5. Uso aceptable de los recursos de tecnología de la información

5.1 Introducción. La tecnología de la información (TI), la creciente gran variedad de recursos de comunicación de datos de informática y electrónicos, es una parte integral del cumplimiento de las funciones docentes, de investigación, administrativas y de servicios de la Universidad de New Hampshire. Los miembros de la comunidad de la Universidad tienen acceso a estos recursos de TI y la responsabilidad como encargados de no usarlos indebidamente. Esta Política de Uso Aceptable (PUA) establece directrices para el uso aceptable de los recursos de TI de la Universidad, así como también el acceso a la información de la Universidad para gestionar estos recursos.

5.1.2 El uso de los recursos de tecnología de la información se puede clasificar ampliamente como aceptable, permitido o prohibido.

5.1.3 El uso aceptable de los recursos de tecnología de la información es el uso legal acorde con la misión de la Universidad de New Hampshire; es decir, el uso que impulsa la misión de aprendizaje y docencia, investigación y extensión de la Universidad.

5.1.4 El uso permitido es el uso legal para otros fines que no afecta el uso aceptable. La cantidad de uso permitido puede variar con el paso del tiempo en función de la reserva de capacidad de los recursos de tecnología de la información disponibles más allá del uso aceptable.

5.1.5 El uso prohibido es el uso ilegal y cualquier otro uso que no sea ni aceptable ni permitido.

5.1.6 La mayor parte del uso de TI se asemeja a la actividad familiar en otros medios y formatos, lo que hace que las políticas actuales de la Universidad sean importantes para determinar cuál es el uso apropiado. El uso del correo electrónico (*e-mail*) en vez de la correspondencia escrita corriente, por ejemplo, no fundamentalmente altera la naturaleza de la comunicación, ni tampoco las políticas que la orientan. Las políticas de la Universidad que ya rigen la libertad de expresión, el acoso discriminatorio y cuestiones relacionadas en el contexto de la expresión escrita corriente, también rigen la expresión electrónica. Esta PUA aborda las circunstancias que son específicas del campo de la TI y tiene como objetivo ampliar, pero no sustituir, otras políticas pertinentes de la Universidad.

5.1.7 Para conocer las declaraciones de otras políticas vigentes de la Universidad, se debe consultar el Manual de política del Sistema de la Universidad de New Hampshire (University System of New Hampshire Policy Manual, OLPM); el Manual de procedimientos económicos y administrativos (Financial and Administrative Procedures Manual, FAP); los manuales de los profesores, personal PAT y personal operativo; los Derechos, Normas y Responsabilidades de los Estudiantes; y las políticas que rigen el uso de laboratorios y sistemas de TI específicos. Se deben consultar también los enlaces a documentos en línea de la sección de contra referencias de la política que se presentan más abajo.

5.2 Objetivo. El objetivo de esta PUA es garantizar una infraestructura de tecnología de la información que impulse las misiones fundamentales de la Universidad en relación con la docencia, investigación, administración y servicio. En particular, esta PUA aspira a impulsar estos objetivos:

5.2.1 Garantizar la integridad, confiabilidad, disponibilidad y rendimiento de los recursos de TI.

5.2.2 Garantizar que el uso de los recursos de TI sea cónsono con los principios y valores que rigen el uso de otras facilidades y servicios de la Universidad.

5.2.3 Garantizar que los recursos de TI se usen para los objetivos previstos.

5.2.4 Establecer procedimientos para atender violaciones a la política y sanciones para quienes cometan violaciones.

5.3 Definiciones

5.3.1 OLPM. "OLPM" es el Manual de política en línea del Sistema de la Universidad de New Hampshire, que es la compilación original de políticas institucionales formales de todo el sistema y el campus.

5.3.2 FAP. "FAP" se refiere al Manual de procedimientos económicos y administrativos que se aplica a todos los campus del USNH, como lo aprobó el Consejo de Administración o el Consejo de Políticas Económicas y Planificación.

5.3.3 PUA. "PUA" es la política de uso aceptable de los recursos de tecnología de la información y se refiere a este documento.

5.3.4 Universidad. El término "Universidad" se refiere a la Universidad de New Hampshire (UNH); ambos recintos, Durham y Manchester.

