



UNIVERSIDAD TÉCNICA DE MACHALA

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE MACHALA

1. INTRODUCCIÓN

La Universidad Técnica de Machala ha crecido notablemente en el área tecnológica, convirtiéndose en una herramienta imprescindible para el desempeño de la gestión institucional, debiendo cumplir estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

Conscientes de esta necesidad es preciso establecer lineamientos generales de seguridad a los que se debe sujetar la comunidad universitaria a fin de procesar la información de manera confiable, así como también el uso correcto de los equipos informáticos.

La Dirección de Tecnologías de la Información y Comunicación tiene como función la de apoyar a la Universidad Técnica de Machala en la realización eficiente de sus labores y servicios a través de procedimientos especializados en tecnologías de información y comunicación, buscando siempre las mejores prácticas. Es por ello que propone el presente documento a fin de implantar las normas de seguridad de la información a las que se deberá sujetar la UTMACH

2. OBJETIVO

Establecer el ámbito operacional, para la seguridad de la información en la Universidad Técnica de Machala, definiendo los mecanismos y controles para asegurar su confidencialidad, integridad y disponibilidad.

3. ALCANCE

La Universidad Técnica de Machala emite la presente política de seguridad de la Información, a fin de gestionar adecuadamente la seguridad de información en los siguientes aspectos:

- Aplicaciones informáticas
- Control de software malicioso
- Acceso a internet
- Correo electrónico
- Equipos Informáticos
- Gestión de contraseña de usuarios
- Copias de respaldo
- Acuerdo de confidencialidad

Esta política de seguridad será para aplicación de toda la comunidad universitaria: docentes, empleados y estudiantes.



UNIVERSIDAD TÉCNICA DE MACHALA

4. TERMINOS Y DEFINICIONES

Información: Grupo de datos supervisados y ordenados los cuales se constituyen en el activo más importante de la Universidad Técnica de Machala.

Confidencialidad: Garantizar que la información sea accesible sólo por el personal autorizado.

Integridad: Propiedad que busca mantener la información libre de modificaciones no autorizadas.

Disponibilidad: Garantizar que la información se encuentra siempre a disposición de quienes deben acceder a ella.

Usuario: Persona que utiliza un computador, programa, servicio o cualquier sistema informático y accede de la información.

TIC: Tecnología de la información y comunicación

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1 Aplicaciones Informáticas

El uso adecuado de las aplicaciones informáticas que la Universidad Técnica de Machala pone a disposición de los servidores estará dado por los siguientes lineamientos:

- a) La Dirección de Tecnología de la Información y Comunicación tiene la responsabilidad de desarrollar aplicaciones informáticas acorde a las necesidades de automatización de procesos para cada Departamento y Unidad Académica.
- b) La instalación de cualquier software en las computadoras de uso académico y administrativo de la UTMACH es responsabilidad de la Dirección de TIC, y por lo tanto son los únicos a realizar esta tarea.
- c) El acceso a los sistemas informáticos es restringido dependiendo de los roles y perfiles de cada funcionario.
- d) La autorización para el acceso a los sistemas informáticos debe ser proporcionada por la Dirección de TIC previo una solicitud escrita emitida por el Jefe de cada Departamento o Unidad Académica.
- e) Cuando un usuario cambia de funciones o deja la institución, es responsabilidad de la autoridad del Departamento o Unidad Académica y de la Dirección de Talento Humano dar a conocer a la Dirección de TIC a fin de que se bloquee el acceso.
- f) Cuando un usuario deja de laborar en la UTMACH es su responsabilidad dejar en el computador personal toda la información generada durante su tiempo de trabajo en la institución, debiendo el Jefe inmediato retirar al servidor del equipo de forma inmediata, procediendo a su recepción.

5.2 Control de Software malicioso

Todo software malicioso también conocido como *malware*, término que incluye a virus, gusanos, software espía y troyanos que pueden afectar la seguridad e integridad de la información, ante tal



UNIVERSIDAD TÉCNICA DE MACHALA

situación la UTMACH establece que todos los recursos informáticos deben estar protegidos mediante equipos y suites de seguridad.

