidad del acceso.

3.3.2. Credenciales de Acceso Institucional

La Dirección de Gestión Digital y Transparencia será la encargada de generar las credenciales de acceso Institucional a Sistemas Informáticos, la cual será el mecanismo principal de autenticación y acceso a todos los servicios y sistemas institucionales. Además, deberá proveer un mecanismo de asignación de roles asociadas a las credenciales para autorizar el acceso a los diferentes sistemas.

3.3.3. Contraseñas a Sistemas Informáticos Institucionales

Considerando que las contraseñas son el elemento principal para la autenticación de usuarios se regirán por la siguiente política:

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

- El resguardo de la contraseña es de exclusiva responsabilidad del usuario. Para ello deberá seguir las siguientes indicaciones:
  - Mantener las contraseñas en secreto.
  - Cambiar la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
  - Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
  - Los usuarios y contraseñas son intransferibles.

3.3.4. Acceso a Aplicaciones Institucionales

El acceso a las aplicaciones corporativas de tipo Cliente Servidor se permitirá bajo las siguientes condiciones:

- El usuario deberá estar conectado a la red local de la UTA, ya sea en forma cableada o WiFi corporativa, donde se implementarán un segundo factor de autenticación.
- La autenticación del usuario será mediante credencial de acceso Institucional.
- Ante la necesidad de conectarse desde fuera de la red UTA deberá utilizar la VPN-SSL institucional previa autorización de su jefatura directa.
- El usuario deberá contar con la autorización previa, según los privilegios solicitados en concordancia con el rol y tarea a efectuar.

3.3.5. Acceso a la Base de Datos Institucional

La Base de Datos (BD) Corporativa contiene los principales activos de información de la institución. Por lo anterior el acceso a ella será restringido por medio de las siguientes medidas:

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA CHILE

- El acceso a la BD solo se podrá realizar por medio de las aplicaciones administrativas desarrolladas por la Institución.
- Solo el personal autorizado según sus respectivos roles tendrá acceso a la BD por medio de las aplicaciones administrativas y se autenticará utilizando su credencial de acceso remoto.
- El acceso a la BD por medio de las aplicaciones administrativas deberá originarse solo desde equipos conectados a la red de la institución. No se permiten accesos remotos a menos que estos se realicen por medio de la VPN institucional y autorizados previamente por la jefatura correspondiente.
- El acceso a la BD desde otras aplicaciones deberá realizarse por medio de servidores de aplicaciones que cuenten con control de acceso.
- Aplicaciones desarrolladas por externos a la Dirección de Gestión Digital y Transparencia que requieran acceso a la BD deberán ser realizadas por medio de un API que provea control de acceso, autenticación y control de carga.
- Cualquier tipo de acceso a la BD deberá ser autorizada y coordinada con los propietarios de la información.

3.4. Políticas de Seguridad en el Desarrollo de Sistemas

La seguridad de la información en los sistemas desarrollados por la institución deberá ser incorporado desde el diseño y considerando los principales riesgos a los cuales pueda verse expuesto los activos de información relevantes. Se entenderá como activos de información relevantes todos aquellos que intervengan directamente en los procesos misionales de la institución. Para ello se establece la siguiente política:

- Se deberá contar con tres ambientes para el desarrollo de sistemas: Desarrollo, Testing (QA) y Producción.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO ARICA - CHILE

- Los ambientes de Desarrollo y Testing debieran estar separados del ambiente de producción, ya sea en instancias físicas o virtuales.
- Para el ambiente de Desarrollo no se deberá utilizar datos de producción para pruebas internas.
- En aquellos sistemas donde es necesario almacenar contraseñas estas deberán ser cifradas mediante algoritmos criptográficos que aseguren la confidencialidad de la información.
- Toda información considerada sensible que viaje por la red deberá realizase utilizando protocolos que aseguren la integridad y confidencialidad, tales como SSL, HTTPS, etc.

3.5. Políticas de Seguridad de las Personas

Esta política tiene como objetivos asegurar el uso de la interacción de usuarios con los sistemas de información.

3.5.1. Competencias mínimas

Los usuarios deberán contar con competencias mínimas sobre el uso de las tecnologías de información y de seguridad que deben ser comprobadas y validadas por sus respectivas jefaturas.

3.5.2. Durante la contratación de Personal

Todo personal contratado por la institución deberá conocer la presente política y aceptarla como parte del proceso de contratación. Su registro e ingreso en el Sistema de Personal automáticamente lo facultará para contar con las credenciales de acceso Institucional.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO ARICA - CHILE

3.5.3. Durante la desvinculación de Personal

La Dirección de Gestión de Personas y Bienestar deberá informar periódicamente a la Dirección de Gestión Digital y Transparencia el personal desvinculado de la institución de manera de proceder a bloquear el acceso a los respectivos sistemas según los roles asignados. Las excepciones para mantener credenciales de acceso Institucional, en particular para el uso del correo electrónico (jubilados, profesores eméritos, etc.) deberán ser solicitados a la Dirección de Gestión de Personas y Bienestar.