5.3.5 Recursos de TI. De acuerdo con la definición del OLPM (USY.VI.F.4.2), "los recursos tecnológicos incluirán, entre otros, teléfonos, aplicaciones de correo de voz, computadoras de escritorio, redes informáticas y aplicaciones de correo electrónico, que la UNH posea u opere. El término también incluirá recursos tecnológicos no institucionales que se usen en la ejecución de obligaciones oficiales por parte de los profesores, los empleados o los administradores, pero sólo en la medida de dicho uso".

5.3.6 Usuario. Un "usuario" es cualquier persona, autorizada o no, que haga uso de cualquier recurso de TI desde cualquier lugar. Por ejemplo, usuarios son aquellos que tienen acceso a los recursos de TI en un laboratorio de computadoras o a través de una red electrónica. La "condición de usuario" se refiere a su relación con la Universidad; es decir, estudiante, profesor, empleado, contratista, egresado, miembro del público, etcétera.

5.3.7 Autoridad disciplinaria. Si una resolución informal no surte efecto o el uso indebido es más grave, se referirá al procedimiento judicial o disciplinario vigente de la Universidad, según corresponda de acuerdo a la condición del usuario. Por ejemplo, los estudiantes están amparados por el código de conducta y procedimientos judiciales para estudiantes, los empleados están amparados por el OLPM y los profesores están amparados por el convenio colectivo. Esto puede incluir la policía de la Universidad cuando parece haberse infringido la ley.

5.3.8 Autoridad de sistemas. En tanto la Universidad como entidad es la propietaria o la operadora legal de todos sus recursos de TI, delega la supervisión de sistemas particulares al director de una subdivisión, oficina o departamento específico de la Universidad ("autoridad de sistemas"), o a un miembro específico del personal docente, en el caso de recursos de TI adquiridos con fondos para investigación o de otro tipo por los que son responsables individualmente. Por ejemplo, la autoridad de sistemas del ambiente de Exchange administrado centralmente es el Assistant Vice-President, Enterprise Technology Services.

5.3.9 Administrador del sistema. Las autoridades de sistemas pueden designar a otra persona como "administrador del sistema" para administrar los recursos del sistema específico del cual es responsable la autoridad de sistema. Los administradores de sistemas supervisan la actividad diaria del sistema y están autorizados para determinar a quién se le permite acceder a los recursos de TI específicos, de conformidad con las políticas y procedimientos vigentes.

5.3.10 Cuenta electrónica. Una "cuenta electrónica" es cualquier nombre de acceso y su contraseña asociada que se asigna a un usuario para acceder a los recursos de tecnología de la información.

5.3.11 Autorización específica. Esto se refiere al permiso documentado que proporciona el administrador del sistema correspondiente.

5.4 Alcance

5.4.1 Esta política se aplica a todos los usuarios de los recursos de TI, lo que incluye, entre otros, a los estudiantes, profesores y empleados de la Universidad, y al uso de todos los recursos de TI. Estos comprenden sistemas, redes e instalaciones administradas por Tecnología de la Información de UNH (UNH IT), así como también aquellos administrados por instituciones educativas, departamentos, laboratorios de la Universidad individuales, y otras entidades universitarias. Esto incluye al público en general.

5.4.2 El uso de los recursos de TI de la Universidad, aun cuando se lleve a cabo en una computadora de propiedad privada que no sea manejada ni mantenida por la Universidad, se rige por esta política.

5.5 Uso aceptable de los recursos de TI. Si bien esta política establece los límites generales de uso aceptable de los recursos de TI, los estudiantes, profesores y empleados deben consultar sus respectivos manuales sobre la política vigente para obtener información más detallada sobre el uso autorizado y apropiado. Esto incluye el Manual de política del Sistema de la Universidad de New Hampshire (University System of New Hampshire Policy Manual, OLPM); el Manual de procedimientos económicos y administrativos (Financial and Administrative Procedures Manual ,FAP); los manuales para profesores, personal profesional y técnico (PAT) y personal operativo; los Derechos, Normas y Responsabilidades de los Estudiantes; y restricciones específicas que pudieran implementar los administradores de sistemas sobre el uso de recursos. Las autoridades o administradores de los recursos de TI pueden decidir

imponer controles más estrictos que los que exige esta política. En todos los casos en los que los controles sean menos restrictivos que lo que indica esta PUA, se aplicará esta PUA.

