D.J. (1346)

SANTIAGO, 28 DICIEMBRE 2023

RESOLUCIÓN N° 05252 EXENTA

VISTOS: lo dispuesto en la Ley Nº 19.239; en el D.S. N° 86 de 2021; en las letras b) y d) del artículo 11 y artículo 12 del D.F.L. N° 2 de 1994; en el DFL N° 2 de 2009, que fija el texto refundido, coordinado y sistematizado de la Ley N° 20.370, Ley General de Educación, con las normas no derogadas del DFL N° 1 de 2005 que a su vez, fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.962, Orgánica Constitucional de Enseñanza, todos del Ministerio de Educación; en el DFL N° 1 de 1981 que fija normas sobre Universidades; en la Ley N° 21.094; la Ley N° 21.180 sobre Transformación Digital del Estado; la Resolución Exenta N° 777 de 2020; y lo solicitado por el Director del Departamento de Sistemas de Servicios de Informática con fecha 22 de diciembre de 2023;

CONSIDERANDO:

1. Que, de conformidad al artículo 1º de la Constitución Política de la República, el Estado reconoce y ampara a los grupos intermedios a través de los cuales se organiza y estructura la sociedad y les garantiza la adecuada autonomía para cumplir sus propios fines específicos. Asimismo, consagra que el Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respeto a los derechos y garantías que esta Constitución Establece.

2. La Ley Nº 21.094, por su parte, define a las Universidades del Estado como instituciones de Educación Superior de carácter estatal, creadas por ley para el cumplimiento de las funciones de docencia, investigación, creación artística, innovación, extensión, vinculación con el medio y el territorio, con la finalidad de contribuir al fortalecimiento de la democracia, al desarrollo sustentable e integral del país y al progreso de la sociedad en las diversas áreas del conocimiento y dominios de la cultura. Asimismo, la Ley Nº 19.239 que crea la Universidad Tecnológica Metropolitana la define como una institución de educación superior del Estado, como organismo autónomo, con personalidad jurídica y patrimonio propios.

3. Que habida consideración de lo anterior y lo dispuesto en el artículo 3° de la Ley N° 18.575, las Universidades como integrantes del Estado, están al servicio de la persona humana y su finalidad es promover el bien común atendiendo las necesidades públicas en forma continua y permanente y fomentando el desarrollo del país a través del ejercicio de las atribuciones que le confiere las Constitución y las leyes.

4. Que de acuerdo con el artículo 2° de la Ley Nº 21.094, se dispone que las Universidades del Estado gozan de autonomía académica, administrativa y económica. Por otro lado, el artículo 104° del DFL N° 2 de 2009 que fija el texto refundido, coordinado y sistematizado de la Ley N° 20.370, General de Educación, con las normas no derogadas del DFL N° 1 de 2005 que a su vez, fija el texto refundido, coordinado y sistematizado de la Ley Nº18.962, Orgánica Constitucional de Enseñanza, todos del

Ministerio de Educación, indica que se entenderá por autonomía el derecho de cada establecimiento de educación superior a regirse por sí mismo, de conformidad con lo establecido en sus estatutos en todo lo concerniente al cumplimiento de sus finalidades y comprende la autonomía académica, económica y administrativa.

5. Que la autonomía universitaria, según ha establecido la jurisprudencia del Excelentísimo Tribunal Constitucional, tiene fundamento en la autonomía de los cuerpos intermedios, reconocida en el artículo 1°, inciso 3° de la Constitución Política de la República (STC N° 523 cc.21 y 24) y "*se ejerce según y en silencio de ley*" (STC N° 2731), es decir, reconoce como límites de la misma a los estatutos de la entidad y a la ley, de suerte tal que aquellos son los contornos legales que validan jurídicamente las decisiones que se adopten en el uso de dicha facultad. Respecto a las Universidades Estatales, ha señalado que "*Las universidades estatales dotadas de autonomía por mandato de la ley, deben ejercerla dentro del marco legal que establece su estructura interna, su organización y atribuciones*" (STC N° 352 c.18).

6. Que, el artículo 2º de la Ley N°19.239 señala que la Universidad Tecnológica Metropolitana tendrá las funciones que, de acuerdo con la legislación vigente, son propias de este tipo de instituciones. Su objetivo fundamental será ocuparse, en un nivel avanzado, de la creación, cultivo y transmisión de conocimiento por medio de la investigación básica y aplicada, la docencia y la extensión en tecnología, y de formación académica, científica, profesional y técnica orientada preferentemente al quehacer tecnológico.

7. Que según el plan de desarrollo estratégico UTEM 2021 – 2025, esta Casa de Estudios Superiores tiene como misión formar personas con altas capacidades académicas y profesionales, en el ámbito preferentemente tecnológico, apoyada en la generación, transferencia, aplicación y difusión del conocimiento en las áreas del saber que le son propias, para contribuir al desarrollo sustentable del país y de la sociedad de la que forma parte.

8. Que, por otra parte, con fecha 11 de noviembre de 2019, se publicó en el Diario Oficial la ley Nº 21.180, de Transformación Digital del Estado. Así, esta Ley tiene por objeto efectuar una transformación digital del Estado, a través de la modificación de diversos cuerpos legales, para que éste avance hacia un Estado ágil y eficiente, cuyo actuar se condiga con los tiempos actuales y se beneficie de las ventajas del desarrollo electrónico y digital. En ese sentido, la Ley impulsa que el ciclo completo de los procedimientos administrativos de todos los órganos de la Administración del Estado sujetos a Ley de Bases de Procedimiento Administrativo (Ley N° 19.880), se realice en formato electrónico.

9. Que, en virtud de la Ley N° 21.464 promulgada el 8 de junio de 2022 y publicada el 9 de junio de 2022, se modifica diversos cuerpos legales, en materia de transformación digital del Estado**,** incluyendo el DFL N° 1 de 2021 donde constaba la aplicación de gradual de la Ley N° 21.180.

10. Que, en virtud de la Resolución Exenta N° 03724 de fecha 15 de septiembre de 2022, se constituyó de instancia de trabajo para analizar implicancias operativas de la Ley N° 21.180 sobre Transformación Digital del Estado, que estará integrada por la Vicerrectoría de Administración y Finanzas, la Dirección General de Análisis Institucional y Desarrollo Estratégico y la Dirección Jurídica.

