MANUAL DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

UNIVERSIDAD NACIONAL DE MORENO

Mayo de 2014

Universidad Nacional de Moreno

MANUAL DE SEGURIDAD DE LA INFORMACIÓN[1]

OBJETIVO:

La finalidad de este MANUAL es establecer, en la UNM, los lineamientos generales que garanticen calidad, confiabilidad y confidencialidad en los servicios relacionados con las TICs.
Estos lineamientos deberán ser contemplados en las tareas de organización, administración y operación de los datos de la UNIVERSIDAD, así como en sus soportes tecnológicos, de modo de minimizar en lo posible los riesgos asociados al trabajo con las TICs.
Con el espíritu de acompañar el cumplimiento de los objetivos institucionales, este documento estará sujeto a revisiones periódicas, incorporación de mejoras y ajustes de las políticas definidas, según la organización lo determine necesario y la evaluación que se realice de las mismas, contemplando además las sugerencias que sean recibidas de las distintas áreas de la UNM.

ALCANCE:

Este MANUAL está dirigido al personal administrativo, docente, consultores y personal técnico externo que presten servicios en la UNIVERSIDAD, en sus dependencias centralizadas o descentralizadas, o intervenga en organizaciones y eventos relacionados con el Organismo y que cuente con acceso a los recursos tecnológicos de la UNM.
Todos los servicios informáticos utilizados por la UNM, ya sea en sus dependencias centralizadas o descentralizadas, están soportados sobre la infraestructura tecnológica de la universidad, administrada por la SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (STIC), cuya Responsabilidad Primaria y Funciones han sido establecidas en la Resolución UNM-R Nº 479/12 y sus modificatorias.

RESPONSABILIDADES:

Es responsabilidad de la STIC, con aprobación de las autoridades de la UNIVERSIDAD, la creación, actualización e implementación de las políticas de seguridad definidas.
Del mismo modo, es responsabilidad de la STIC, la difusión de estos lineamientos al personal de la UNM, de modo que sean contemplados en el manejo que realizan sobre los datos y en el uso de los bienes informáticos (hardware y software) de que disponen para la realización de sus actividades.
En relación a las herramientas tecnológicas de la UNIVERSIDAD, son responsables todos sus funcionarios de su exclusiva utilización con fines académicos, de investigación, extensión, vinculación o servicios, y toda otra función autorizada por el órgano rector de la UNM que corresponda.
Toda persona que, con la autorización adecuada, utilice los servicios informáticos en la UNM (equipos, mail, acceso a sistemas, etc.), deberá cumplir y respetar las pautas definidas en este MANUAL.

Administración de la Infraestructura Tecnológica
Es responsabilidad de la STIC implementar los mecanismos que habiliten el buen funcionamiento de la red, servidores, software de base (sistemas operativos, bases de datos) y sistemas de información que se encuentran instalados y operativos en la UNM.
Asimismo, es su responsabilidad proteger la información almacenada en la infraestructura tecnológica de la UNM, así como la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna

[1] Aprobado por Resolución UNM-R Nº 197/14

institucional como a dependencias o redes externas como Internet.
Para ello, la SUBSECRETARÍA debe:

- Implementar monitoreos que permitan minimizar y prever, en lo posible, los eventos que pudieren ocasionar bajas en los niveles de servicio necesarios para cada sistema, o su interrupción temporaria.
- Diseñar, implementar y documentar procedimientos de resguardo de la información, los sistemas de gestión y su documentación.
- Diseñar, implementar y documentar procedimientos de recuperación de los mismos en caso de fallas.

Al respecto, colaborará cada una de las áreas, en la formulación y aprobación de un PLAN DE CONTINGENCIAS que documente las operaciones a realizar y los aspectos técnicos a considerar en casos de caída de servicios en cada una de ellas, de acuerdo a sus responsabilidades y actividades y las del responsable informático del área, en caso de haberse previsto.
Asimismo, deberá contemplar buenas prácticas de administración, como el aviso a los usuarios de los equipos y sistemas previo a la realización de una tarea de mantenimiento que interfiera en el funcionamiento de alguna herramienta informática (por ejemplo, reiniciar un servidor o servicio, poner un sistema fuera de línea, etc.).