3.5.4. Trabajo a Distancia

El personal de la institución que solicite a la modalidad de trabajo a distancia y que requiera hacer uso de los sistemas de información deberá cumplir con lo siguiente:

- El dispositivo a utilizar deberá contar con un software de seguridad que prevenga incidentes asociados a Malware y otros.
- Se deberá evitar el uso de equipos con cuentas compartidas o de uso público.
- Para tomar el control remoto de algún dispositivo ubicado en la red de la UTA deberá utilizar la VPN y contar con las autorizaciones respectivas de su jefatura directa.
- Será de responsabilidad del usuario velar por la seguridad de la conexión remota.

3.6. Políticas de Copias de Seguridad y Recuperación Ante Desastres

El objetivo de esta política es asegurar la disponibilidad y recuperación de datos en caso de incidentes de pérdida de información.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

3.6.1. Realización de Copias de Seguridad

Se deben realizar copias de seguridad periódicas de toda la información crítica. La frecuencia dependerá de la importancia de los datos y en un proceso que permita dar continuidad al servicio informático Institucional.

3.6.2. Almacenamiento de Copias de Seguridad

Las copias deben almacenarse en un lugar seguro, idealmente en un sitio remoto y con acceso restringido.

3.6.3. Pruebas de Recuperación

Las copias de seguridad deben probarse regularmente para verificar su integridad y efectividad en la recuperación de información.

3.6.4. Plan de Continuidad de Negocio

La universidad debe contar con un plan de continuidad para garantizar la operación en caso de incidentes graves, incluyendo desastres naturales.

3.7. Política de Gestión de Incidentes de Seguridad de la Información

El objetivo de esta política es detectar, gestionar y responder a incidentes de seguridad de la información para minimizar el impacto en la universidad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

3.7.1. Detección y Notificación de Incidentes

Todo miembro de la universidad debe reportar cualquier incidente de seguridad a la brevedad.

3.7.2. Plan de Respuesta a Incidentes

Se debe implementar un plan para contener, erradicar y recuperar sistemas comprometidos, además de analizar las causas para prevenir futuros incidentes.

3.7.3. Documentación y Lecciones Aprendidas

Cada incidente debe documentarse y revisarse para mejorar los procesos de seguridad en la universidad.

3.8. Política de Gestión de Activos de la Información

El objetivo de esta política es proteger los activos de información mediante un adecuado control y clasificación de la información.

3.8.1. Inventario de Activos

Todos los activos de información (hardware, software, datos y documentos) deben ser registrados y etiquetados en un inventario detallado.

3.8.2. Clasificación de la Información

La información debe clasificarse en función de su sensibilidad (confidencial, interna, pública, restringida, sensible, estadística o crítica) y aplicarse

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO ARICA - CHILE

controles de seguridad acordes a cada nivel.

3.8.3. Responsabilidad de Activos

Cada activo debe tener un responsable designado encargado de su protección y de aplicar las políticas de seguridad correspondientes.

3.8.4. Política de Uso Aceptable

Los activos de la universidad deben usarse únicamente para actividades relacionadas con las funciones de la institución. El uso indebido está prohibido.

3.9. Política de Conservación y Destrucción de Información

El objetivo es establecer los lineamientos para la conservación, almacenamiento y destrucción segura de la información generada y/o custodiada por la Universidad de Tarapacá, en cumplimiento de la normativa vigente en materia de educación superior, protección de datos personales, transformación digital y gestión documental. Esta política también se alinea con los principios establecidos en la Ley N.° 21.180 sobre Transformación Digital del Estado, la Ley N.° 19.799 sobre Firma Electrónica, la Ley N.° 21.459 sobre Protección de Datos Personales en el Tratamiento Automatizado, y la Resolución Exenta N.° 173 del Ministerio de las Culturas, las Artes y el Patrimonio.

3.9.1. Conservación de la información

La información académica, administrativa y financiera será conservada por los plazos establecidos en la normativa sectorial o en los planes de archivo

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

institucionales. Los datos personales serán conservados solo por el tiempo necesario para cumplir con la finalidad para la cual fueron recolectados, salvo obligación legal de conservación. En el caso de documentación digital, se aplicarán los principios establecidos en la Ley N.° 18.845, asegurando la integridad, autenticidad y disponibilidad de los documentos electrónicos.

3.9.2. Destrucción de la información

La destrucción de documentos físicos o digitales que contengan datos personales o información sensible deberá realizarse mediante métodos seguros e irreversibles (trituración, borrado seguro, destrucción física de soportes). Todo proceso de eliminación deberá ser documentado, incluyendo fecha, responsable, método utilizado y tipo de información destruida.

La eliminación de documentos originales microcopiados o digitalizados se regirá por el marco normativos de Ley 19.628 de Protección de la Vida Privada que establece los principios y normas para el tratamiento de datos personales, incluyendo la obligación de las universidades de proteger la información que manejany Ley 21.719 de Protección de Datos Personales introduce nuevas regulaciones y desafíos para la protección de datos personales en Chile, incluyendo las universidades.

3.10. Política de Protección Contra Malware

El objetivo de esta política es proteger los sistemas de la Universidad contra software malicioso que pueda afectar la integridad y disponibilidad de la información.

3.10.1. Instalación y Actualización de Software Antimalware

Todos los equipos institucionales conectados a la red universitaria deben contar con software antimalware actualizado que incluya protección contra virus, spyware, ransomware, entre otros a cargo de la Dirección de Servicios y

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

Logística.