11. Que, en virtud de la Resolución Exenta N° 777 del año 2020, se aprobaron las "INSTRUCCIONES SOBRE USO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES DE LA UNIVERSIDAD TECNOLÓGICA METROPOLITANA Y MEDIDAS DE CIBERSEGURIDAD".

12. Que, atendido el desarrollo tecnológico de la Universidad, así como la nueva Ley de Modernización del Estado que precisamente requiere de los Órganos de la Administración del Estado establecer procesos que conlleven a la digitalización de sus procedimientos, es que, el Director del Departamento de Sistemas de Servicios de Informática con fecha 22 de diciembre de 2023 ha requerido la actualización de la Resolución Exenta N° 777 de 2020, por tanto;

RESUELVO:

1. **DÉJESE SIN EFECTO,** la Resolución Exenta N° 777 de 2020.

2. **APRUÉBENSE,** las nuevas **INSTRUCCIONES SOBRE USO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES DE LA UNIVERSIDAD TECNOLÓGICA METROPOLITANA Y MEDIDAS DE CIBERSEGURIDAD,** cuyo texto es el siguiente:

Título I
UNIDAD OPERATIVA RESPONSABLE

Artículo 1°. Dirección encargada. Para el cumplimiento del objetivo del presente acto administrativo, se establece que el Área de TIC responsable de coordinar, ejecutar y gestionar el cumplimiento de las políticas, instrucciones y directrices definidas por la institución, será el Departamento de Sistemas y Servicios de Información (en adelante también "SISEI"), sin perjuicio de las obligaciones que deben cumplir todas las autoridades, usuarios y dependencias en el ámbito de sus competencias.

Artículo 2°. Presupuesto. La Vicerrectoría de Administración y Finanzas (en adelante también "VRAF"), deberá adecuar los presupuestos y funcionamiento para el cumplimiento de los procesos que indica la presente resolución.

Título 2
INSTRUCCIONES SOBRE USO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Artículo 3°. Ámbito de aplicación. El presente Instructivo será obligatorio para todos los usuarios que hagan uso de los recursos, equipamientos y servicios de tecnología de información y comunicaciones de propiedad de la UTEM.

Artículo 4°: Asignación de los Recursos Computacionales. La Institución, por medio del SISEI y VRAF, cumplirá con lo siguiente:

1. **Asignación de equipos TIC**. La UTEM asignará a cada usuario el equipamiento de tecnología de información y comunicaciones, necesario para el cumplimiento

de sus labores, de acuerdo con su función efectiva, comunicada por la Dirección de Desarrollo de las Personas al momento de su nombramiento, teniendo en consideración la factibilidad técnica y los presupuestos disponibles.

La UTEM definirá el equipamiento estándar para cada función efectiva. En caso de circunstancias excepcionales, como problemas médicos debidamente justificados o por necesidades adicionales a las labores propias de la función, la jefatura podrá solicitar requerimientos especiales a SISEI, el que analizará la factibilidad de dicha solicitud.

Cuando un usuario sea trasladado en la misma sede, manteniendo su función efectiva, deberá permanecer con el equipo inicialmente asignado. En caso de que la sede de desempeño y/o la función efectiva cambie, SISEI deberá evaluar una nueva asignación.

El personal que preste servicios en calidad de honorarios o destinados a un proyecto específico en la Universidad, podrá hacer uso de un equipamiento institucional. Para lo anterior, su contraparte técnica al interior de la Universidad, o quien esté a cargo del Proyecto deberá solicitar dicho equipamiento, quien se hará responsable administrativamente de este préstamo de equipamiento, quedando registrado a su nombre. De igual manera, la entrega del equipamiento se hará previa suscripción de contrato de comodato con la persona usuaria del mismo.

2. **Devolución de equipos:** Cuando un usuario por cualquier motivo deje de pertenecer a la Institución, deberá entregar el equipamiento tecnológico a su cargo directamente a su jefatura quien lo deberá comunicar y/o enviar a VRAF, informando a SISEI. Además, se suspenderán los servicios TIC al momento del cese correspondiente. Por razones de seguridad, la suspensión de los servicios podrá ser previa a la total tramitación del cese y deberá ser informada por el Dirección de Desarrollo de las Personas al SISEI.

   SISEI respecto de usuarios que realicen labores directivas y/o críticas podrá realizar un respaldo de la información contenida en su equipamiento.

3. **Renovación de equipos.** Los equipos computacionales serán renovados de acuerdo con los siguientes criterios:

   i. Obsolescencia tecnológica, periodo en que el equipo cumple su vida útil, desde el punto de vista técnico, lo que se definirá en un documento aprobado por el Director del SISEI, en coordinación con VRAF, que se publicará en el portal Mi.Utem

   ii. Costos de reparación superior al 40% del valor del equipo.

   iii. Requerimientos adicionales sea por labores críticas realizadas por el usuario o por situaciones de fuerza mayor, pérdida, hurto o robo.

4. **Prestamos de Equipos a usuarios.** Los equipos que se entreguen en calidad de préstamo deben

    i. Quedar inventariados
    ii. Contar con la autorización de alguna Jefatura responsable y de VRAF.
    iii. Se debe informar al SISEI y a VRAF el estado y las fechas de entrega y devolución.

5. **Asignación de licencias de software de uso transversal.** Se pondrá a disposición de los usuarios, a través del portal mi.utem las distintas licencias de softwares de uso transversal que la universidad disponga en ese instante. Cualquier otro requerimiento de software deberá ser canalizadas por la jefatura o encargado respectivo por los conductos regulares, en los procesos de formulación presupuestaria.

6. **Uso de software específico de las carreras.** Cada Director o Directora de Carrera, Departamento o Escuela deberá definir los softwares de uso específico de uso en sus planes de estudio, los cuales deben ser presupuestados con la debida antelación y solicitados a la Vicerrectoría de Administración y Finanzas e informando oportunamente a SISEI.

7. **Asignación de anexos telefónicos.** Actualmente, el equipamiento telefónico, es una extensión de la red de datos institucional. De esta forma, en la medida que existan recursos disponibles, se asignará a cada usuario bajo su cargo un equipo telefónico acorde a su rol institucional, el que formará parte de los bienes asignados. Es responsabilidad del usuario mantener en buena forma dicho equipamiento y actualizar el número de anexo en las plataformas y el nombre desplegado a través de las interfases provistas para tales efectos.

