D.J. (307)

SANTIAGO, 11 JUN. 2020

RESOLUCION Nº 0777

VISTOS: lo dispuesto en la Ley Nº 19.239; en el D.S. N° 130 de 2017; 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; en el Decreto N° 83 de 2004 del Ministerio Secretaría General de Gobierno que "Aprueba norma técnica para los órganos de administración del estado sobre seguridad y confidencialidad de los documentos electrónicos", y el acuerdo adoptado por el Honorable Consejo Superior de la Universidad de fecha 14 de mayo de 2020, que consta en certificado emitido por su Secretario con fecha 10 de junio de 2020,

CONSIDERANDO:

1.- Que de conformidad a la Ley N° 19.239 la Universidad Tecnológica Metropolitana es una institución de educación superior del Estado, autónoma, con personalidad jurídica y patrimonio propios. Su objeto fundamental es 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 la formación académica, científica, profesional y técnica orientada preferentemente al quehacer tecnológico.

2.- Que, de conformidad a lo prescrito por las normas que gobiernan a la institución, el Rector sometió a consideración del Honorable Consejo Superior, organismo colegiado de mayor jerarquía de la Corporación, la propuesta denominada "Políticas referidas al uso de recursos tecnológicos, comunicaciones y seguridad de la información de la Universidad Tecnológica Metropolitana", por cuanto es competencia del órgano colegiado de más alta jerarquía de la Corporación fijar las políticas globales de desarrollo institucional y cautelar los fines de la Universidad, de acuerdo al artículo 4 del DFL N° 2 de 1994 del Ministerio de Educación, que aprueba el Estatuto Orgánico de la Universidad, las que fueron aprobadas en sesión de fecha 14 de mayo de 2020.

3.- Que, las referidas políticas establecen que el área de TIC de la UTEM deberá dictar y actualizar las instrucciones que sean necesarias para la correcta implementación de estas políticas. Para cumplir dicho mandato, el Director del Departamento de Sistemas de Información y Servicios de Informática, ha solicitado aprobar las instrucciones que acompaña a su correo de fecha 10 de junio de 2020.

4.- Que, entre los fundamentos tenidos a la vista para la elaboración y aprobación de estas instrucciones, se encuentra la circunstancia que, el Estado de Chile en sus diferentes procesos de modernización ha fijado a las tecnologías de información como un medio importante y principal para los procesos de innovación y desarrollo, teniendo en cuenta la masividad y popularidad de éstas. Para ello, ha dictado una serie de normativas legales como por ejemplo el Decreto N° 83 de 2004 del Ministerio Secretaría General de Gobierno que "Aprueba norma técnica para los órganos de administración del estado sobre seguridad y confidencialidad de los documentos electrónicos". En dicha regulación, se indica "Las exigencias y recomendaciones previstas en esta norma, tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada." Complementariamente a lo anterior, se ha aprobado la Ley N° 19.799 sobre "Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma".

5.- Que, por otro lado, en el año 2017 se dio a conocer un Plan Nacional de Ciberseguridad que ha dejado de ser un tema circunscrito al ámbito técnico, pasando a ser parte de la política pública nacional. En forma previa y de acuerdo a lo expuesto en la agenda digital y, con el fin de formular una estrategia en materia de seguridad cibernética, en abril de 2015, mediante el Decreto Supremo N° 533, se creó el Comité Interministerial sobre Ciberseguridad (CICS). La Política Nacional de Ciberseguridad se articula en dos ejes centrales, el primero de ellos establece una agenda con disposiciones específicas para ser implementadas entre los años 2017-2019, y objetivos a largo plazo orientados al año 2022, siendo su principal meta lograr para Chile un ciberespacio libre, abierto, seguro y resiliente. Complementariamente, el pasado mes de noviembre se publicó la Ley N° 21.180 sobre Transformación Digital del Estado la cual introduce una serie de modificaciones a diversos cuerpos normativos con el objeto de incorporar la tecnología en distintos procedimientos seguidos ante organismos públicos, buscando de esa manera reducir sus tiempos de tramitación y facilitar el acceso de la ciudadanía a diversos trámites a cargo del Estado.