Para la protección de los sistemas se establece que:

- a) La Dirección de TIC debe autorizar el uso de las herramientas y asegurar que el software de seguridad sea actualizado permanentemente y que no sea deshabilitado bajo ninguna circunstancia.
- b) Es responsabilidad del usuario revisar a fin de comprobar que su equipo de computación cuenta con el software antivirus actualizado, en caso contrario deberá solicitar a la Dirección de TIC su inmediata instalación o actualización.
- c) En caso de notar un comportamiento inusual en su computador, el usuario debe cerrar la aplicación que esté usando, apagar el equipo y comunicar inmediatamente a la Dirección de TIC.
- d) No está permitido:
 - Introducir en los computadores personales cualquier tipo de medio de almacenamiento sin que previamente haya sido revisado a través de un software antivirus.
 - Conectar en la red de la UTMACH cualquier equipo de computación sin la autorización de la Dirección de TIC.
 - Desinstalar y/o desactivar el software y herramientas de seguridad instaladas previamente por la Dirección de TIC.
 - Introducir código de programación que afecte al normal funcionamiento del software o equipos informáticos.
 - Guardar en los dispositivos de almacenamiento de los equipos computaciones de escritorio y laptop cualquier tipo de información de la cual no se conozca su origen que pueda ocasionar daños.
 - Abrir o reenviar mensajes de correo electrónico de procedencia desconocida que no garantice la seguridad.
 - Descargar anexos recibidos a través de correo electrónico que no se conozca la fuente.

5.3 Acceso a Internet

El internet se ha convertido en una herramienta de trabajo, de la que se requiere alta disponibilidad y debido a que su acceso puede abarcar sitios no necesariamente acorde al ámbito laboral, es necesario supervisar su navegación a fin de evitar riesgos ocasionados por su inadecuada utilización, por lo cual se debe considerar que:

- a) Es responsabilidad de la Dirección de TIC implementar las herramientas necesarias a fin de llevar un control de la navegación y páginas visitadas por parte de la comunidad universitaria, así como también las actividades y tiempos de acceso a cada una.

+



UNIVERSIDAD TÉCNICA DE MACHALA

- b) Los usuarios de la red de la UTMACH tienen la responsabilidad de dar un uso adecuado a este recurso y por ningún motivo realizar prácticas, pruebas o accesos indebidos que afecten la seguridad de la información tanto interna como externa.
- c) El uso de este recurso es exclusivamente para asuntos relacionados con las actividades institucionales.
- d) En caso de requerir el acceso a un sitio bloqueado el jefe de la unidad debe solicitar la autorización de la máxima autoridad y enviarla a la Dirección de TIC.
- e) No está permitido:
 - La navegación por sitios de internet relacionados con temas de: pornografía, alcohol, drogas, religión, compras, diversión, entretenimiento y en general cualquier página cuyo contenido vaya en contra de la ética, moral y ajena por completo a las funciones de cada usuario.
 - En la red administrativa el acceso a redes sociales y de mensajería instantánea y otros que tenga como objetivo formar foros o grupos para compartir información ajena a las funciones institucionales.
 - La entrega a terceros o difusión de información de propiedad de la UTMACH.
 - La descarga o uso en línea de: juegos, música, películas, videos, software de libre distribución y en general cualquier archivo ejecutable que atente contra la integridad, disponibilidad y confidencialidad de la información e infraestructura tecnológica de la UTMACH.
 - La conexión a internet a través de otro medio que no sea el autorizado o instalado por la Dirección de TIC.

5.4 Correo electrónico

Los docentes, empleados y estudiantes de la UTMACH, a quienes la Dirección de TIC ha proporcionado una cuenta de correo institucional deberán seguir los siguientes lineamientos:

- a) El Departamento de TIC por ningún concepto solicita claves de acceso a través de correos electrónicos.
- b) Es obligación de los servidores universitarios: docentes y empleados, utilizar la cuenta de correo institucional para el envío y recepción de mensajes, información y archivos, relacionados con procesos internos y externos de acuerdo a las funciones asignadas a cada uno por la UTMACH.
- c) En caso de requerir una cuenta de correo institucional para un Departamento o Unidad Académica, el responsable de la Unidad debe solicitar su creación a la Dirección de TIC.
- d) El envío de información corporativa hacia cualquier persona u organización se debe realizar a través de la cuenta de correo institucional
- e) Siendo el correo institucional un medio de comunicación, es obligatorio que todos los usuarios revisen diariamente la bandeja de entrada a fin de que puedan dar inmediata atención a lo solicitado.
- f) La correcta administración del correo institucional es de responsabilidad exclusiva de cada usuario y debe mantener solo la información relacionada a sus funciones.
- g) No está permitido:

fs



UNIVERSIDAD TÉCNICA DE MACHALA

- El envío de correos masivos para asuntos de índole personal, religioso, político, racista, sexista, pornográfico o cualquier otro tipo de mensajes que atenten contra el normal desempeño del servicio de correo institucional.
- Utilizar la dirección de correo institucional, como contacto en las redes sociales.
- Enviar archivos de música o videos, sin previo visto bueno de la Dirección de TIC
- Abrir, enviar ni reenviar correos no deseados conocidos como *spam*.
- Contestar correos que soliciten información personal, usuarios ni contraseñas.