Artículo 5: Cuidado de los recursos computacionales. La comunidad universitaria que use equipamiento institucional deberá cumplir con las siguientes disposiciones:

1. **Seguridad Física.** Los recursos físicos computacionales y telefonía son elementos delicados y de alto costo que deben ser tratados con el cuidado necesario por parte de los usuarios y personal interno y externo relacionado con la UTEM, quienes deben considerar a lo menos:

    a. **Cuidado de equipos institucionales:** El cuidado básico de los equipos y dispositivos asignados a un usuario es de su responsabilidad, lo que incluye componentes externos e internos, debiendo reportar todo incidente que afecte a dichos equipos a su jefatura y a la Mesa de Ayuda del SISEI. En el caso de los equipos portátiles, dispositivos móviles, anexos telefónicos o bien equipos estacionarios asignados para su uso fuera de las dependencias de UTEM, este cuidado debe extenderse consecuentemente.

    b. **Seguridad de acceso físico:** Será responsabilidad de la Vicerrectoría de Administración y Finanzas el control del acceso a las instalaciones de la Institución, coordinando con SISEI las medidas especiales para el control

del ingreso físico a las dependencias de dicha unidad. Sin perjuicio de los controles regulares dispuestos por la Universidad para el control de acceso, se debe procurar mantener los equipos con el resguardo adecuado.

c. **Seguridad para evitar hurto y/o robo:** Mantener medidas prácticas de seguridad para evitar hurtos y/o robos de los recursos computacionales de la UTEM, especialmente en los casos de equipos portátiles y de telefonía, como por ejemplo notebooks, impresoras, celulares, anexos, memorias externas, dispositivos de comunicaciones y otros. En estos casos se debe reportar a la Mesa de Ayuda del SISEI, adjuntando la constancia en Carabineros, quien informará a la Vicerrectoría de Administración y Finanzas. El uso de dichos equipos de propiedad de la UTEM, fuera de las dependencias debe estar autorizado por la respectiva Jefatura del usuario, quien deberá informar vía correo electrónico a la Vicerrectoría de administración y Finanzas y a SISEI de dicha autorización.

d. **Derrame de líquidos y otros elementos extraños:** El usuario deberá tomar todas las precauciones para evitar riesgos al equipamiento de la UTEM, frente a derrames de líquidos u otros elementos que puedan dañarlos.

e. **Golpes:** El usuario deberá tener especial cuidado para que los dispositivos computacionales no sufran golpes, como por ejemplo los teclados, pantallas, y cualquier elemento del computador estacionario o portátil. El cuidado se extiende al equipamiento móvil que le sea asignado.

f. **Otros daños por mal uso o descuido:** Evitar en todo momento que los recursos computacionales y telefonía sean dañados por mal uso o descuido.

g. **Daños por mal manejo**: Si bien los notebooks están diseñados como equipos móviles, deben tomarse las precauciones para evitar golpes, caídas, temperaturas extremas y derrames de líquidos.
Con todo, en virtud de lo dispuesto en el artículo 84 letra j) del Estatuto Administrativo, en caso de deterioro de los equipamientos institucionales por causas atribuibles al usuario, se harán efectiva las responsabilidades administrativas, lo que deberá demostrarse a través del proceso sumarial respectivo. En caso de personal que preste servicios en calidad de honorarios, deberá incluirse en los contratos de comodato una cláusula que determine su responsabilidad por los deterioros en el equipamiento, causados por su persona.

h. **Otros medios de Seguridad:** SISEI será responsable de poner a disposición de los usuarios cualquier otro medio de seguridad en materias de TIC que la institución incorpore, informando acerca de su uso correcto.

i. **Inventario de infraestructura TIC:** Será responsabilidad de la VRAF el inventario institucional de la infraestructura de TIC, sin perjuicio que SISEI llevará el registro y control técnico de dichos elementos.

2. **Uso y seguridad de la información.** Los equipos computacionales, los servicios, las aplicaciones y sistemas de la UTEM manejan información de trabajo de la Universidad ya sea pública, reservada y/o sensible, y debe ser responsabilidad del usuario que tiene autorización para accederla, mantener un nivel de seguridad adecuado.

   a. **Sistemas de seguridad.** Tanto los computadores, como los servicios, aplicaciones y sistemas de información con que cuenta la UTEM, disponen de sistemas de seguridad basado en la entrega de una "Cuenta", la que tiene asociada una "Contraseña" o "clave secreta" de uso individual e intransferible.

      1- La "Cuenta" corresponde al nombre que identifica de manera única a un usuario de un sistema y es asignado por el SISEI y será denominado Pasaporte Institucional

      2- La "Contraseña" o "clave secreta" corresponde a un conjunto de caracteres, compuesto por números, letras o símbolos que tiene por objeto impedir el acceso no autorizado al computador o al sistema usando una identificación que lo individualice. Las contraseñas o claves son de uso individual e intransferible, y no deben entregarse a ninguna persona, perteneciente o no a la UTEM. Las contraseñas deben considerar a lo menos lo siguiente:

      a) No crear claves fáciles de adivinar, tales como nombres, fechas, lugares, el número directo de su anexo, número de rut, etc.
      b) Cada cierto tiempo cambiar las claves.
      c) No compartir las claves.
      d) No intentar acceder a sistemas o computadores que no han sido expresamente autorizados para su uso. Esta acción puede suponer intento de accesos maliciosos o suplantación de identidad.
      e) No registrar las contraseñas o claves en papel.
      f) Evitar configurar el navegador de internet para que recuerde su usuario y contraseña.
      g) Cambiar las contraseñas o claves cuando haya indicios de un posible compromiso de estas.
      h) Elegir contraseñas que tengan una longitud mínima de ocho caracteres.
      i) Evitar reutilizar contraseñas antiguas.
      j) Cambiar la contraseña temporal al iniciar la primera sesión.
      k) El SISEI podrá gestionar cambios periódicos de contraseñas.

