Res. 074/01 CS UNPA – Reglamento para el manejo de software y hardware PSTI

Río Gallegos, 27 de abril de 2001

VISTO:

El Expediente N° 03042–R-01; y

CONSIDERANDO:

Que se encuentra en funcionamiento el Programa de Sistemas y Tecnologías de la Información – PSTI – ;

Que resulta necesario fijar las normas y procedimientos que aseguren la integridad y seguridad tanto del manejo de datos como de éstos propiamente dichos, como así también el buen uso del software, hardware, servicios y bienes de la organización que dependen del PSTI, con el fin de lograr el mejor aprovechamiento de los ítems antes mencionados a un bajo costo;

Que atento el riesgo que para el sistema implica el ingreso por parte de terceros al sistema de red de la UNPA, es necesario dejar establecido políticas claras de seguridad de sistema y de manejo de contraseñas, que brinden tanto seguridad para los usuarios como protección eficiente para los datos y archivos;

Que resulta necesario establecer las normas que garanticen la legitimidad y confiabilidad del software utilizado en la institución, en protección de los derechos de propiedad intelectual respectivos y de seguridad del sistema mismo;

Que a fin de agilizar y eficientizar las tareas de los distintos agentes de las Unidades de Gestión de la Universidad, resulta conveniente habilitar, mediante el uso de la red de las Unidades de Gestión, la información categorizada como de acceso publico, atento a su utilidad para los distintos sectores;

Que deben establecerse procedimientos seguros y centralizados de backup de todos los datos informatizados que existen en cada Unidad de Gestión;

Que el uso indiscriminado de los recursos de Internet y correo electrónico encierra un potencial problema en cuanto a la disponibilidad del recurso para su fin esencial;

Que a fin de optimizar el aprovechamiento de dichos recursos corresponde reglamentar el mismo, clarificar a los agentes su función, y limitarlo a aquellos casos justificados por razones de trabajo;

Que debe fijarse una clara política de compras de recursos informáticos, que sea adecuada a las necesidades de la institución y con el criterio de mejor aprovechamiento de los recursos disponibles atendiendo a las necesidades de cada área;

Que únicamente personal específicamente capacitado puede garantizar la ejecución de dicha política;

Que asimismo, debe ejercerse un control en la solicitud, compra y recepción de los productos informáticos adquiridos atento a las especificidades técnicas que ellos presentan y para garantizar su adecuación a lo requerido;

Que la Comisión de Presupuesto y Reglamentaciones recomienda en su despacho aprobar el reglamento en lo general, girar a las Unidades Académicas para su consulta y análisis y su puesta en marcha en carácter de prueba piloto;

Que puesto a votación se aprueba por unanimidad;

POR ELLO:

EL RECTOR DE LA

UNIVERSIDAD NACIONAL DE LA PATAGONIA AUSTRAL

R E S U E L V E :

ARTICULO 1º: APROBAR en lo general la reglamentación sobre manejo de software, hardware, servicios y bienes que dependen del PSTI y que como anexo forma parte de la presente.

ARTICULO 2°: GIRAR dicha reglamentación a las Unidades Académicas para su consulta y análisis y puesta en marcha en carácter de prueba piloto.

ARTICULO 3°: TOMEN RAZON Secretarías de Rectorado, Unidades Académicas, dése a publicidad y cumplido, ARCHÍVESE.

Adela Muñoz
Secretaria Consejo Superior

Ing. Héctor Anibal Billoni
Rector

REGLAMENTACION SOBRE MANEJO DE SOFTWARE, HARDWARE, SERVICIOS Y BIENES QUE DEPENDEN DEL PSTI

I. OBJETIVOS Y DESTINATARIOS

ARTICULO 1º: El presente reglamento tiene por objetivo establecer normas y procedimientos que tienden a asegurar la integridad y seguridad de datos, como del manejo de los mismos; el buen uso del software, hardware, y demás servicios y bienes que dependen del PSTI.

ARTICULO 2º: Todo usuario de tecnología informática de cada Unidad de Gestión de la UNPA deberá sujetarse al presente reglamento.

II. USO DE CONTRASEÑAS

ARTICULO 3º: Las contraseñas para acceso a los sistemas y redes de cada Unidad de Gestión son de uso personal, exclusivo, intransferible y confidencial.

Se prohíbe expresamente dar a conocer la contraseña a terceros. A los fines del presente artículo, entiéndase por tercero a toda persona distinta a la del usuario de la contraseña, sea este empleado de la UNPA o agente externo.

Contraseñas de mail: en los casos que el responsable de grupos o áreas de trabajo cuente con un único mail para esa área, dicho responsable podrá otorgar la clave de mail a sus subordinados, bajo su responsabilidad.