3.10.2. Capacitación y Concientización

Se deben realizar campañas informativas a través de distintos medios de comunicación sobre los riesgos del malware y las prácticas para evitarlos, como no abrir correos sospechosos ni descargar archivos de fuentes desconocidas.

3.10.3. Monitoreo y Respuesta a Incidentes

La Direccion de Gestión Digital y Transparencia debe monitorear continuamente la red para identificar y mitigar posibles amenazas. Además, debe contar con un plan de respuesta a incidentes específico para actividad sospechosa.

3.11. Política de Uso del Correo Electrónico Institucional

El objetivo de esta política es establecer las directrices y normas para el uso adecuado del correo electrónico institucional, con el fin de proteger la seguridad, integridad y reputación de la Institución. Se espera que el correo institucional sea utilizado de manera responsable, ética y en línea con los valores de la universidad, asegurando que apoye las actividades académicas, administrativas e investigativas de la institución.

La política aplica a todos los miembros de la comunidad universitaria, incluidos funcionarios académicos, funcionarios de gestión, estudiantes, y cualquier otra persona o entidad que tenga acceso a una cuenta de correo electrónico proporcionada por la universidad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

3.11.1. Uso Aceptable

- El correo electrónico institucional debe usarse exclusivamente para actividades relacionadas con la labor académica, administrativa y de investigación de la universidad.
- Se prohíbe el uso del correo institucional para fines personales, comerciales o actividades que no estén alineadas con los intereses y objetivos de la universidad.
- Los correos deben ser utilizados de acuerdo con las políticas de confidencialidad y privacidad de la institución, asegurando el correcto tratamiento de la información sensible o confidencial.

3.11.2. Confidencialidad y Seguridad

- Los usuarios deben proteger sus credenciales de acceso (por ejemplo usuario y contraseña) y no compartirlas con terceros. La universidad no se hace responsable de los daños derivados del uso indebido de las credenciales de acceso.
- No está permitido enviar información confidencial, privada o sensible sin las debidas medidas de seguridad (como cifrado o acceso restringido).
- En caso de pérdida o compromiso de la cuenta, y que no pueda ser recuperado por el/la usuario/a, el usuario debe notificarlo de inmediato a la Dirección de Gestión Digital y Transparencia para tomar las medidas correctivas necesarias.

3.11.3. Contenido de los Mensajes

- Se espera que el contenido de los correos sea respetuoso. Queda estrictamente prohibido el envío de mensajes ofensivos, discriminatorios, difamatorios, que inciten al odio, o que infrinjan derechos de terceros.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

- No está permitido el uso del correo institucional para el envío de correos en masa no autorizados (SPAM) o mensajes de cadena.

3.11.4. Responsabilidad de los Mensajes

- Los usuarios son responsables de la información que envían a través del correo institucional. La universidad no se hace responsable de las opiniones o afirmaciones personales expresadas en los correos enviados desde cuentas institucionales

3.11.5. Almacenamiento y Gestión de Cuentas

- La capacidad de almacenamiento del correo institucional es limitada. Los usuarios deben hacer un uso razonable del espacio y eliminar correos que no sean necesarios para el desempeño de sus funciones, siempre que sea posible de acuerdo a la norma [4].
- Las cuentas de correo institucional (académicos y gestión) serán desactivadas y eliminadas cuando el usuario ya no pertenezca a la comunidad universitaria. Se crearán mecanismos para establecer este proceso a través de la Vicerrectoría de Administración y Finanzas, dependiendo de los casos que se presenten.
- En el caso de alumnos, se les mantendrá la cuenta con el propósito de tener contacto con egresados de la Institución, la cual tendrá reducción de espacio para una mejor administración de los recursos Institucionales.
- Los dominios de los correos electrónicos institucionales serán establecidos por el comité ad-hoc creado para este propósito.
- Para prestadores de servicio (contrato a honorarios):
  - Se le asignará un correo electrónico con dominio a ser definido por comité desigando para tal propósito.
  - El correo electrónico permanecerá activo sólo durante el período que dure el contrato de honorario.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

4. Mecanismos de Difusión

La presente política debe ser conocida por todos/as los/as funcionarios/as de la Universidad de Tarapacá, para ello es necesario contar con una difusión a través de la Intranet y en el sitio web oficial de la UTA para las partes interesadas externas. La difusión de esta política debe ir acompañada, siempre que sea posible, de capacitaciones continuas. Asimismo, se implementará un programa de inducción para los/as funcionarios/as que se incorporen a la Universidad de Tarapacá, con el objetivo que toda dotación se sensibilice en uso y protección de los activos de la información como parte del quehacer institucional y del desarrollo de las personas.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACÁ
SECRETARIO
DE LA
UNIVERSIDAD

5. Período de Revisión

La revisión y mantención de la presente política será realizada por el Oficial de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad y la máxima autoridad universitaria.