3- SISEI será responsable de la implementación y administración de cualquier otro medio de autenticación y autorización de la cuenta que la institución incorpore.
4- SISEI podrá entregar elementos de autenticación, autorización y firma de acuerdo a la normativa y resoluciones vigente.

b. **La información es uno de los activos de valor estratégico en la institución.** Por tanto, se debe velar por el correcto uso y adoptar precauciones de seguridad de esta, para lo cual:

1- Se debe utilizar para el trabajo diario y labores educativas los servicios, aplicaciones y sistemas de información entregados por la institución, de acuerdo con los roles y/o perfiles asignados al usuario.
2- El usuario debe priorizar el ingreso en línea de la información a los sistemas evitando en la medida de lo posible mantener la información en medios distintos.
3- Se debe utilizar para el trabajo diario, sólo los productos de software provisto y autorizado por la institución.
4- Los usuarios deberán abstenerse de ingresar, almacenar y/o manipular archivos que pudieran tratar contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista y en general aquellos que sean ajenos a las funciones que les correspondan, manteniendo un comportamiento de acuerdo con la normativa institucional.
5- Las aplicaciones y sistemas de la UTEM manejan información reservada y/o sensible y es responsabilidad del usuario que tiene autorización para accederla, mantenerla a buen recaudo.
6- Es responsabilidad del usuario respaldar en forma periódica, toda la información complementaria residente en los computadores a su cargo, en los medios entregados por la institución. SISEI proveerá acceso a nube (cloud) para respaldo a todos los usuarios.
7- El usuario debe conectar el computador personal a la red de UTEM en forma periódica, a lo menos cada 15 días, para los efectos de actualizar los software y servicios de uso general tales como antivirus, sistema operativo y políticas de dominio.
8- La información que se almacena en las bases de datos, producto de la utilización de los sistemas corporativos y servicios de la plataforma TIC, es uno de los activos de valor estratégico en la institución. Por tanto, se debe velar por el correcto uso y precauciones de seguridad de esta, para lo cual:
   a. SISEI será responsable del respaldo de los datos de los sistemas de información corporativos y los servicios de plataforma central TIC que se definan como críticos. Aquellos usuarios y dependencias que requieran respaldo de algún servicio o sistema sectorial, deberá solicitarlo a SISEI.
   b. El cierre de sesión automática de escritorio de cada equipo, del portal de UTEM e intranet y el tiempo de expiración de transacción de sistemas, serán definidos por el SISEI.

c. El SISEI implementará un sistema de control de acceso y monitoreo de los sistemas de información críticos. El periodo de almacenamiento de los registros del monitoreo de sistema será definido por el SISEI.

9- Los funcionarios de SISEI, como así también de las Empresas contratistas o relacionadas, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza, que bajo cualquier medio le sea entregada de parte de la Universidad y que forme parte de los datos, información, procedimientos, conocimientos, comportamientos, actividades, desempeños, funcionamientos, metodologías, rutinas, acciones y en general de toda expresión, en el medio que fuere, que pertenezca a la propiedad exclusiva de la Universidad, esto debe quedar por escrito como cláusula de confidencialidad en las resoluciones de contratación o contratos en el caso de proveedores externos.

c. Uso de las nubes institucionales:

i. La Institución informará en mi.utem.cl, las plataformas oficiales de almacenamiento externo denominadas Nube o Cloud indistintamente.

ii. La Institución determinará el espacio asignado en la nube para cada tipo de usuario, dependiendo de las tareas y funciones institucionales.

iii. El usuario deberá almacenar en el espacio provisto en la nube, toda la información de carácter institucional, en la que se encuentre o haya trabajado, la cual, para todos los efectos jurídicos es propiedad de la Institución. Asimismo, respecto de ella se aplicará cabalmente lo dispuesto en la Resolución Exenta N° 3190 de 2019 que aprueba el Reglamento de Propiedad Intelectual e Industrial de la Universidad Tecnológica Metropolitana.

iv. En caso de que el usuario del equipamiento deje por cualquier motivo de pertenecer a la Institución, la información institucional almacenada en el espacio de la nube quedará disponible para ser accedida por la jefatura directa o su contraparte técnica, previa autorización del Contralor Interno.

Artículo 6°. Uso de los servicios de la plataforma tecnológica. La plataforma tecnológica de la UTEM está compuesta de los elementos de hardware, software y comunicaciones, de su propiedad, necesarias para la prestación de los servicios de tecnologías de información a la institución.

La red de comunicaciones y datos institucionales es un recurso compartido y limitado que sirve para el acceso y uso autorizado de los usuarios internos y externos, de los distintos servicios que entrega la plataforma tecnológica.

SISEI dispone de servicios y sistemas para monitorear los enlaces de comunicación, los accesos y navegación.

Los servicios se ponen a disposición de los usuarios para el uso de las tareas y/o funciones institucionales, en el marco de sus competencias. Se debe evitar cualquier uso privado o particular de ellos.

Para el uso de los servicios de tecnologías de información en la institución, se debe cumplir a lo menos con lo siguiente:

1. **Acceso a la red institucional:**

   a) Los usuarios tendrán acceso a la red de datos institucional previa autorización del SISEI e identificación del rol y/o perfil usuario por parte de la Vicerrectoría de Administración y finanzas o jefatura autorizada.
   b) Ante el uso inadecuado en relación con los fines institucionales de los servicios de la plataforma tecnológica o solicitud de la Autoridad Superior, el SISEI podrá suspender el acceso a la red de datos institucional y/o a los servicios TIC al usuario identificado.
   c) Una vez ingresado a la red de datos institucional, el usuario es responsable por el uso adecuado con relación a los fines institucionales, de los servicios y sistemas disponibles en la plataforma tecnológica y del contenido de las comunicaciones realizadas.
   d) Los usuarios deberán abstenerse de realizar acciones o descargar u operar con archivos o contenido que pudieran tratar elemento insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista o que pudiera afectar de forma negativa o con características de *bullying* a terceros.
   e) En el caso de las redes inalámbricas de invitados se debe procurar no transferir sus credenciales.

2. **Navegación en internet:** Al navegar por internet desde las instalaciones de la UTEM el usuario debe seguir las siguientes instrucciones:

   a. El sistema de navegación a través de internet, que la UTEM pone a disposición de sus usuarios, es una herramienta de trabajo que debe ser usada para estos efectos, debiendo los usuarios ajustarse a una adecuada utilización de dicho sistema, de acuerdo con los valores institucionales.

b. SISEI de la UTEM, por iniciativa propia o a requerimiento de alguna autoridad superior, podrá suspender el acceso a sitios que considere que afectan al buen funcionamiento de la red o que se considere son ajenos a las funciones institucionales.

c. Los usuarios deben informar a SISEI cuando consideren que algún sitio de internet deba ser bloqueado, quien evaluará la solicitud e implementará si la estima procedente.

d. Los usuarios tendrán acceso a los distintos niveles de navegación en internet, de acuerdo con su rol y/o Perfil usuario.

e. Los usuarios deberán abstenerse de visitar sitios o descargar archivos que pudieran tratar contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista o participar en sitios sociales relacionados con las materias señaladas y en general aquellos que sean ajenos a las funciones que les correspondan, manteniendo un comportamiento de acuerdo con lo que indica la normativa institucional.

f. Los usuarios deberán abstenerse de realizar descarga no autorizada de material digital protegido por propiedad intelectual o no aprobado por la institución.

g. Si un usuario requiere del acceso a algún sitio que se encuentre restringido en las instalaciones de la UTEM, deberá solicitar a SISEI la autorización de acceso a dicho sitio, para la evaluación de su procedencia.