5.5.1 Los recursos de TI sólo se pueden usar para los fines autorizados; es decir, para apoyar la misión principal de docencia, investigación y extensión de la Universidad (BOT.II.H.1.1). Los objetivos particulares de los recursos de TI, al igual que la naturaleza y el alcance del uso autorizado y el uso personal eventual, pueden variar de acuerdo con las obligaciones y responsabilidades del usuario.

5.5.2 Autorización adecuada. Los usuarios solamente tienen derecho a acceder a aquellos elementos de los recursos de TI que estén acordes con su autorización.

5.5.3 Uso permitido. Está permitido el uso personal incidental de los recursos de TI, como por ejemplo navegar en la red y el correo electrónico personal, en tanto sea consistente con esta PUA y las políticas y directrices vigentes de las unidades de trabajo departamentales. La capacidad de los recursos de TI disponibles más allá del uso aceptable variará con el transcurso del tiempo y por lo tanto el uso individual se limitará si interfiere con la misión principal de la Universidad.

5.6 Uso prohibido. El uso prohibido es el uso ilegal y cualquier otro uso que no sea ni aceptable ni permitido. Las siguientes categorías de uso son inapropiadas y están prohibidas.

5.6.1 Uso que impida, interfiera, perjudique o cause perjuicio de alguna forma a las actividades de otras personas. Los usuarios no deben interferir, ni intentar interferir con el uso normal de los recursos de TI por parte de otros usuarios. La interferencia comprende: ataques de denegación de uso, uso indebido de listas de correo electrónico, propagación de cadenas de cartas o bromas, y envío intencional o involuntario de correo electrónico no deseado a usuarios sin autorización específica o una forma de excluirse (captación indebida de usuarios o *slamming*). También se prohíben los comportamientos que provocan la carga de tráfico de la red que interfiera con el uso normal y previsto de los recursos de TI.

5.6.2 Uso que sea incompatible con la condición de organización sin fines de lucro de la Universidad. La Universidad es una organización exenta de impuestos, sin fines de lucro, y como tal está sujeta a leyes federales, estatales y locales específicas con respecto a las fuentes de ingreso, actividades políticas, uso de la propiedad y cuestiones similares. Como consecuencia, por lo general está prohibido el uso comercial de los recursos de TI para fines no relacionados con la Universidad, salvo si está específicamente autorizado y permitido de conformidad con las políticas de conflicto de intereses,

empleo externo, y otras políticas relacionadas de la Universidad (FAP 8-006). Se espera que los administradores de sistemas elaboren directrices más detalladas para el uso del correo electrónico, páginas web y otros servicios en recursos específicos de TI.

5.6.3 También se prohíbe el uso de los recursos de TI de una manera que sugiera el aval de la Universidad a un candidato político o iniciativa de votación. Los usuarios deben abstenerse de usar recursos de TI con fines de cabildeo que sugiera la participación de la Universidad, salvo en el caso de cabildeo autorizado a través o en colaboración con la oficina del *General Counsel* del Sistema de la Universidad de New Hampshire.

5.6.4 Acoso o uso intimidatorio. Esta categoría incluye, por ejemplo, el acoso discriminatorio, la exhibición del material ofensivo o sexual en el lugar de trabajo, y contactos no bienvenidos reiterados con otra persona.

5.6.5 Uso que daña la integridad de la Universidad u otros recursos de TI. Esta categoría incluye, entre otras, las siguientes actividades:

5.6.5.1 Tentativas de anular la seguridad del sistema. Los usuarios no deben anular ni intentar anular la seguridad de los recursos de TI, como por ejemplo mediante análisis (descifrar contraseñas o *cracking*), o adivinar y emplear la contraseña de otro usuario, o afectar la cerradura de habitaciones o sistemas de alarma. Sin embargo, esta disposición no prohíbe que UNH IT o los administradores de sistemas usen programas de análisis de seguridad dentro del alcance de autoridad de sus sistemas.

5.6.5.2 Acceso o uso no autorizado. La Universidad reconoce la importancia de preservar la privacidad de los usuarios y los datos guardados en los sistemas de TI. Los usuarios deben respetar este principio absteniéndose del acceso no autorizado a los recursos de TI, y no colaborando con el acceso no autorizado. Esto se aplica a diversas situaciones:

5.6.5.2.1 Por ejemplo, una organización o persona que no pertenezca a la Universidad, no puede usar recursos de TI que no sean públicos sin una autorización específica.