1) RECURSOS DE RED

La STIC debe controlar el acceso a los servicios de red, tanto internos como externos, para evitar que conexiones no seguras o el uso excesivo de los recursos afecten a toda la UNIVERSIDAD y, así, garantizar que los usuarios tengan el acceso que requieren a los servicios, sin comprometer la seguridad de los mismos.
La STIC sólo puede brindar acceso a los recursos de red, siguiendo el procedimiento detallado en el presente MANUAL, mediante autorización formal de la autoridad competente.

2) SERVIDORES Y SOFTWARE DE BASE

La STIC debe implementar las medidas y los estándares técnicos necesarios para controlar el acceso a los equipos instalados en el centro de cómputos y al software de base (sistemas operativos y bases de datos). Deberá realizar monitoreos de estos accesos y del uso de los sistemas por parte de los usuarios.
Respecto a la integridad del equipamiento, el software y la información allí almacenada, los PLANES DE CONTINGENCIA que se aprueben documentarán en forma detallada los recaudos a seguir y las acciones a tomar en caso de falla, según corresponda en cada caso.

3) ANTIVIRUS

Se considera un virus informático todo aquel software malicioso que amenace al sistema informático, infiltrándose a través de correos electrónicos, archivos adjuntos o con la sola acción de navegar la Internet.
La STIC, es la responsable de tomar las medidas de prevención y cuidar de la totalidad de la infraestructura informática de ataques provenientes de software pernicioso, mitigado en lo posible los efectos dañinos de este tipo de software.
Para ellos, la STIC deberá instalar, en todas las estaciones de trabajo y servidores de la UNM, un agente de antivirus que renueve su base de registro de virus en forma constante y segura.
Como medida adicional, deberá implementar los mecanismos necesarios, tendientes a evitar los ataques con virus del tipo troyano, por ejemplo, filtrando los archivos que envían o reciben por el correo electrónico de la UNM.

Control de Acceso a la Información:

1) ADMINISTRACIÓN DE USUARIOS

Todo personal de la UNM que necesite disponer de herramientas o servicios informáticos, debe ser inicialmente autorizado por medio del FORMULARIO aprobado a tal fin, el cual, deberá estar firmado por la máxima autoridad del área (con rango no menor a SECRETARIO o la máxima autoridad de nivel equivalente).
Este FORMULARIO deberá ser entregado a la STIC, que asignará los elementos (hardware, usuario de red, mail institucional y accesos a los sistemas de información de la UNIVERSIDAD), según lo determine dicho responsable.
Si se necesitara posteriormente modificar (ampliar o reducir) los accesos ya otorgados, se utilizará el mismo procedimiento de alta de usuario: confección del FORMULARIO, autorización por parte de un superior y entrega a la SUBSECRETARÍA.
En caso de retiro de un funcionario, es responsabilidad de las autoridades informar a la STIC sobre la anulación y cancelación de los derechos otorgados como usuario informático de la UNM.
Los funcionarios de la STIC no pueden realizar actividad alguna que vulnere la seguridad de accesos a la información y a los sistemas, y deberán tomar los recaudos necesarios para la detección de accesos no autorizados a las aplicaciones que utilizan los usuarios (registros de auditoría, logs, eventos, etc.).

2) CONTRASEÑAS

Para acceder a la red, los sistemas de información y correo electrónico de la UNM, la STIC debe facilitar a los usuarios contraseñas iniciales, que serán obligatoriamente cambiadas por los usuarios durante el primer intento de conexión al sistema.
Cualquier requerimiento posterior a la STIC de cambio de claves se deberá realizar previa identificación del titular de la cuenta y sólo al titular se facilitará dicha contraseña.