3. **Uso del correo electrónico:** Los usuarios y/o usuarios relacionados, deben hacer una adecuada y responsable utilización de las casillas institucionales que se les asignen para el cumplimiento de sus funciones, teniendo en consideración la normativa institucional. Respecto del uso del correo electrónico, deberá observarse en especial lo siguiente:

a) El uso del correo electrónico es para fines institucionales, se debe evitar el tráfico de mensajes de índole privado o personal usando la casilla con dominio xxxx@utem.cl

b) Previa orden judicial o requerimiento del Ministerio Público, la UTEM podrá entregar información acerca del contenido de los correos electrónicos.

c) La UTEM, en la medida que el presupuesto institucional y los aspectos técnicos lo permita, manejará respaldos globales del correo electrónico Institucional a determinada fecha, la que definirá el SISEI, con el fin de recuperar dichos correos ante errores, fallas o solicitudes especiales, así como mantener registros de trazabilidad u otros parámetros técnicos que se requieran.

d) En caso de cese de funciones de un usuario, el SISEI suspenderá o eliminará la cuenta de correo electrónico asociada.

e) La Universidad, como servicio público perteneciente a la Administración del Estado está obligada a atender las necesidades públicas en forma continua y permanente. De esta manera, en caso de ser necesario el acceso a una información institucional almacenada en una cuenta de correo electrónico que esté suspendida, se deberá gestionar la solicitud con Contraloría Interna, quién si lo considera atendible, en virtud del ordenamiento jurídico vigente, solicitará a SISEI el acceso a dicha información institucional almacenada en la cuenta de correo electrónico. Es relevante destacar que, esta acción deber estar fundamentada en virtud del cumplimiento de fines institucionales y el deber que

tiene la Universidad de prestar su servicio de forma permanente y continua. Lo anterior se regulará en el "PROTOCOLO PARA EL ACCESO DE INFORMACIÓN DE INTERÉS Y DE CONTENIDO INSTITUCIONAL Y NO PERSONAL, ALMACENADA EN BASES DE DATOS, SISTEMAS, Y PLATAFORMAS INSTITUCIONALES, CUYA GENERACIÓN ES PRODUCTO DE LA UTILIZACIÓN DE LOS SISTEMAS CORPORATIVOS Y SERVICIOS DE LA PLATAFORMA TIC POR PARTE DE LOS USUARIOS UTEM".

f) El uso del correo debe ser adecuado a los fines institucionales.

g) El usuario es responsable de respaldar y vaciar periódicamente su casilla de correo, previniendo que su espacio de datos o cuota asignada se agote.

h) El usuario deberá usar un lenguaje respetuoso en su texto; los mensajes de ninguna forma podrán ser de contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.

i) El usuario deberá abstenerse de enviar cadenas de mensajes, mensajes no deseados, promociones comerciales o mensajes de uso comercial.

j) El usuario deberá abstenerse de enviar mensajes masivos ya sea al interior de la UTEM o hacia el exterior. En caso de ser requerido, se deberá contar con la autorización de la jefatura y siempre con fines institucionales.

k) El usuario deberá abstenerse de abrir por correo y/o ejecutar programas o documentos con contenido ejecutable cuya procedencia no sea conocida o sea sospechosa, dado que pueden ser archivos que contienen virus. Asimismo, queda prohibido enviar este tipo de contenidos.

l) Ante la salida por cualquier motivo de la institución el usuario entregará la información institucional de la UTEM que manejaba en virtud de su cargo o función, en caso de no hacerlo, se entenderá como disponible para el uso y continuidad de los servicios.

4. **Uso de sistemas de almacenamiento.** SISEI definirá una configuración estándar para los servicios de almacenamiento central:

a. Discos de servidores compartidos o de Red:
Los discos compartidos o de red son áreas para almacenar y trabajar archivos comunes a más de un usuario o para almacenar información de carácter institucional.

b. Servicios Centralizados
Los servicios centrales de almacenamiento, especialmente los del repositorio documental y de sitios colaborativos, deberán ser utilizados según los procedimientos definidos en sus diferentes aplicaciones.

c. Unidad de disco virtual
SISEI podrá dejar a disposición un disco virtual para aquellos usuarios que desempeñen labores críticas, el cual será respaldado periódicamente.

d. Servicios en la NUBE
La UTEM podrá contratar servicios a proveedores en infraestructura externa, denominada NUBE (cloud), con el fin de procesar los servicios y sistemas de

TIC, ya sea como sitio central o de contingencia para todos los usuarios. Será obligación de los usuarios almacenar toda la información institucional en ella.

e. **Servicios de almacenamiento externo**
La información institucional se debe almacenar en cualquier dispositivo de la plataforma tecnológica de UTEM. El usuario podrá solicitar acceso temporal a medios de almacenamientos en plataformas externas, no administradas por UTEM, en cuyo caso la información contenida en estos repositorios será de exclusiva responsabilidad del usuario. SISEI autorizará dichos accesos previa validación de factibilidad técnica y aprobación de la jefatura respectiva.

Artículo 7°. Medidas básicas de Ciberseguridad. Las unidades organizacionales de la UTEM deberán considerar que la ciberseguridad es un aspecto prioritario de considerar y difundir al interior de su comunidad y deberán prestar colaboración a las Unidades técnicas que lo requieran, para la defensa de los activos de información.

La UTEM, en todos los niveles organizacionales y estudiantiles deberá tener en cuenta que los aspectos relativos a la seguridad y ciberseguridad son prioritarios de considerar en todos los procesos internos.

La UTEM deberá tener en cuenta que los procesos que desarrollen y mantengan redes y servicios de telecomunicaciones/TIC seguros, sean fiables y resilientes para aumentar la confianza en el uso de las TIC.