6.- Que, en uso de su autonomía, la UTEM recientemente ha aprobado las "Políticas referidas al uso de recursos tecnológicos, comunicaciones y seguridad de la información", que justamente tributan a los fines generales previstos por la Administración del Estado, las cuales sirven como estándar para el desarrollo en esta área del conocimiento. A mayor abundamiento, el carácter tecnológico impreso en su misión y objetivo, conmina a esta Corporación a regular el uso de losrecursos de tecnología e información, de acuerdo con el mandato entregado por su Consejo Superior, por tanto

RESUELVO:

Artículo único. - **Apruébense** las **INSTRUCCIONES SOBRE USO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES LA UNIVERSIDAD TECNOLÓGICA METROPOLITANA**, cuyo texto es el siguiente:

I. UNIDAD OPERATIVA RESPONSABLE

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.

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.

II. INSTRUCCIONES SOBRE USO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Para el cumplimiento de las políticas antes indicadas, se imparten las siguientes instrucciones que deben seguir todos los usuarios que hagan uso de los recursos y servicios de tecnología de información y comunicaciones de propiedad de la UTEM.

1. ASIGNACIÓN DE LOS RECURSOS COMPUTACIONALES

La institución, por medio del SISEI y VRAF, cumplirá con:

a. 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 el 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, el SISEI deberá evaluar una nueva asignación.

b. 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.

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

c. Renovación de equipos
Los equipos computacionales serán renovados de acuerdo a 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.

d. 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.

2. CUIDADO DE LOS RECURSOS COMPUTACIONALES

2.1.SEGURIDAD FISICA

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 el

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.

h. Otros medios de Seguridad:
   El 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 SISE llevara el registro y control técnico de dichos elementos.

2.2.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. 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.

   i. 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

   ii. 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.

   iii. El SISEI será responsable de la implementación y administración de cualquier otro medio de autenticación y autorización de la cuenta que la institución incorpore.

   iv. 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:

i. Se debe utilizar para el trabajo diario y labores educativas los servicios, aplicaciones y sistemas de información entregados por la institución, de acuerdo a los roles y/o perfiles asignados al usuario.

ii. 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.

iii. Se debe utilizar para el trabajo diario, sólo los productos de software provisto y autorizado por la institución.

iv. 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 a la normativa institucional.

v. 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.

vi. 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.

vii. 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.

viii. 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) El 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.

ix. 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.

3. USO DE LOS SERVICIOS DE LA PLATAFORMA TECNOLOGICA

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.

El SISEI de la UTEM 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:

3.1. 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 bulling a terceros.

e. En el caso de las redes inalámbricas de invitados se debe procurar no transferir sus credenciales.

3.2.NAVEGACION 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. El 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 al 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 a 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 al SISEI la autorización de acceso a dicho sitio, para la evaluación de su procedencia.

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

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

g. 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.

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

i. 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.

j. 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.

k. 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.

3.4.USO DE SISTEMAS DE ALMACENAMIENTO

El SISEI definirá una configuración estándar para los computadores institucionales, que asegure la correcta instalación del sistema operativo y del área de trabajo:

a. Disco local para Sistema Operativo (C:):
Corresponde al disco duro local principal del PC y/o notebook, en el cual reside el sistema operativo y el software necesario que haya sido instalado. En este disco no deben encontrarse archivos de trabajo, ni siquiera en forma temporal, ya que no existen respaldos ni forma de recuperar los archivos perdidos o dañados. La UTEM no desplegará esfuerzos por recuperar archivos de un disco duro C: y su recuperación será mediante formateo e instalación estándares.

b. Disco D: o área de trabajo.
Corresponde al área habilitada al usuario del PC y/o notebook, para el manejo de los archivos de trabajo, la cual debe ser respaldada en forma periódica por el usuario.

El 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, que deba ser respaldada.

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. El 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, con el fin de procesar los servicios y sistemas de TIC, ya sea como sitio central o de contingencia para todos los usuarios

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. El SISEI autorizará dichos accesos previa validación de factibilidad técnica y aprobación de la jefatura respectiva.

4. INFRAESTRUCTURA TECNOLOGICA INSTITUCIONAL

La institución cuenta con una plataforma tecnológica 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:

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

d. Los elementos de software, hardware y comunicaciones deberán renovarse de acuerdo a 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.

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

4.3.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 el SISEI sobre la infraestructura de hardware y software a su cargo.

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

c.- Actualizar el software informando al 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 el 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

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

5. GESTION 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 al SISEI, a través de los mecanismos que se encuentren a disposición, cualquier incidente vinculado con los servicios de la plataforma tecnológica y comunicaciones.

El 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, el que se debe actualizar cada 3 años.

6. 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.

d. Software protegido.
   En la UTEM no podrá utilizarse software que infrinja la normativa vigente.

e. 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.

7. 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 del SISEI.

8. 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.