La presente política deberá ser revisada y aprobada por el Comité de Seguridad, de acuerdo a las necesidades de la Universidad una vez al año contados desde su publicación. Sin embargo, esta política podrá ser revisada y actualizada antes de cumplirse este periodo según requerimiento de alguno de sus miembros o por alguna circunstancia coyuntural que lo requiera, que afecten la adecuada protección de la información, considerando como tales entre otros, cambios a nivel estructural de la Universidad, en la misión, objetivos estratégicos, productos estratégicos, personal y/o cambios tecnológicos que impacten la seguridad de la información, entre otros. Hechos los cambios y aprobación, el Oficial de seguridad de la Información deberá difundir la nueva versión.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO ARICA - CHILE

6. Incumplimiento y Sanciones

El incumplimiento de la presente política dará lugar a las medidas disciplinarias establecidas en el Estatuto Administrativo, así como en las ordenanzas académicas y estudiantiles, en virtud de las infracciones a los deberes establecidos en dichas normativas. Lo anterior es sin perjuicio de la aplicación de los protocolos institucionales vinculados a la Ley N.° 21.369, la Ley Karin u otras normativas equivalentes que resulten pertinentes, cuando corresponda.

Asimismo, las personas contratadas como prestadores de servicios a honorarios deberán considerar como infracción a los deberes establecidos en sus respectivos contratos el incumplimiento de la presente política, lo que dará lugar a las sanciones contempladas en dichos contratos.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

7. Glosario de Términos

Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.

Activo de Información:Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.

Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado o afectado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.

Cliente Servidor: Modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.

Confidencialidad: Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Control de Seguridad:Conjunto de estándares, buenas prácticas y normativas que permiten administrar los riesgos en las tecnologías de la información.

Disponibilidad: Atributo de los activos y activos de información, relativo a su accesibilidad y utilización a requerimiento de una entidad o proceso autorizado.

Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Estación de Trabajo: Equipo computacional conectado a una red de computadores que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Evaluación de Riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la institución) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.

Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.

Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.

Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.

Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

SECRETARIO DE LA UNIVERSIDAD DE TARAPACA - CHILE

aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Programa malicioso (malware): Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora. También se denominan malware.

Red local: En términos de informática, una red local o LAN (del inglés Local Area Network) es un conjunto de dispositivos (como computadores, impresoras, servidores, teléfonos, etc.) interconectados entre sí dentro de un área geográfica limitada, como una casa, oficina, edificio o campus

Reglamento: Decreto supremo N° 4, de 2020, del Ministerio Secretaría General de la Presidencia, que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley N° 21.180 sobre Transformación Digital del Estado.

Restricción del acceso: Acción consistente en la delimitación de acceso de los funcionarios, estudiantes o terceras partes a determinados recursos físicos o lógicos.

Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

Servidor: Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.

Sistema informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.

Sistema de comunicaciones electrónicas: Se refiere a todo medio o dispositivos que permite comunicarse. Entiéndase: correo electrónico, mensajería instantánea (por ejemplo WhatsApp, Instagram, Discord, WeChat, Facebook Messenger, Line, Viber, Snapchat, Skype u otros), Teleconferencia (por ejemplo Skype, Zoom, Microsoft Team, Webex, Jitsi u otros), Telefonía fija y móvil, u otros.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

Trabajo a distancia: aquel en el que el trabajador o funcionario presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

8. Términos Abreviados

API: Interfaz de Programación de Aplicaciones

CSI: Comité de seguridad de la información

OSI: Oficial de seguridad de la información

LAN: Red de Area local. (Local Area Network).

BD: Base de Datos

HA: High Availability

PI: Propietario de la información

TI: Tecnologías de la Información

UI: Usuario de la información

VLAN: Red de Área Virtual (Virtual Local Area Network)

VPN: Red Privada Virtual (VPN)

WPA2: Protocolo de seguridad para redes WiFi que proveen seguridad de la información

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

Referencias

[1] República de Chile, *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*, Promulgada el 25 de agosto de 2022 y publicada en el Diario Oficial el 5 de septiembre de 2022. Establece disposiciones relacionadas con la protección de datos personales., 2022. dirección: https://www.bcn.cl/leychile.

[2] B. del Congreso Nacional, *REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES*, [Online; accessed 2025-05-13], Diciembre de 2024. dirección: https://www.bcn.cl/leychile/navegar?idNorma=1209272.

[3] República de Chile, *SOBRE PROTECCION DE LA VIDA PRIVADA*, Promulgada el 18 de agosto de 1999 y publicada en el Diario Oficial el 28 de agosto de 1999. Regula el tratamiento de datos personales y la protección de la privacidad., 1999. dirección: https://www.bcn.cl/leychile.

[4] República de Chile, *SOBRE ACCESO A LA INFORMACIÓN PÚBLICA*, Promulgada el 11 de agosto de 2008 y publicada en el Diario Oficial el 20 de agosto de 2008. Establece normas sobre transparencia y el derecho de acceso a la información pública., 2008. dirección: https://www.bcn.cl/leychile.

[5] Gobierno de Chile, *Decreto N° 273/2022: Normativa específica (indicar el tema, por ejemplo, 'Regulación sobre...')* Publicado en el Diario Oficial, establece disposiciones relacionadas con (especificar tema si es necesario), 2022. dirección: %7Bhttps://www.diariooficial.cl%7D.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

UNIVERSIDAD DE TARAPACA SECRETARIA DE LA UNIVERSIDAD ARICA - CHILE

Comisión Nacional de Acreditación CNAChile

UNIVERSIDAD ACREDITADA
NIVEL DE EXCELENCIA
6 AÑOS
HASTA JUNIO DE 2027
• GESTIÓN INSTITUCIONAL
• DOCENCIA DE PREGRADO
• INVESTIGACIÓN
• VINCULACIÓN CON EL MEDIO
• DOCENCIA DE POSTGRADO

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799.
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ZTPDPU-727

Políticas de Seguridad de la Información

Junio 2025

UNIVERSIDAD DE TARAPACÁ
Universidad del Estado

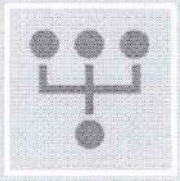
DGDT
Dirección de Gestión Digital y Transparencia

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL
ARICA - CHILE

Objetivo y Alcance



Proteger los activos digitales de la universidad: confidencialidad, integridad, autenticidad y disponibilidad.