Será considerado como falta a los deberes funcionariales o estudiantiles, realizar acciones que pudieran considerarse como ciberataque o ciberamenaza, que vulnere los servicios y sistemas de información o infraestructura tecnológica. En caso de existir un incidente de esta naturaleza, la Universidad administrará las medidas tendientes a perseguir las responsabilidades administrativas y disciplinarias y remitirá los antecedentes al Ministerio Público para efectos de la investigación penal.

Los usuarios se obligar a seguir las directrices técnicas de seguridad que imparta SISEI en la materia, al resguardo de la información a la que tienen acceso y al tratamiento de datos de conformidad a las políticas e instrucciones institucionales y disposiciones legales sobre la materia que resulten aplicables.

Artículo 8°. Infraestructura Tecnológica Institucional. La Institución cuenta con una plataforma tecnológica híbrida (local y nube) que presta servicios a todas sus dependencias, la que es administrada por el SISEI.

Se entenderá por plataforma tecnológica central a todos los elementos de software, hardware y comunicaciones que componen las salas de procesos central, la sala de procesos de contingencia y las salas de procesos externas. La administración de dicha infraestructura debe considerar a lo menos:

1- Sala de Proceso

a. Las salas de proceso deberán contar con medidas de seguridad y vigilancia apropiada de manera que los usuarios no tengan acceso físico directo, tales como puerta y sistema de control de acceso, sistema de vigilancia y todas aquellas que la normativa vigente amerite.

b. El acceso de terceras personas debe ser identificado y controlado, por personal de la unidad responsable.

c. SISEI debe velar por la mantención periódica de las salas de proceso.

d. Los elementos de software, hardware y comunicaciones deberán renovarse de acuerdo con los criterios de obsolescencia tecnológica, término del soporte por parte del fabricante, existencia de nuevas tecnologías que entreguen mejor servicio a la plataforma y otros que la autoridad determine.

2- Sala de contingencia

a. La Institución podrá contar con una sala de contingencia interna o externa, que debe cumplir con lo señalado en el punto anterior y albergar los servicios y/o sistemas definidos como críticos por la autoridad superior.

b. SISEI deberá documentar y publicar en el portal Mi.Utem, los sistemas y servicios definidos como críticos, salvo aquellos considerados como reservados.

3- Infraestructura de laboratorios y proyectos. Sin perjuicio de la dependencia administrativa, los encargados de laboratorios o proyectos dependientes de la UTEM deberán:

a. Coordinarse, siguiendo las instrucciones técnicas impartidas por SISEI sobre la infraestructura de hardware y software a su cargo.

b. Realizar las mantenciones al equipamiento a su cargo, informando periódicamente a SISEI el calendario y los resultados de éstas.

c. Actualizar el software informando a SISEI de sus resultados

d. Informar al SISEI para el registro técnico y a la VRAF para el inventario institucional, el movimiento de equipos que posee, incluyendo las altas y bajas y actualización de software, hardware y elementos de comunicaciones.

e. Mantener actualizado, con la información requerida, los servicios y sistemas que SISEI le indique.

f. Tomar las acciones pertinentes para el resguardo de la seguridad física y lógica de los sistemas y equipamiento tecnológico a su cargo

g. Informar a sus Jefaturas, el resultado las coordinaciones realizadas con SISEI y VRAF

h. En caso de que existan carreras que, por su deferencia disciplinar requieran softwares específicos, estos deberán ser solicitados con la oportunidad necesaria a VRAF, informando a SISEI. Con todo, SISEI elaborará las directrices técnicas necesarias para su instalación y uso en el equipamiento institucional.

i. SISEI deberá documentar y publicar en el portal Mi.Utem, los sistemas y servicios definidos como críticos, salvo aquellos considerados como reservados.

Artículo 9°. Gestión de Incidentes. Se entiende por incidente cualquier evento que no sea parte de la operación estándar de un servicio y que cause o pueda causar una interrupción o una reducción en la calidad del servicio.

La jefatura y/o el usuario debe reportar a SISEI, a través de los mecanismos que se encuentren a disposición, cualquier incidente vinculado con los servicios de la plataforma tecnológica y comunicaciones.

SISEI es el responsable operativo de la gestión de incidentes vinculados con los servicios de la Plataforma Tecnológica Central, considerando a lo menos el registro, clasificación, resolución y cierre del incidente. Sin perjuicio de lo anterior, cualquier incidente sectorial debe ser reportado a SISEI para su análisis y tratamiento similar.

La UTEM deberá contar con un plan de recuperación ante desastres (DRP), sin perjuicio de lo que la normativa vigente le asigne al encargado de seguridad de la Institución.

Artículo 10°. Propiedad Intelectual. El uso de software sin la correspondiente licencia que autoriza su uso infringe la ley y las normas internas de esta Institución, comprometiendo, por ende, la responsabilidad del usuario involucrado.

De esta forma, y de acuerdo con las normas respectivas, debe estarse a lo siguiente:

a. **Otros materiales protegidos por propiedad intelectual**. Cualquier otro material protegido, como e-books, fotografías, música, videos o similares, no puede copiarse ilegalmente ni mantenerse en los recursos tecnológicos de la UTEM.
b. **Programas P2P**. Los programas de intercambio de archivos están prohibidos, ya que suelen poner en riesgo la seguridad, proveen de copias ilegales de material protegido y, además, son grandes consumidores del ancho de banda de Internet que la UTEM dispone para la realización de sus funciones.
c. **Software autorizado.** En el caso de software libre, "open source", en demo temporal, o de propiedad del usuario, de carácter legal, la instalación en los equipos de la UTEM deberá ser supervisada por el SISEI, el que podrá denegar su instalación atendiendo a las prevenciones de riesgos indicadas. Lo mismo regirá para la conexión al computador de dispositivos externos, como grabadores de CD/DVD, escáneres, cámaras digitales y otros, incluyendo la instalación de software asociado (drivers).
d. **Inscripción de Sistemas de Información.** Los sistemas desarrollados por el SISEI son de propiedad de la Institución, para lo cual el SISEI deberá preparar la documentación y antecedentes necesarios, y requerir a la Vicerrector de Administración y Finanzas o a la Dirección Jurídica para la realización de las gestiones necesarias para su inscripción ante la entidad de propiedad intelectual respectiva, salvaguardando los derechos en cuestión.
e. **Software protegido.** En la UTEM no podrá utilizarse software que infrinja la normativa vigente.
f. **Software no autorizado.** Para prevenir infracciones a la normativa vigente, la introducción de virus, spyware o vulnerabilidades en la red o manejo de la información los usuarios no están autorizados a instalar software en los PCs y notebooks de la UTEM. Toda solicitud de instalación deberá ser coordinada con SISEI de la UTEM.