ARTICULO 4º: Las contraseñas sólo podrán ser instaladas con la autorización y conocimiento del Coordinador del PAM – Plan de Acción de Mantenimiento - e instaladas por personal de dicha área, a requerimiento fundado y avalado por el Secretario o jefe del área correspondiente, o el Rector y Decano en su caso.

ARTICULO 5º: El Coordinador del PAM otorgará las contraseñas de acuerdo a las reglas de seguridad propias del área, no pudiendo darla a conocer a terceros, ni aún a los superiores del agente, salvo en el cumplimiento de medidas disciplinarias, o para el cumplimiento de las funciones que se le atribuyen al PSTI por el presente, u otras causas debidamente justificadas.

ARTICULO 6º: No se deberá dejar logueada la máquina con su contraseña por periodos prolongados sin la supervisión del usuario, a fin de evitar problemas de seguridad de la información de la organización, y mala utilización del mail por parte de terceros.

ARTICULO 7º: El área de personal de cada Unidad de Gestión deberá notificar fehacientemente al coordinar del PAM respectivo de las bajas de personal, incluidos contratados y pasantes, y cambios de función con el objetivo de adecuar las claves, cuentas y permisos a las novedades producidas.

Manejo de Contraseñas por PAM

ARTICULO 8º: Las contraseñas administrativas de todos los servidores y equipos críticos de Unidades de Gestión UNPA se encontraran en sobre cerrado, junto con el procedimiento de apertura de las cajas fuertes ignífugas donde se encuentran todos los Backup de datos, de todas las locaciones y serán entregadas para su custodia al responsable del PAM.

III- LICENCIAS E INSTALACION DE SOFTWARE - HARDWARE

ARTICULO 9º: Todas las instalaciones de software, Sistemas Operativos, Aplicativos, Utilitarios, de Oficina, Técnicos o de cualquier índole deben ser realizadas por personal del PAM o con su conocimiento y autorización.

ARTICULO 10º: El Coordinador del PAM tendrá como obligación a su cargo la de supervisar que el software instalado posea la correspondiente licencia original de utilización y que de ninguna manera se afecten los derechos de propiedad intelectual. En caso de detectarse software instalado en violación a lo establecido en el presente, deberá procederse a su desinstalación, previo requerimiento al usuario del origen, licencia y utilización del software.

La instalación del software deberá ser solicitada fehacientemente, y autorizada por el superior inmediato, respetando en todo momento la legislación vigente, aún cuando la mencionada instalación sea solicitada por un periodo de tiempo restringido. En este último caso se deberá contar con la licencia respectiva o autorización expresa de la empresa desarrolladora.

ARTICULO 11º: Las computadoras, Impresoras, Plotters, Scanners, Servidores, y demás hardware provisto por la Unidad de Gestión UNPA son para uso exclusivo de los trabajos encomendados por el mismo y/o la realización de las funciones asignadas.

ARTICULO 12º: Solo el personal del PAM o bajo la supervisión o autorización del Coordinador del PAM, se puede desarmar, mudar o alterar la configuración del equipamiento informático. Queda autorizado el Coordinador del PAM para disponer la reubicación y distribución del equipamiento informático, software y servicios de acuerdo a las necesidades que se presenten y con el objetivo de permitir al personal de Unidad de Gestión cumplir sus tareas en forma eficiente y tender a la optimización de los recursos.

IV- RECURSOS DE RED

ARTICULO 13º: La utilización de la Red de cada Unidad de Gestión es solo para fines laborales y propios de la institución, quedando expresamente prohibido utilizar la misma para almacenar información personal.

ARTICULO 14º: Queda expresamente prohibido comunicar a terceros contraseñas del sistema de redes de la Unidad de Gestión.

ARTICULO 15º: Cada usuario dispondrá en la red de una carpeta personal o del área, identificada con su nombre de usuario. Esta carpeta es de acceso restringido al propietario de los datos, para almacenar información que considere critica e importante y que por razones de seguridad (resguardo y acceso) no puede ser almacenada en su PC. El tamaño máximo de información en megabytes en esta carpeta estará limitada. En caso de que la misma resultare insuficiente, se solicitará su aumento.

La integridad y resguardo de la información almacenada en la estación de trabajo del usuario es responsabilidad del mismo.

ARTICULO 16º: Todas las maquinas que acceden a la red de la Unidad de Gestión UNPA deberán ser previamente homologadas. No podrán conectarse a ella PC y/o Notebooks personales sin la correspondiente autorización fehaciente.

Acceso a los Datos

ARTICULO 17º: En la red del Unidad de Gestión UNPA existen datos públicos y privados, los públicos pueden ser leídos por toda la organización o por el área correspondiente y los privados solo por los usuarios de la Secretaría, Departamento y/o sector en cuestión.