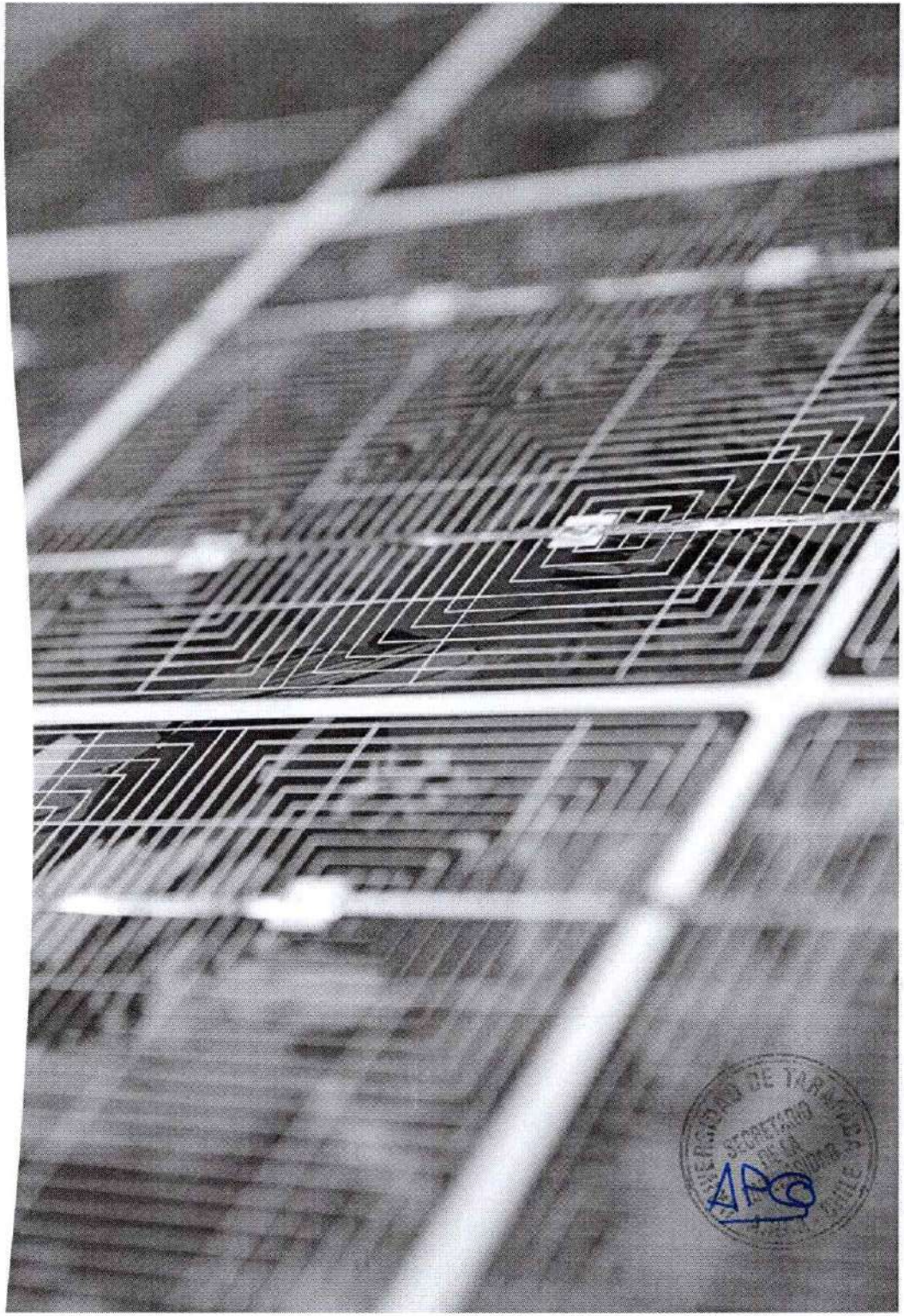


Aplica a todos los procesos y unidades que gestionen o accedan a información institucional.