Artículo 11°. Metodología de gestión de proyectos. Todo proyecto de modernización o innovación Tecnológicos que se lleve adelante en la Universidad y que incluya aspectos relacionados con sistemas de información, plataformas, equipos computacionales, software y transmisión de datos, voz e imágenes, contará con el apoyo logístico y técnico del SISEI.

Para apoyar las principales funciones institucionales el SISEI debe implementar y mantener sistemas de información administrativos que respondan a los procesos operativos y estratégicos de la UTEM.

El desarrollo y mantención de dichos sistemas debe garantizar estándares de calidad, ya sean provistos internamente o a través de proveedores externos. Por esta razón el SISEI debe implementar, mantener y difundir una Metodología de Gestión de Proyectos, que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de sistemas en un ambiente de mitigación del riesgo y aseguramiento de la calidad, la que debe ser publicada en la intranet institucional.

El podrá utilizar para proyectos de infraestructura, administración de servicios y atención de usuarios, una metodología que contenga las mejores prácticas en dichas temáticas, basada en estándares tecnológicos, la que será definida por el Director de SISEI.

Artículo 12°. Interoperabilidad entre sistemas de información. La interoperabilidad de los sistemas institucionales debe considerar el proceso de comunicación establecido para dichos efectos, el lenguaje, la accesibilidad multicanal, el ambiente externo, la identificación y autorización legal, técnica y/o administrativa, la firma electrónica y todo elemento que la normativa vigente establezca.

Artículo 13°. Encargado de seguridad y ciberseguridad. Existirá un Encargado de Seguridad de la Información, designado por el/la Jefe/a Superior del Servicio, quien tendrá por función asesorar a la autoridad superior en las materias relativas a seguridad de la información física y digital, de acuerdo con la normativa vigente.

Las labores de ciberseguridad serán atendidas por un funcionario de SISEI designado por su Director, encargado de la seguridad de la información de los sistemas y servicios de información e infraestructura tecnológica, para proteger y disminuir los riesgos de ciberataques o ciber amenazas.

Capitulo III.
PROTOCOLO PARA EL ACCESO DE INFORMACIÓN DE INTERÉS Y DE CONTENIDO INSTITUCIONAL Y NO PERSONAL, ALMACENADA EN BASES DE DATOS, SISTEMAS, Y PLATAFORMAS INSTITUCIONALES, CUYA GENERACIÓN ES PRODUCTO DE LA UTILIZACIÓN DE LOS SISTEMAS CORPORATIVOS Y SERVICIOS DE LA PLATAFORMA TIC POR PARTE DE LOS USUARIOS UTEM

Artículo 14°. La información que se almacena en las bases de datos, sistemas y plataformas institucionales, producto de la utilización de los sistemas corporativos y servicios de la plataforma TIC, es uno de los activos de valor estratégico en la

Institución. En cuanto activo, de dominio institucional, que se torna en un recurso trascendental para el desarrollo de la Universidad.

Artículo 15°. Los servicios de la plataforma TIC se ponen a disposición de los usuarios para el uso de las tareas y/o funciones institucionales, en el marco de sus competencias debiendo evitarse cualquier uso privado o particular de ellos.

Artículo 16°. Al producirse la devolución de los equipos tecnológicos y la inhabilitación o eliminación de cuentas institucionales cuando un usuario por cualquier motivo deja de pertenecer a la Institución, SISEI podrá realizar un respaldo de la información contenida en su equipamiento y/o cloud y/o plataformas institucionales, cuando éstos realicen labores directivas y/o críticas. En consecuencia, será responsabilidad del usuario que, antes del término de su vínculo jurídico estatuario o contractual con la Universidad, hacer entrega formal de la información institucional que manejaba en virtud de su cargo o función, y en caso de no hacerlo, se entenderá acepta de forma irrevocable que la misma estará disponible para el uso y continuidad de los servicios de la Universidad.

De forma excepcional, se aplicará el siguiente protocolo, para el acceso a información contenida en equipamiento y/o cloud y/o plataformas institucionales, cuando los funcionarios que realicen labores directivas y/o críticas, se encuentren ausentes de la Institución por cualquier motivo, entre ellos, y sin que la presente disposición sea taxativa, por licencia en virtud de reposo laboral, feriado legal, permisos, entre otros.

Cualquiera de los casos señalados en los incisos precedentes, el acceso a la información deberá estar fundamentado en que la información es de interés y de contenido institucional y no personal y, asimismo, la Universidad, como servicio público perteneciente a la Administración del Estado está obligada a atender las necesidades públicas en forma continua y permanente.

Artículo 17°. Para efectos del acceso a la información institucional contenida en cuentas o dispositivos de personas que han dejado de pertenecer a la Institución o se encuentren ausentes de esta, se deberá cumplir con los siguientes criterios, asegurando la transparencia y formalidad para hacer efectivas las disposiciones precedentemente señaladas:

a) La solicitud de acceso a la información de interés y de contenido institucional y no personal, deberá realizarla la jefatura máxima de la unidad respectiva, por escrito, dirigida al Director del SISEI.

b) La solicitud deberá especificar la información de manera pormenorizada, es decir, al menos debe señalar: usuario que la utilizó, especificando si realizaba labores directivas, y de no realizarlas, explicar el por qué dicha información de propiedad institucional se considera críticas para la Corporación; fecha, si es posible hora; bases de datos, sistema, o plataforma institucional en la cual se generó y almacenó; tipo de archivo que la contiene.

c) Se deberá especificar en la solicitud el motivo por el cual el usuario que almacenó la información no puede hacer entrega por sí mismo a esta y proveerla directamente.

d) Se deberá explicar en la solicitud por qué la información requerida es de propiedad y contenido institucional y no personal.

e) El Director de SISEI, realizará un examen de admisibilidad de la solicitud, teniendo especial cuidado que se cumplan todos los requisitos antes señalados, si tiene alguna duda al respecto, le consultará a la Contraloría Interna.

f) Aceptada la solicitud, se concertará día y hora para que personal del SISEI, con la presencia de Secretario General como ministro de fe de la gestión y la jefatura solicitante, se reúnan en dependencias del SISEI y se efectúe la búsqueda y respaldo de la información institucional solicitada.

g) De la gestión realizada se levantará un acta con 3 copias, que deberá suscribir, el funcionario del SISEI, la jefatura solicitante, y el Secretario General como ministro de fe. Se entregará una copia para cada interviniente para su conocimiento y archivo.

h) De todo lo anterior quedará eximido el solicitante, si en su solicitud acompaña autorización del funcionario que dejo de pertenecer a la Institución o se encuentra ausente de la misma, para el uso de sus cuentas UTEM por cualquier medio idóneo, debiendo en este caso, dirigir su solicitud a la Contraloría Interna.