3) RESPONSABILIDADES DEL USUARIO

En forma adicional a las acciones que están bajo la responsabilidad de la STIC, en lo que hace a la seguridad de accesos, los usuarios deben cuidar aspectos de seguridad que están bajo su compromiso:

- No usar accesos a los datos y los servicios informáticos para fines no vinculados a actividades ajenas a las que realiza para la UNM.
- Cambiar las contraseñas provisorias en el primer inicio de sesión.
- No revelar las contraseñas asignadas o permitir que un tercero utilice sus claves para acceder a la red o a los sistemas; y denunciar y pedir su cambio, si sospecha que existe algún tipo de riesgo: pérdida, robo, etc.
- Ingresar contraseñas que sean fáciles de recordar, que no estén basadas en algún dato que otra persona pueda obtener fácilmente (iniciales, nombres, fecha de nacimiento, números de teléfono, etc.), o que sean caracteres iguales o consecutivos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar contraseñas anteriores.
- No guardar contraseñas en archivos o formularios en los que haya ingresado alguna vez.
- Concluir las sesiones activas al finalizar las tareas en los casos en que no puedan ser protegidos por un mecanismo de bloqueo adecuado como un protector de pantalla resguardado por contraseña.

Seguridad Medioambiental:

1) SEGURIDAD EN EL CENTRO DE CÓMPUTOS

El CENTRO DE CÓMPUTOS de la UNM es un área restringida, por lo que solo el personal autorizado por la STIC puede acceder a este ámbito.
Cuando un funcionario no autorizado o un visitante requieran ingresar a la sala de servidores, debe contar con autorización de una autoridad competente: SUBSECRETARÍA, SECRETARIO o máxima autoridad superior equivalente.
Para autorizar a un visitante externo a realizar tareas contratadas por la UNIVERSIDAD en dicho ámbito, se deberá solicitar autorización con anterioridad de igual manera, especificándose el tipo de actividad a realizar y tiempos de la estadía. En el momento de ingresar al CENTRO deberá contar en todo momento con la presencia de un agente de la STIC.
La STIC deberá solicitar a las autoridades de la UNM los elementos de protección de las instalaciones que crea necesarias para casos de catástrofes: prevención de incendios, inundaciones, sistema eléctrico de respaldo, UPS, etc..

2) EQUIPAMIENTO DE OFICINA

El DEPARTAMENTO DE INFRAESTRUCTURA TECNOLÓGICA de la STIC presta servicios a los usuarios de la tecnología en lo que hace a la instalación, configuración y mantenimiento del equipamiento de oficina, incluyendo computadoras, periféricos y el software necesario para la realización de las actividades en la UNIVERSIDAD.
Es responsabilidad de esta área, además, realizar el mantenimiento preventivo de la infraestructura ofimática.

3) RESPONSABILIDADES DEL USUARIO

Los usuarios de los servicios informáticos en el UNM no podrán extraer información almacenada en las computadoras que tenga asignadas para ser utilizada en funciones ajenas a la UNIVERSIDAD.
Cada funcionario tiene la obligación primera en el uso y custodia del equipamiento, estaciones de trabajo, servidores de archivos, periféricos o accesorios que se encuentren instalados en su área y bajo su responsabilidad, aun cuando no se esté utilizando o no contenga información relevante. Es responsable de su protección en lo que hace a robos, extravíos o pérdidas de los mismos. En caso de ocurrir un evento de esta naturaleza deberán los usuarios informarlo de manera inmediata a la STIC.
Los usuarios no deben abrir, destapar o reubicar el equipamiento informático, ni retirar sellos de seguridad, instalar o desinstalar software, sin la autorización de la STIC; en caso de requerir este servicio deberá solicitarlo a esta SUBSECRETARÍA.
Cuando se requieran cambios múltiples de equipamiento derivados de reubicación de lugares físicos de trabajo, deberán ser notificados a la STIC con los días de anticipación necesarios para lleva a cabo esta tarea.
Los usuarios de los sistemas en la UNM, no deberán introducir software pernicioso en la red o en los servidores sobre los cuales trabaja; asimismo no deberán instalar software sin la licencia de uso adecuada.
Deberán reportar de forma inmediata a la STIC cuando se detecte algún riesgo real o potencial sobre equipos informáticos o de comunicaciones, tales como derrames de agua, choques eléctricos, caídas, golpes o peligros de incendio.
El funcionario que tenga permitido el uso de dispositivos extraíbles de almacenamiento externo (Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos) será responsable del buen uso de ellos

El préstamo de equipos portátiles deberá ser solicitado a la STIC con la autorización por escrito de la SECRETARÍA GENERAL de la UNIVERSIDAD o autoridad superior.