Marco Normativo Aplicable

- NCh-ISO 27002:2009 / ISO/IEC 27002
- Ley 19.628: Protección de la Vida Privada
- Ley 21.663 y DS N°164: Ciberseguridad
- Ley 21.180: Transformación Digital del Estado
- Ley 21.459: Delitos Informáticos



Principios Fundamentales

Confidencialidad: acceso solo autorizado

Integridad: exactitud y completitud

Autenticidad: validación del origen

Disponibilidad: acceso cuando se requiera





Roles y Responsabilidades Clave

- Comité de Seguridad de la Información (CSI)
- Oficial de Seguridad de la Información (OSI)
- Autoridades Universitarias
- Usuarios: conocimiento y cumplimiento de la política

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Resumen de Políticas Específicas

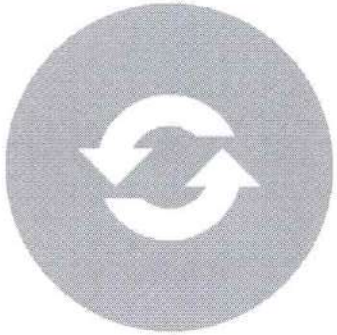
- Gestión de redes, respaldos y acceso remoto
- Control de acceso digital con credenciales seguras
- Respaldo y recuperación ante desastres
- Gestión y respuesta a incidentes de seguridad
- Uso adecuado del correo electrónico institucional

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Mecanismos de Difusión



PUBLICACIÓN EN INTRANET Y SITIO WEB INSTITUCIONAL



CAPACITACIONES CONTINUAS



INDUCCIÓN A NUEVOS FUNCIONARIOS

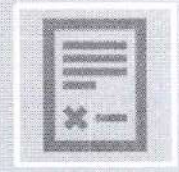
Revisión y Sanciones



Revisión mínima de 1 vez al año o ante cambios relevantes



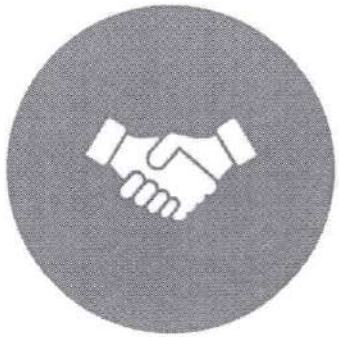
Sanciones según Ley 21.369, Ley Karin, y aquellas del Estatuto Administrativo.



Aplicación contractual para terceros

UNIVERSIDAD DE TARAPACA
SECRETARIO
ARICA - CHILE

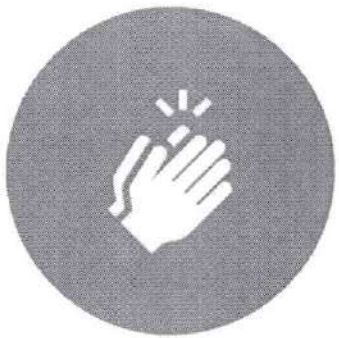
Cierre



COMPROMISO INSTITUCIONAL CON LA SEGURIDAD DE LA INFORMACIÓN.



REQUIERE APOYO TRANSVERSAL DE TODAS LAS UNIDADES.



SE PRESENTA AL COMITÉ PARA SU APROBACIÓN.



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.

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

UNIVERSIDAD DE TARAPACÁ
ARICA - CHILE

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

DECRETO EXENTO Nº 00.930/2025.

Arica, julio 28 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 DACI N°96/2025 de fecha 28 de julio de 2025, Carta REC.N°2306/2025, de fecha 28 de julio de 2025; los antecedentes adjuntos y las facultades que me confiere el Nº 2, del artículo 13° del D.F.L. Nº 150, ya citado en relación con el Decreto Exento RA N°335/12/2025, tomado de razón el 02 de junio de 2025.

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, mediante carta DACI N°96/2025 de fecha 28 de julio de 2025, la Directora de Auditoría y Control Interno solicita la emisión de un decreto exento que permita oficializar los Procedimientos Complementarios de las Políticas de Seguridad de Información.

Que, los documentos indicados han sido revisados por el Comité de Seguridad de la Información de la Universidad y se estima pertinente su oficialización mediante el presente acto administrativo.

El mérito de lo ordenado por la Dra. Jenniffer Peralta Montecinos, Rectora(S) a través de carta REC N° 2306/25 de fecha 28 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) Políticas de Creación y Mantenimiento de Contraseñas y Uso de Cuentas de Usuario, contenido en documento adjunto, compuesto por cuatro (4) páginas, debidamente rubricadas por el Secretario (S) de la Universidad de Tarapacá.

b) Instructivo Uso de Software Legal – Universidad de Tarapacá, contenido en documento adjunto, compuesto por cuatro (4) páginas, debidamente rubricadas por el Secretario (S) de la Universidad de Tarapacá.

c) Formulario de Toma de Conocimiento "Informativo Cuentas de Usuario y Contraseñas", contenido en documento adjunto, compuesto por tres (3) páginas, debidamente rubricadas por el Secretario (S) 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 TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

ALVARO CORTINEZ PONTONI
Secretario (S) de la Universidad

UNIVERSIDAD DE TARAPACÁ RECTORA(S) ARICA

JENNIFFER PERALTA MONTECINOS
Rectora(S)

JPM.ACP.yvv

UNIVERSIDAD DE TARAPACÁ CONTRALORÍA ARICA

28 JUL 2025

Políticas de Creación y Mantenimiento de Contraseñas y Uso de Cuentas de Usuario

UNIVERSIDAD DE TARAPACÁ
SECRETARIA
DE LA
UNIVERSIDAD
ARICA - CHILE

1. Objetivo

Establecer directrices claras para la creación, mantenimiento y uso seguro de contraseñas y cuentas de usuario en la Universidad de Tarapacá, con el fin de proteger la información institucional y personal, asegurando un acceso controlado y seguro a los sistemas.