Capitulo IV.
ACTUALIZACIÓN Y DIFUSIÓN DE POLÍTICAS E INSTRUCCIONES

Artículo 18°. Será responsabilidad de todos los usuarios el cumplimiento de las instrucciones impartidas, como asimismo de todos los niveles de jefaturas su supervisión.

Artículo 19°. La implementación técnica y operativa, así como la necesaria generación y actualización de instructivos técnicos que sobre el particular se adopten será de responsabilidad del Director de SISEI, quien deberá mantener informado a las autoridades, además de procurar su difusión y publicación en el portal Mi.Utem.cl

Artículo 20°. El presente documento deberá ser evaluado en forma periódica, a lo menos cada tres años.

Regístrese y Comuníquese

Mario Ernesto Torres Alcayaga
Firmado digitalmente por Mario Ernesto Torres Alcayaga
Fecha: 2023.12.28 17:20:02 -03'00'

MARISOL PAMELA DURAN SANTIS
Firmado digitalmente por MARISOL PAMELA DURAN SANTIS
Fecha: 2023.12.28 16:51:57 -03'00'

DISTRIBUCIÓN:

RECTORÍA
DIRECCIÓN GENERAL DE ANÁLISIS INSTITUCIONAL Y DESARROLLO ESTRATÉGICO
- Departamento de Desarrollo Estratégico
- Departamento de Autoevaluación y Análisis
- Departamento de Sistemas de Servicios de Informática - SISEI

DIRECCIÓN DE ASUNTOS NACIONALES E INTERNACIONALES
GABINETE DE RECTORÍA
- Programa de Comunicaciones y Asuntos Públicos

DIRECCIÓN JURÍDICA
- Programa Fomento a la Investigación, Desarrollo e Innovación (PIDI)
- Programa de Genero y Equidad

VICERRECTORÍA ACADÉMICA
DIRECCIÓN GENERAL DE DOCENCIA
- Subdirección de Docencia
- SECRETARIAS DE ESTUDIOS (3)
- SISTEMA DE BIBLIOTECAS (5)

DIRECCIÓN DE DESARROLLO ESTUDIANTIL
- Servicio de Bienestar Estudiantil
- Servicio de Educación Física, Deportes y Recreación
- Servicio de Salud Estudiantil - SESAES
- Programa Propedéutico

DIRECCIÓN DE ASEGURAMIENTO DE LA CALIDAD DE PREGRADO Y POSTGRADO
SISTEMA DE BIBLIOTECAS
- Biblioteca Sede Central
- Biblioteca Sede Macul
- Biblioteca Sede Providencia
- Biblioteca Sede Almirante Latorre

DEPARTAMENTO DE ADMINISTRACIÓN DE SEDES REGIONALES Y LICEOS
UNIDAD DE ESTUDIOS
DIRECCIÓN DE EVALUACIÓN ACADÉMICA
DIRECCIÓN DE TECNOLOGIA EDUCATIVA Y APRENDIZAJE CONTINUO
DIRECCIÓN DESARROLLO ACADEMICO
UNIDAD DE APOYO TECNICO
FACULTAD DE ADMINISTRACIÓN Y ECONOMÍA
- Programa de Estudios de Políticas Públicas - PEPP

FACULTAD DE CIENCIAS DE LA CONSTRUCCIÓN Y ORDENAMIENTO TERRITORIAL
- Programa de Competencias Laborales
  Programa: Centro de Ensayos e Investigaciones de Materiales – CENIM

FACULTAD DE CIENCIAS NATURALES, MATEMÁTICAS Y DEL MEDIO AMBIENTE
- Programa: Centro de Desarrollo de Tecnologías Agroindustriales - CEDETAI
- Programa: Centro de Desarrollo de Tecnologías para el Medio Ambiente - CEDETEMA

FACULTAD DE HUMANIDADES Y TECNOLOGÍAS DE LA COMUNICACIÓN SOCIAL
- Programa: Centro de Desarrollo Social - CEDESOC
- Programa: Centro de Familia y Comunidad - CEFACOM
- Programa Centro de Cartografía Táctil

FACULTAD DE INGENIERIA
- Programa Tecnológico del Envase – PROTEN

VICERRECTORIA DE INVESTIGACION Y POSTGRADO
DIRECCIÓN DE INVESTIGACIÓN
- Programa de Prospectiva e Innovación Tecnológica - PROTEINLAB

DIRECCIÓN DE ESCUELA DE POSTGRADO
VICERRECTORÍA DE TRANSFERENCIA TECNOLÓGICA Y EXTENSIÓN
DIRECCIÓN DE TRANSFERENCIA TECNOLÓGICA
DIRECCIÓN DE CAPACITACIÓN Y POSTÍTULOS
- Editorial
- Desarrollo Cultural

VICERRECTORÍA DE ADMINISTRACIÓN Y FINANZAS
DIRECCIÓN DE ADMINISTRACIÓN
- Departamento de Obras y Servicios Generales
- Departamento de Abastecimiento
- Unidad de Bodega
- Unidad de Inventario
- Jefe de Campus Área Central
- Jefe de Campus Providencia
- Jefe de Campus Macul

DIRECCIÓN DE FINANZAS

- Departamento de Contabilidad
- Departamento de Aranceles
- Departamento de Administración de Fondos
- Departamento de Cobranza
- Unidad de Estudios
- UNIDAD DE CONTROL PRESUPUESTARIO

DIRECTOR DE DESARROLLO Y GESTIÓN DE PERSONAS

- Departamento de Desarrollo Organizacional
- Departamento de Gestión de Personas

SERVICIO DE BIENESTAR DEL PERSONAL

SECRETARÍA GENERAL

- Unidad de Títulos y Grados
- Unidad de Archivo Institucional
- Oficina General de Partes

CONTRALORÍA INTERNA

- Departamento de Control de Legalidad

Departamento de Auditoría Interna

AFAUTEM

ANFUTEM

ANFUTEM 2.0

PCT

PCT/GMN