5.6.5.2.2 Por ejemplo, las computadoras de propiedad privada se pueden usar para proporcionar recursos de información pública, pero dichas computadoras no pueden alojar (*host*) sitios ni servicios, en

toda la red de la Universidad, para organizaciones que no pertenezcan a la Universidad sin la autorización específica.

5.6.5.2.3 Por ejemplo, los usuarios tienen prohibido acceder o intentar ingresar datos en los recursos de TI a los que no están autorizados a acceder.

5.6.5.2.4 Por ejemplo, los usuarios no deben hacer ni intentar hacer cambios deliberados, no autorizados, a los datos de un sistema de TI.

5.6.5.3 Equipo de conexión de redes y software. Salvo que lo autorice específicamente el administrador del sistema de red, ningún usuario conectará equipos de conexión de redes (dispositivos de encaminamiento o *router*s, distribuidores, programa detectores de paquetes o *sniffers*, etc.) a la red del campus, ni operará software de servicios de red (encaminamiento o *routing*, detección de paquetes o *sniffing*, nombre de dominio, servicio de difusión, etc.) en una computadora conectada a la red.

5.6.5.4 Uso oculto: Los usuarios no deben ocultar su identidad al usar los recursos de TI, salvo cuando la opción de acceso anónimo está explícitamente autorizada. Los usuarios también tienen prohibido suplantar o hacerse pasar por otras personas o usar una identidad falsa de cualquier otra manera.

5.6.5.5 Distribución de mensajes falsos de alarma y virus informáticos. Los usuarios no deben distribuir ni activar a sabiendas mensajes falsos de alarma, virus informáticos, gusanos ni otros programas maliciosos cuyo objetivo sea poner en peligro los recursos de TI.

5.6.5.6 Retiro de datos o equipos. Sin la autorización específica de un administrador de sistema, los usuarios no deben retirar de su ubicación normal ningún equipo de recursos de TI que sea administrado por la Universidad o de su propiedad.

5.6.6 Violación de la ley

5.6.6.1 Está prohibido el uso ilegal de los recursos de TI, es decir, el uso que viole el derecho civil o el derecho penal a nivel federal, estatal o local. Algunos ejemplos de tales usos son: promover el esquema

de pirámide, distribuir material obsceno ilegal; recibir, transmitir o poseer pornografía infantil; infringir derechos de autor; y hacer amenazas de bombas.

5.6.6.2 Con respecto a la infracción de derechos de autor, los usuarios deben tener presente que la ley de derechos de autor rige (entre otras actividades) la copia, visualización y uso de software y otras obras en forma digital (texto, sonido, imágenes y otros contenidos multimedia). La ley permite el uso de material protegido por el derecho de autor sin la autorización del titular del derecho de autor para "uso razonable" limitado. El uso educativo debe cumplir con las directrices de uso razonable normal.

5.6.7 Violación de contratos de la Universidad. Todo el uso de los recursos de TI debe ser conforme a las obligaciones contractuales de la Universidad, entre las que se incluyen las limitaciones definidas en los contratos de software y otros acuerdos de licencia.

5.6.8 Violación de las políticas de redes de información externas. Los usuarios deben cumplir con todas las políticas vigentes sobre redes de información externa cuando usen dichas redes.

5.7 Responsabilidad por la cuenta personal. Los usuarios son responsables de mantener la seguridad de sus propias cuentas y contraseñas para acceder a los recursos de TI. Las cuentas y contraseñas normalmente se asignan a los usuarios individuales y no se deben compartir con ninguna otra persona sin la autorización del administrador del sistema correspondiente. Se asume que los usuarios son responsables de cualquier actividad realizada con sus cuentas del sistema de TI o publicada en sus páginas web personales.

5.8 Identificación personal. Cuando lo solicite un administrador de sistema u otra autoridad de la Universidad, los usuarios deben presentar una identificación válida.

5.9 Condiciones del acceso a los recursos de la Universidad. Hay circunstancias en las cuales el acceso de un usuario a los recursos de TI se puede desactivar o finalizar, o las expectativas de privacidad se pueden renunciar en el marco de las siguientes condiciones especiales.