De requerirse acceso temporal o permanente a datos que no pertenezcan a su sector o Secretaría se deberá tener autorización de la Secretaría requeriente y la aprobación de la Secretaría responsable de los datos. Dicha autorización será comunicada por escrito o vía mail al responsable del PAM.

El usuario que utiliza los recursos de la red de la Unidad de Gestión UNPA es responsable por la utilización de los datos que almacena tanto en los discos con acceso publico como en su estación de trabajo.

Ingreso a redes externas

ARTICULO 18º: No se podrá ingresar desde cualquier puesto de trabajo de la red de Unidades de Gestión UNPA a otra red ajena, tanto vía telefónica o vía cualquier otro medio de conexión, a no ser que cuente con la autorización del responsable del PAM. Queda excluido el acceso mediante los servicios de Internet.

V- CORREO ELECTRONICO

ARTICULO 19º: El correo electrónico puesto a disposición de los usuarios sólo puede ser utilizado con fines laborales y/o para el desarrollo de las actividades asignadas; quedando expresamente prohibido su utilización para fines personales, o para solicitar, promover, publicitar alguna organización, producto o servicio; o para difundir mensajes que contengan material ofensivo de cualquier tipo. Asimismo se deberá cumplir con la legislación vigente de propiedad intelectual, ya que el mail es un medio de difusión.

ARTICULO 20º: Las direcciones de mail y Web de la UNPA pertenecerán al dominio unpa.edu.ar y serán las únicas avaladas oficialmente. Cualquier dirección que no respete este dominio deberá considerarse no oficial. Estará prohibido publicitar o dar a conocer direcciones no oficiales como si pertenecieran a la UNPA.

ARTICULO 21º: No se permite enviar mail superiores a 2 MB. En caso de requerir una transferencia mayor a la indicada, deberá acordarse con personal del PAM la mejor alternativa para realizar la operación.

ARTICULO 22º: El espacio personal en la post-office del servidor de correo no podrá superar los 15 MB, pasado ese umbral no se podrá enviar ni recibir correo, para subsanar este inconveniente deberá depurar su casilla o pasar elementos a su carpeta personal.

ARTICULO 23º: No se podrá acceder al correo electrónico y al archivo personal de mensajes de otro empleado sin su expresa autorización.

ARTICULO 24º: El correo electrónico es un activo de la organización y está sujeto a revisión y/o control, por disposición del responsable del área y cuando existan causas justificadas.

VI- USO DE INTERNET

ARTICULO 25º: Solo podrá acceder a los distintos servicios de Internet el personal autorizado. La autorización será efectuada por el Secretario del área respectiva o el Rector o Vicerrector, en su caso, en consulta con el Coordinador del PSTI, a fin de que este considere sobre la disponibilidad técnica del recurso, y el mejor aprovechamiento del mismo. Los Secretarios de Unidad de Gestión sólo podrán autorizar el uso de Internet en función a la necesidad con fines laborales y cumplir con los roles y responsabilidades del puesto de trabajo o tareas encomendadas. Toda persona que no posea el permiso explícito para su utilización deberá ser justificado por escrito por el responsable del área.

ARTICULO 26º: El uso de Internet será auditado mensualmente por el PSTI con informes que se elevaran a la correspondiente Secretaría o jefatura, a los fines que éstas estimen corresponder.

ARTICULO 27º: Esta prohibido bajar software (Aplicativos, Utilitarios, etc.) de Internet sin la supervisión y/o autorización del personal del PAM.

VII- ADQUISICION DE EQUIPAMIENTO

ARTICULO 28º: Toda compra o adquisición a cualquier título de equipamiento, ya sea Software y/o Hardware, partes o servicios del área de informática, excluyendo los insumos deberá contar con el aval del Coordinador del PAM, quien se expedirá sobre los siguientes puntos:

1. Estándar, garantía y respaldo del producto;

2. La necesidad de la adquisición en base a los requerimientos laborales y los equipos, software y servicios existentes en Unidad de Gestión;

3. La adecuación a los pliegos ETAP – Estándares Tecnológicos para la Administración Pública- de la Secretaría de la Función Pública.

La recepción del equipamiento será controlada por PSTI y se realizará según las normas establecidas por el ETAP.

ARTICULO 29º: Las ordenes de compra serán controladas por personal del PAM a fin de verificar las especificaciones técnicas.

ARTICULO 30º: Efectuada la compra y recepcionado el producto, las actuaciones serán remitidas al PAM, junto con la totalidad de la documentación que avale la garantía de los equipamientos adquiridos, a fin de que este extraiga las copias pertinentes. El PAM deberá, en base a esta documentación, conformar un archivo que le permita llevar un control adecuado del equipamiento.

VIII. BACKUP, DISPOSITIVOS DE ALMACENAMIENTO MASIVO, CABLEADO DE DATOS.

ARTICULO 31º: Los dispositivos de almacenamiento masivo serán administrados por PSTI, para realizar backup y/o distribución de Información.