2. Alcance

Estas políticas aplican a todos los miembros de la comunidad universitaria que utilizan cuentas de usuario institucionales para acceder a los sistemas, aplicaciones y redes de la universidad.

3. Políticas de Creación de Contraseñas

3.1 Requisitos de Contraseña Segura

- Las contraseñas deben tener al menos **8 caracteres**.
- Deben incluir una combinación de:
  - **Letras mayúsculas y minúsculas** (Ej.: A y a).
  - **Números** (Ej.: 1, 3, 7).
  - **Caracteres especiales** (Ej.: !, @, #, $, %).
- **Prohibiciones**:
  - No usar nombres, fechas de nacimiento u otra información personal.
  - Evitar palabras comunes o secuencias obvias (Ej.: 123456, password).

3.2 Cambio Periódico de Contraseña

- Todas las contraseñas deben renovarse cada **6 meses**.

UNIVERSIDAD DE TARAPACÁ SECRETARIO DE LA UNIVERSIDAD ARICA - CHILE

- El sistema notificará a los usuarios con anticipación sobre el vencimiento de su contraseña.

3.3 Evitar Reutilización de Contraseñas

- No se permite el uso de contraseñas previas. Los usuarios deben crear una nueva combinación cada vez que actualicen su contraseña.

4. Mantenimiento Seguro de Contraseñas

4.1 No Compartir Contraseñas

- Las contraseñas son personales e intransferibles. No se permite compartirlas bajo circunstancia, salvo con el personal autorizado de la Unidad de Soporte Técnico para fines de soporte y restablecimiento.

4.2 Almacenamiento Seguro de Contraseñas

- Los usuarios deben evitar almacenar contraseñas en archivos sin protección o en papel.
- Se recomienda el uso de gestores de contraseñas confiables y seguros si el usuario necesita almacenar múltiples credenciales.

4.3 Notificación de Sospechas de Compromiso

- Si un usuario sospecha que su contraseña ha sido comprometida, debe cambiarla de inmediato y notificar a la Unidad de Soporte Técnico.

5. Políticas de Uso Adecuado de Cuentas de Usuario

5.1 Exclusividad de Uso

- Cada cuenta de usuario es de uso exclusivo para la persona a la que se le ha asignado. No está permitido el uso de cuentas compartidas o de otra persona.

5.2 Cierre de Sesión

UNIVERSIDAD DE TARAPACÁ SECRETARÍA DE LA UNIVERSIDAD ARICA - CHILE

- Los usuarios deben cerrar sesión al finalizar su trabajo en cualquier sistema, especialmente cuando usen dispositivos compartidos o públicos.

5.3 Acceso Seguro

- Los usuarios deben acceder a sus cuentas solo desde dispositivos y redes confiables. Se recomienda evitar el acceso desde redes públicas no seguras.

5.4 Control de Accesos Especiales

- Cualquier acceso especial (e.g., cuentas con privilegios de administrador) debe ser solicitado formalmente y aprobado por la Unidad de Soporte Técnico. Estas cuentas solo serán asignadas a personal autorizado y deben usarse estrictamente para fines administrativos.

6. Auditoría y Monitoreo

- La Unidad de Soporte Técnico realizará auditorías periódicas para asegurar el cumplimiento de estas políticas.
- Los registros de acceso y actividad de las cuentas se revisarán regularmente para detectar actividades inusuales o no autorizadas.

7. Consecuencias por Incumplimiento

El incumplimiento de estas políticas puede resultar en sanciones disciplinarias, que incluyen desde advertencias hasta la suspensión temporal o permanente del acceso a los sistemas institucionales, dependiendo de la gravedad de la infracción.

8. Soporte y Contacto

Para preguntas, asistencia o reporte de problemas relacionados con contraseñas o cuentas de usuario, los usuarios pueden contactar a la Unidad de Soporte Técnico.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

Universidad de Tarapacá

INSTRUCTIVO USO DE SOFTWARE LEGAL Universidad de Tarapacá

MAYO 2024

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

INSTRUCTIVO USO DE SOFTWARE LEGAL

Historial de Revisiones

Fecha	Versión	Descripción	Responsable
Mayo 2024	1.0	Actualización de propuesta inicial de Instructivo de Uso de Software Legal	Dirección de Servicios y Logística



INSTRUCTIVO SOBRE USO DE SOFTWARE LEGAL

INTRODUCCIÓN

El propósito del presente instructivo es informar, normar y regularizar el uso e instalación de software en la Universidad de Tarapacá, como también dar a conocer la normativa y procedimientos para la asignación y uso de licencias de software que son asignadas o distribuidas.

Es importante mencionar que el uso inapropiado de software, expone a la Universidad de Tarapacá contra riesgos legales y de seguridad informática, tales como la pérdida de información, filtración de datos, infracción de derechos de autor, exposición de los sistemas internos a códigos maliciosos, interrupciones o degradación de servicios de red, suplantación de identidad, daños de sistemas, entre otros.

ALCANCE

El presente documento es aplicable a todos los académicos, funcionarios, estudiantes, personal a honorarios y ayudantes, que utilicen equipamiento computacional inventariado por la Universidad de Tarapacá o que hayan sido adquiridos por medio de proyectos de investigación que funcionen en las mismas condiciones de seguridad y control que un equipo computacional inventariado.