4) CAPACITACIÓN

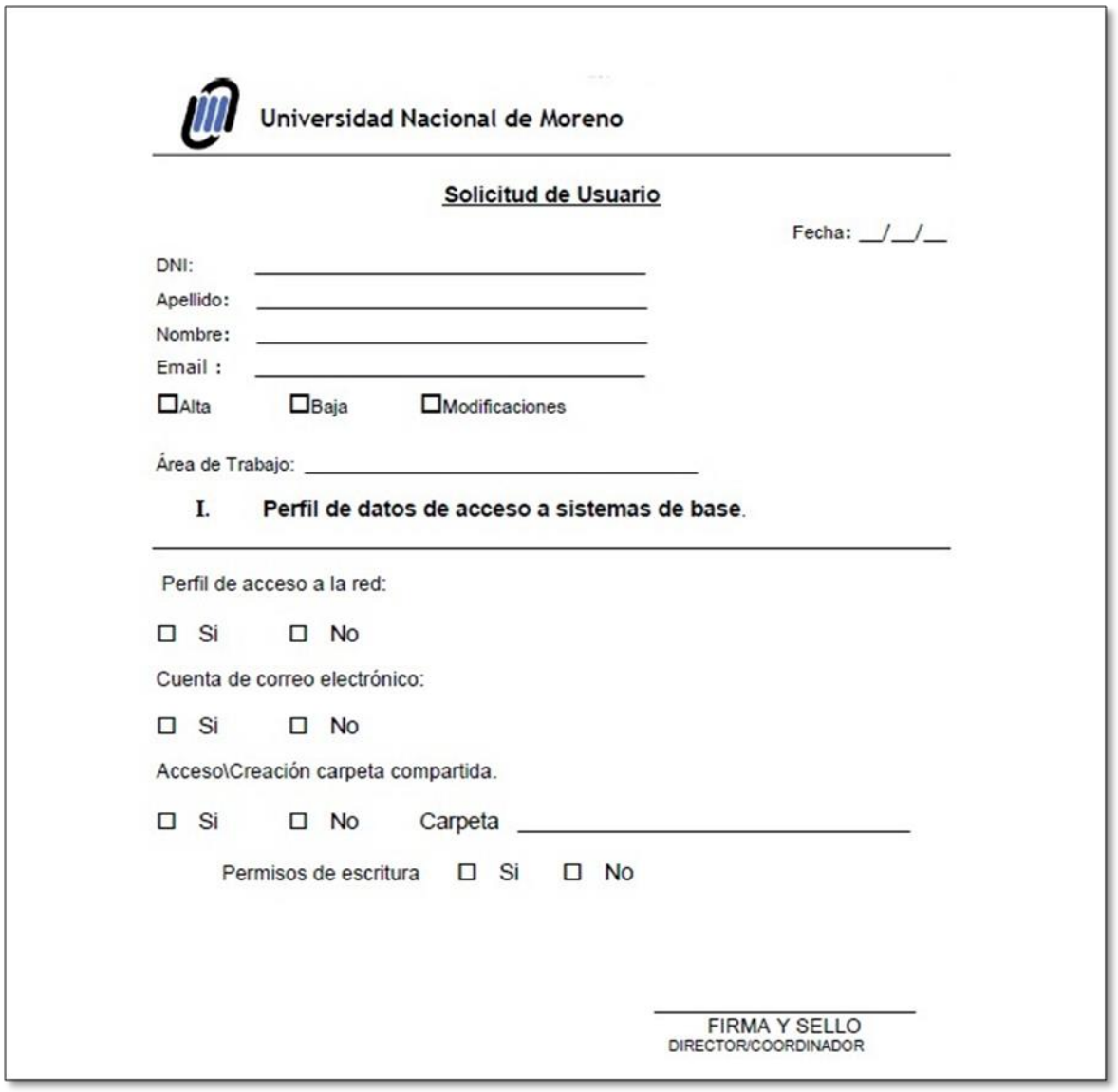
La STIC debe brindar, gestionar o sugerir la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en los equipos de oficina, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
Es responsabilidad del usuario solicitar a la STIC o la DIRECCIÓN GENERAL DE RECURSOS HUMANOS, la capacitación que necesite sobre todas las herramientas informáticas que se utilizan en su oficina, la cual se incorporará al PLAN ANUAL DE CAPACITACIÓN de cada año.
La STIC, por su parte, pone a disposición de los usuarios, instructivos varios destinados a ayudar a los usuarios en el manejo de distintas herramientas: INSTRUCTIVO CAMBIO DE CLAVE CORREO INSTITUCIONAL UNM, INSTRUCTIVO UTILIZACIÓN DEL CORREO ELECTRÓNICO, etc..