5.9.1 Condiciones especiales. Las siguientes condiciones especiales para el acceso institucional a materiales de TI, sin el consentimiento del usuario, se aplicarían de conformidad con las medidas de protección del procedimiento especificadas en UNH.VI.F.4.4.

5.9.2 Diagnóstico. Cuando sea necesario identificar o diagnosticar problemas y vulnerabilidades de seguridad o de los sistemas, o preservar la integridad de los recursos de TI en cualquier otro respecto.

5.9.3 Por disposición de la ley. Cuando lo exijan las leyes federales, estatales, o locales o las disposiciones administrativas.

5.9.4 Motivos fundados. Cuando haya motivos fundados para creer que podría haber ocurrido una violación de la ley y el acceso y la inspección o supervisión podrían producir evidencia relacionada con la violación.

5.9.5 Actividades empresariales esenciales. Cuando dicho acceso a los recursos de TI sea necesario para llevar a cabo funciones empresariales esenciales de la Universidad.

5.9.6 Salud y seguridad. Cuando sea necesario para preservar la seguridad y la salud pública.

5.10 Proceso. Acorde con los procedimientos especificados en el OLPM con respecto al acceso institucional a materiales y registros sin el consentimiento del usuario, dicho acceso debe ser anotado por el administrador del sistema para revisión posterior por parte del vicepresidente correspondiente.

5.10.1 Desactivación del acceso del usuario. La Universidad, por medio del administrador del sistema correspondiente, puede desactivar los privilegios de tecnología de la información de un usuario, incluso en ausencia de una presunta violación de la PUA, cuando sea necesario para preservar la integridad de los recursos de TI. El administrador del sistema debe notificar por escrito al usuario de dicha medida en el plazo de 48 horas (UNH.VI.F.4.4).

5.10.2 Sistemas de control de seguridad. Al conectar computadoras de propiedad privada u otros recursos de TI a la red de la Universidad, los usuarios permiten el uso de programas de control de seguridad por parte de la Universidad mientras están conectados a la red.

5.10.3 Archivos de registro. La mayoría de los sistemas de TI habitualmente registran las acciones de los usuarios por diversas razones, entre las que se incluyen la recuperación del sistema, solución de problemas, reportes de uso y planificación de recursos. Se espera que todos los administradores de sistemas establezcan y publiquen una descripción de las políticas y procedimientos de conexión para los sistemas que administran. Puede consistir en una declaración de privacidad o una declaración de funcionamiento más general.

5.10.4 Material codificado criptográficamente. Los profesores y la plantilla de la Universidad, como empleados, pueden codificar archivos, documentos y mensajes para protegerlos contra la divulgación no autorizada durante el almacenamiento o el proceso de transmisión. Sin embargo, dicha codificación debe permitir que las autoridades, cuando se exija y autorice adecuadamente, decodifiquen la información (UNH.VI.F.4).

5.11 Procedimientos de Ejecución

5.11.1 Denuncias de presuntas violaciones. Un elemento importante en la sanción de violaciones a esta PUA es la intención, es decir, si una violación se llevó a cabo con conocimiento y a sabiendas de las consecuencias. En el caso de violaciones menores, lo que se espera es resolver la violación el nivel más bajo de administración del sistema involucrado. Se espera que los administradores de sistemas usen su propio criterio para reportar una violación para un proceso formal judicial o disciplinario. Se puede consultar al administrador de la PUA para que brinde asesoramiento interpretativo, como se describe a continuación. Visto como un diagrama simple:

Una persona que cree que fue perjudicada por una presunta violación a esta política puede presentar una queja de conformidad con los procedimientos de quejas y agravios establecidos de la Universidad. También se exhorta a la persona a reportar la presunta violación ante la autoridad de sistemas responsable y derivar el asunto a las autoridades disciplinarias de la Universidad.

5.11.2 Reporte de violaciones presenciadas. Si una persona ha presenciado o de algún otro modo tiene conocimiento de una presunta violación a la PUA, pero no ha sido perjudicado por la presunta violación, puede reportar el asunto a la autoridad de sistemas responsable del centro que esté involucrada más directamente y derivar el asunto a las autoridades disciplinarias de la Universidad.