9. ENCARGADO DE SEGURIDAD Y CIBERSEGURIDAD

Existirá un Encargado de Seguridad de TIC, designado por el Rector, quien tendrá por función asesorar a la autoridad superior en las materias relativas a seguridad de la información, de acuerdo con la normativa vigente. Las labores de ciberseguridad serán atendidas por un funcionario de SISEI designado por su Director.

III. ACTUALIZACIÓN Y DIFUSIÓN DE POLITICAS E INSTRUCCIONES

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

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 del Departamento de Sistemas y Servicios SISEI, quien deberá mantener informado a la Jefatura Superior, además de procurar su difusión y publicación en el portal Mi.Utem.cl

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

Regístrese y comuníquese

pbr

LUIS LEONIDAS PINTO FAVERIO

Firmado digitalmente por LUIS LEONIDAS PINTO FAVERIO
Fecha: 2020.06.12 08:34:59 -04'00'

DISTRIBUCION:

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
Programa de Fomento a la Investigación, Desarrollo e Innovación y Creación (PIDi)
Programa de Sustentabilidad
DIRECCIÓN JURÍDICA
VICERRECTORÍA ACADÉMICA
DIRECCIÓN DE DESARROLLO ACADÉMICO
Programa de Prospectiva e Innovación Tecnológica - PROTEINLAB
DIRECCIÓN DE RELACIONES ESTUDIANTILES
Servicio de Bienestar Estudiantil
Servicio de Educación Física, Deportes y Recreación
Servicio de Salud Estudiantil – SESAES
Oficina de Denuncia
DIRECCIÓN DE DOCENCIA
SECRETARIAS DE ESTUDIOS (3)
SISTEMA DE BIBLIOTECAS (5)
DIRECCIÓN DE EVALUACIÓN ACADÉMICA
FACULTAD DE ADMINISTRACIÓN Y ECONOMÍA
Programa de Políticas Públicas – PEPP
Departamento de Contabilidad y Gestión Financiera
Departamento de Economía, Recursos Naturales y Comercio Internacional.
Departamento de Estadística y Econometría
Departamento de Gestión de la Información
Departamento de Gestión Organizacional
Escuela de Contadores Auditores
Escuela de Bibliotecología
Escuela de Administración
Escuela de Comercio Internacional
Escuela de Ingeniería Comercial
FACULTAD DE CIENCIAS DE LA CONSTRUCCIÓN Y ORDENAMIENTO TERRITORIAL
Programa de Competencias Laborales
Programa: Centro de Ensayos e Investigaciones de Materiales – CENIM
Departamento de Prevención de Riesgos y Medio Ambiente
Departamento de Ciencias de la Construcción
Departamento de Planificación y Ordenamiento Territorial
Escuela de Prevención de Riesgos y Medio Ambiente
Escuela de Construcción Civil
Escuela de Arquitectura
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
Departamento de Química
Departamento de Matemáticas
Departamento de Física
Departamento de Biotecnología
Escuela de Química

Escuela de Industria Alimentaria y Biotecnología
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
Departamento de Diseño
Departamento de Cartografía
Departamento de Trabajo Social
Departamento de Humanidades
Escuela de Diseño
Escuela de Cartografía
Escuela de Trabajo Social
FACULTAD DE INGENIERIA
Departamento de Informática y Computación
Departamento de Industria
Departamento de Electricidad
Departamento de Mecánica
Escuela de Informática
Escuela de Industria
Escuela de Mecánica
Escuela de Electrónica
Escuela de Geomensura
Escuela de Transporte y Tránsito
Programa Tecnológico del Envase – PROTEN
UTEM-VIRTUAL
PIDI
ESCUELA DE POSTGRADO
VICERRECTORÍA DE TRANSFERENCIA TECNOLÓGICA Y EXTENSIÓN
DIRECCIÓN DE TRANSFERENCIA TECNOLÓGICA
DIRECCIÓN DE CAPACITACIÓN Y POSTÍTULOS
Editorial
Desarrollo Cultural
VICERRECTORIA DE ADMINISTRACIÓN Y FINANZAS
DIRECCIÓN DE ADMINISTRACIÓN
Dirección de Desarrollo y Gestión de Personas
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
Unidad de Estudios
Departamento de Cobranza
UNIDAD DE CONTROL PRESUPUESTARIO
SERVICIO DE BIENESTAR DEL PERSONAL
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
Dirección de Investigación
Dirección de Escuela de Postgrado
ANFUTEM
ANFUTEM 2.0
AFAUTEM
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

PCT
PCT