NORMATIVAS

Sobre el uso e instalación de software.

1- Es su obligación conocer y cumplir con las normativas presentes en este documento.

2- Las licencias de software que proporciona la Universidad de Tarapacá, sólo deben ser utilizadas con fines educacionales o investigación.

3- Con el objetivo de mantener la integridad de los sistemas y redes, estandarización y control en cuanto al cumplimiento en el uso de licencias de software de acuerdo a la Ley N° 17.336, sobre propiedad intelectual (Ley N°20.435, modificación ley N° 17.336), la instalación de software está autorizada solo al personal técnico de la Dirección de Servicios y Logística y/o a quienes se les autorice.

4- Las actualizaciones de software solo podrán ser efectuadas por el personal técnico de la Dirección de Servicios y Logística, y/o a quienes se les autorice, lo mismo ocurre en el caso de actualizaciones de sistema operativo o antivirus.

5- No se podrá instalar software protegido por derechos de autor, sin la respectiva licencia en los equipos computacionales que estén inventariados por la Universidad de Tarapacá, con la excepción de licencias que permitan su uso y distribución libre.



6- No se hará entrega de medios físicos o números de serie de licenciamiento a los usuarios que utilicen la licencia, por tratarse de información delicada y confidencial que tiene por objeto proteger los planes de licenciamientos y compromisos legales de la Universidad de Tarapacá.

7- Los requerimientos de instalación de software que no cuenten con una licencia válida, deberán ser canalizados, formalmente, a través del director de departamento al que está adscrito, quien deberá escalar y evaluar el requerimiento junto a la Dirección de Servicios y Logística para analizar si existen alternativas de software libre, si es posible asignar una licencia disponible, o se gestiona la compra.

8- Cualquier convenio de licenciamiento con la Universidad de Tarapacá, solo tiene cobertura para equipos que hayan sido adquiridos al menos con una licencia básica de sistema operativo. Estas licencias podrán ser instaladas solo en los equipos inventariados por la Universidad de Tarapacá.

Sobre la asignación de licencias de software.

Las asignaciones se regirán además, de acuerdo a las siguientes normativas:

1- La asignación de una licencia, sólo le da derecho a uso por el periodo asignado debiendo solicitar la extensión del periodo, si fuese necesario, para seguir utilizando la licencia.

2- Las licencias de software serán asignadas en el caso de existencia de un convenio corporativo y dependiendo del número de licencias disponibles, aprobación a nivel de Dirección para respaldar su uso, aprobación de descuento al centro de costos o presupuesto si corresponde y la cantidad de horas correspondiente a la jornada laboral de quien solicita.

3- La asignación de una licencia, sólo le da derecho a quien solicita la licencia a que sea instalada en un solo computador inventariado por la Universidad de Tarapacá, en casos excepcionales y justificados, podrán ser instalados en equipos no inventariados que faciliten el desarrollo de proyectos de investigación.

Procedimientos para solicitud y uso de licencias.

1- Los requerimientos de instalación de software que cuenten con una licencia asignada o permitan el uso o distribución libre (Open Source), deberán ser solicitada a la Dirección de Servicios y Logística, donde deberá justificar su uso.

2- Por lo tanto, queda absolutamente prohibida la instalación de software no licenciado o similar, sin la debida autorización de la Dirección de Servicios y Logística.

3- También queda prohibida la instalación de software con licencia, cuyo fin no esté relacionado con el quehacer directo del usuario.



UTA - VAF Toma de Conocimiento Informativo Cuentas de Usuario y contraseñas

1. Informativo VAF - DSL
2. Políticas de Creación y Mantenimiento de Contraseñas y Uso de Cuentas de Usuario
3. Manual de Usuario FInal

rarriagg@gestion.uta.cl Cambiar de cuenta

* Indica que la pregunta es obligatoria

Correo *

Tu dirección de correo electrónico

1.- INFORMACIÓN DEL USUARIO

NOMBRE COMPLETO *

Tu respuesta

CARGO *

Tu respuesta



UNIDAD *

Tu respuesta

CORREO INSTITUCIONAL *

Tu respuesta

ANEXO

Tu respuesta

2.- DECLARACIÓN DE CONOCIMIENTO

¿Ha leído y comprendido el contenido del Manual de Usuario Final? *

- ○ Sí
- ○ No

¿Ha leído y comprendido las Políticas de Usuarios y Claves? *

- ○ Sí
- ○ No

UNIVERSIDAD DE TARAPACA
SECRETARIO DE LA UNIVERSIDAD
ARICA - CHILE

¿Está de acuerdo en seguir las pautas y políticas establecidas en ambos documentos? *

- ◯ Sí
- ◯ No

Me comprometo a utilizar las claves de manera segura y a no compartirlas con terceros. *

- ◯ Sí, me comprometo
- ◯ No, me comprometo

Firma de aceptación *(los usuarios pueden escribir su nombre completo como firma)* *

Tu respuesta

Se enviará una copia de tus respuestas por correo electrónico a la dirección que has proporcionado.

Enviar Página 1 de 1 Borrar formulario

Nunca envíes contraseñas a través de Formularios de Google.

reCAPTCHA
Privacidad Términos

Este formulario se creó en Universidad de Tarapacá.

¿Parece sospechoso este formulario? Informe

Google Formularios