ARTICULO 32º: En caso de requerir un Backup en CD o en cualquier otro medio de almacenamiento para resguardar o retirar información de la organización solicitada por un empleado, este deberá contar con la autorización del responsable de dichos datos la que deberá ser comunicada por escrito o vía mail al PAM.

ARTICULO 33º: Las instalaciones de cableado de datos son responsabilidad del PAM.

ARTICULO 34º: Cualquier instalación, reparación o modificación que afecten cualquiera de los elementos antes mencionados deberán estar informados y aprobados por el PAM y supervisados por el personal de dicho sector.

ARTICULO 35º: Es responsabilidad del PAM la realización de los Backup diarios, semanales y mensuales, los que serán efectuados según las reglas propias de la informática. El PAM sólo es responsable del resguardo de la información almacenada en los servidores de Red.

ARTICULO 36º: Cada usuario tendrá a su disposición los dispositivos de backup de sistemas para resguardar su información cuando crea necesario.

En dicho momento se notificara al personal del PAM que realizará el mismo en un plazo no mayor a 5 días hábiles. Dicho resguardo quedará en poder del PAM, y para ser retirado el usuario deberá contar con la autorización del responsable del cual dependan dichos datos, la cual será remitida por escrito o vía mail al responsable del PAM.

IX. ENTRADA Y SALIDA DE EQUIPAMIENTO.

ARTICULO 37º: El equipamiento informático de Unidad de Gestión no podrá ser retirado de los edificios del mismo salvo en los casos en que exista expresa autorización dada por escrito suscripta por la autoridad directamente responsable del mismo o el Rector o Decano. El permiso deberá indicar expresamente si es con carácter permanente o con carácter temporario y en su caso hasta que fecha. Las autorizaciones otorgadas deberán ser comunicadas por el otorgante al Coordinador del PSTI para su debida nota y registro.

ARTICULO 38º: Esta prohibido el ingreso de cualquier elemento de Hardware, instaladores de software en cualquier tipo de medio magnético que sea propiedad personal del usuario, a no ser que cuente con expresa autorización de la autoridad responsable del área respectiva y del Coordinador del PAM. En ningún caso podrá otorgarse esta autorización sino se justificare en razones de servicio y se considere imprescindible.

X- PROTECTORES DE PANTALLA, FONDOS.

ARTICULO 39º: Solo se admite el uso de protectores y fondos de pantalla provistos por la instalación estándar de Windows o desarrollados a tal fin por el PAM.

Se prohibe expresamente solicitar, promover y/o publicitar organización, producto o servicio a través del medio en cuestión.

XI- SANCIONES

ARTICULO 40º: Se deja expresamente aclarado que la violación de cualquiera de las normas contenidas en la presente constituye una falta administrativa, sin perjuicio de la responsabilidad civil y/o penal derivada de cada caso en particular según su gravedad y consecuencias, en especial, la violación de las normas contenidas bajo el número II, atento a los riesgos que importa para la seguridad del sistema la inobservancia de la normativa referida a contraseñas.

ARTICULO 41º: Es obligación del Coordinador del PAM, poner en conocimiento del responsable del área respectiva todo hecho que llegue a su conocimiento y que importe una violación al presente, a fin de que el Responsable del área dé el curso que estime corresponder, conforme al régimen disciplinario vigente.

XII- NORMAS TRANSITORIAS

ARTICULO 42º: No encontrándose en la actualidad en pleno funcionamiento el sistema de redes, se establece como especial obligación del PAM realizar los procedimientos necesarios a fin de su puesta en funcionamiento y de acuerdo a las reglas establecidas por el presente.

ARTICULO 43º: A fin de determinar la información de la red de Unidades de Gestión que será de acceso público y de acceso privado, otorgar las claves de red, y demás aspectos necesarios para su correcto funcionamiento, el Coordinador del PAM deberá comunicarse con los Secretarios, jefes y demás responsables de las distintas áreas a fin de que le sea comunicado sobre las necesidades de seguridad y carácter público o privado de la información.

ARTICULO 44º: Encontrándose en la actualidad la mayoría de los agentes de Unidad de Gestión autorizados implícitamente al uso de Internet, a fin de dar operatividad a las reglas establecidas en el número VI, los Sres. Secretarios o jefes de cada Unidad de Gestión, el Rector y el Vicerrector, y los Decanos informarán dentro de los diez 10 de la fecha de la presente, sobre los agentes que dependan de su área que deben ser autorizados para el uso de dicho recurso. Remitidas dichas autorizaciones, el Coordinador del PAM procederá a realizar lo respectivo para proveer el mismo a dichos agentes, no pudiendo en lo futuro los agentes no comprendidos en la autorización utilizar el recurso.