5) REGISTRO DE ACTIVOS

Es responsabilidad de la DIVISIÓN DE REGISTRO PATRIMONIAL, dependiente de la SECRETARÍA DE ADMINISTRACIÓN, mantener un registro actualizado de los bienes informáticos de la UNIVERSIDAD.
Esta área recibe los bienes adquiridos directamente del proveedor y lo registra en el inventario institucional como stock perteneciente a la STIC.
En caso de que este equipamiento deba ser entregado a otra área de la UNM, la STIC le informa del traspaso a la DIVISIÓN, vía correo electrónico. La DIVISIÓN rectifica la trasferencia en esa área y deja constancia del cambio en el registro correspondiente.

Uso del Correo Electrónico:
El personal de la STIC que, por su trabajo, administra y tiene acceso a las casillas de correo electrónico está obligado a mantener secreto y confidencialidad respecto del contenido de los correos.
Paralelamente, deberá garantizar que no pueda falsificarse, esconderse, suprimirse o sustituirse la identidad de un usuario de correo electrónico de la UNM.
Al igual que para acceso a la red y a los sistemas de información UNM, se facilitarán contraseñas iniciales para el ingreso al correo electrónico. Será obligatorio cambiar estas claves por parte del usuario durante el primer intento de conexión al correo. Cualquier requerimiento posterior a la STIC de cambio de claves se realizará previa identificación del titular de la cuenta y sólo a este titular se le podrá facilitar la contraseña requerida.
Por su parte, los usuarios del correo no deben usar cuentas asignadas a otras personas, ni recibir mensajes en cuentas de otros usuarios. En caso de que fuera necesario leer el acceder de otra persona, el usuario ausente debe autorizarlo y la STIC podrá re-direccionar los correos que llegan a esa dirección a otra dirección autorizada.
Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vaya destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.

Formulario Alta de Usuario



Universidad Nacional de Moreno

Solicitud de Usuario

Fecha: __/__/__

DNI: _____

Apellido: _____

Nombre: _____

Email : _____

☐Alta ☐Baja ☐Modificaciones

Área de Trabajo: _____

I. Perfil de datos de acceso a sistemas de base.

Perfil de acceso a la red:

☐ Si ☐ No

Cuenta de correo electrónico:

☐ Si ☐ No

Acceso\Creación carpeta compartida.

☐ Si ☐ No Carpeta _____

Permisos de escritura ☐ Si ☐ No

_____

FIRMA Y SELLO

DIRECTOR/COORDINADOR

GLOSARIO:

UNM: UNIVERSIDAD NACIONAL DE MORENO
TICs: TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
STIC: SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN de la UNM
Usuario: Toda persona que utilice algún servicio o herramienta relacionados con las TICs en la UNM.