5.11.3 Procedimientos disciplinarios. Cuando sea posible, el objetivo es resolver problemas de uso y de uso indebido informalmente entre el usuario y el administrador de sistema pertinente, inclusive el uso de procedimientos departamentales informales si fuera útil.

Las presuntas violaciones a esta política se investigarán de conformidad con los procedimientos disciplinarios correspondientes para estudiantes, profesores y empleados, como se describe en las normas para estudiantes pertinentes (por ejemplo los Derechos, Normas y Responsabilidades de los Estudiantes), el manual de los profesores, o el manual de los empleados. Los profesores o los empleados que sean miembros de unidades de negociación reconocidas por la Universidad están amparados por disposiciones disciplinarias establecidas en el acuerdo de sus unidades de negociación. Los factores a considerar en un presunto incidente son: su naturaleza, la intención, el grado del daño, y los antecedentes de delitos, para dar lugar a la medida recomendada.

Los administradores de sistemas pueden participar en procedimientos disciplinarios cuando la autoridad disciplinaria pertinente lo considere adecuado. Y, según las instrucciones de la autoridad disciplinaria correspondiente, los administradores de sistemas están autorizados a investigar presuntas violaciones.

5.11.4 Sanciones. Los usuarios que se determine que violaron esta PUA están sujetos a sanciones estipuladas en otras políticas de la Universidad que abordan la conducta básica. Dichos usuarios también pueden enfrentar sanciones específicas para TI, entre las que se incluyen reducción temporal o permanente o eliminación de algunos o todos los privilegios de TI. La autoridad disciplinaria pertinente determinará las sanciones oportunas en colaboración con el administrador del sistema.

Los administradores de sistemas que violen su autoridad también están sujetos a sanciones como se contempla en otras políticas de la Universidad.

5.11.5 Responsabilidad legal y uso ilegal. Además de la sanción de la Universidad, los usuarios puedan ser objeto de procesos criminal, responsabilidad civil, o ambos, por el uso ilegal de recursos de TI.

5.11.6 Apelaciones. Los usuarios que se detecte que violaron esta política pueden apelar o solicitar la reconsideración de cualquier medida disciplinaria impuesta de conformidad con las disposiciones de apelaciones formales de la autoridad disciplinaria pertinente.

5.12 Desarrollo de la política

5.12.1 Esta PUA se revisará y modificará periódicamente bajo la dirección del vicepresidente adjunto de Servicios de informática e información, en colaboración con los comités y los constituyentes. Este vicepresidente adjunto designará a un administrador de la PUA para ayudar con lo siguiente:

5.12.1.1 Interpretación. Para preguntas o para recibir ayuda con respecto a la interpretación de esta PUA, comuníquese con el administrador de la PUA.

5.12.2 Revisión. El administrador de la PUA revisará esta PUA para verificar su exactitud cuando sea necesario, pero no menos de una vez por año.

5.13 Contra referencias de la política. Los siguientes enlaces van a políticas y documentos en línea relacionados. Hay otras políticas y documentos importantes que todavía no están en línea.

5.13.1 Ley de Derechos de Autor de la Era Digital (Digital Millennium Copyright Act)

5.13.2 FAP sobre procedimiento de contribuciones benéficas y políticas 8-006 (FAP on Charitable and Political Contributions Procedure 8-006)

5.13.3 Confidencialidad de los datos estadísticos de la biblioteca (Library Records Confidentiality)

5.13.4 NH RSA 638:16,17,18. Estatutos estatales sobre delitos informáticos

5.13.5 OLPM sobre Lista de direcciones y directorios (UNH.III.B)

5.13.6 OLPM sobre Privacidad y seguridad de los recursos tecnológicos (UNH.VI.F.4)

5.13.7 Derechos, Normas y Responsabilidades de los Estudiantes. Consulte el Apéndice de la Ley de Derechos Educativos y Privacidad Familiar de 1974 (Family Educational Rights and Privacy Act of 1974), también llamada "La enmienda Buckley".

5.13.8 Manual sobre la Ley de Derechos de Autor y procedimientos relacionados de UNH (UNH Primer on Copyright Law and Recommended Procedures)

5.13.9 Declaración de privacidad de UNHINFO

Esta PUA se elaboró utilizando como modelo, con autorización, la política de uso apropiado de la Universidad de Yale y cumple con UNH.III E con respecto al desarrollo, revisión y aprobación de la política institucional.