5.5 Equipos informáticos

La Universidad Técnica de Machala ha otorgado al personal docente y administrativo computadores de escritorio y portátiles, así como otros equipos informáticos para el desenvolvimiento de las actividades académico – administrativas. De ahí la necesidad de que el servidor universitario cumpla con ciertas normas a fin de dar un buen uso a dichos bienes con el fin de proteger la integridad física de los equipos así como también su información, debe cumplir con lo siguiente:

- a) Cuando un Departamento o Unidad Académica requiera de un equipo informático, debe gestionar su compra previo informe técnico de la Dirección de TIC.
- b) El Departamento de Bodega debe notificar a la Dirección de TIC el ingreso de todo equipo informático, a fin de mantener actualizado el inventario. De igual manera debe comunicar los equipos que se den de baja.
- c) El computador de escritorio o portátil es para uso exclusivo de las actividades institucionales acorde a la función que desempeña cada servidor en el horario establecido para su puesto.
- d) Una vez terminada la jornada de trabajo, el funcionario deberá apagar los equipos y de ser el caso, guardarlos con las seguridades necesarias a fin de evitar su pérdida o daño. Es el responsable del bien.
- e) En caso de presentar algún problema el computador, el funcionario deberá solicitar ayuda a través del Sistema Help-Desk y dependiendo de la ubicación de la oficina se escalará al técnico de Administración Central o la Unidad Académica correspondiente.
- f) En caso de fallas o mal funcionamiento de un equipo en garantía, el usuario debe solicitar un informe técnico a la Dirección de TIC y remitir junto con el equipo a Bodega para su descargo.
- g) Con el propósito de precautelar la información guardada en los computadores, el usuario podrá asignar una contraseña para el encendido y protector de pantalla, la misma que debe darla a conocer a su jefe inmediato quien la mantendrá en reserva para ser utilizada solo en caso de emergencia institucional.
- h) El funcionario a cargo del computador es el dueño de los datos almacenados y por lo tanto tiene la responsabilidad de efectuar los respaldos correspondientes con el propósito de garantizar la continuidad de los procesos.



UNIVERSIDAD TÉCNICA DE MACHALA

- i) Todas las estaciones de trabajo deberán usar fondo de escritorio y protector de pantalla institucional el mismo que se activará después de diez minutos de inactividad.
- j) El software instalado en los computadores deberá ser el estrictamente necesario para llevar a cabo las funciones de cada usuario.
- k) Cuando por alguna necesidad el funcionario se retire de su puesto de trabajo debe dejar bloqueado su computador a fin de evitar que personas ajenas a sus funciones ingresen a la información.
- l) El funcionario a cargo de un computador portátil cuando se ausente temporalmente de la institución por vacaciones, enfermedad o asuntos personales; deberá entregar el equipo a su jefe inmediato para su custodia.
- m) Solo personal autorizado puede realizar administración remota a equipos tecnológicos de la UTMACH.
- n) No está permitido:
 - Hacer cambios en la configuración del computador u otro equipo informático, así como tampoco pueden agregar o quitar partes físicas internas, sin el visto bueno de la Dirección de TIC.
 - Instalar o desinstalar software o componentes de software, configurar o des configurar servicios o en general cualquier otro cambio que afecte a las propiedades iniciales del equipo. En caso de ser necesario realizar cambio, éstos deben hacerse en coordinación con el Departamento de TIC.
 - La instalación de programas que traten de evadir las medidas de seguridad u otros aplicativos de entretenimiento o de uso personal, que nada tengan que ver con el desenvolvimiento institucional.
 - Conectar a la red de la UTMACH equipos informáticos sin previo visto bueno de la Dirección de TIC.

5.6 Gestión de contraseña de usuarios

El acceso a las aplicaciones informáticas y correo institucional es a través de un Login (usuario) y Password (contraseña) cuya confidencialidad es de responsabilidad exclusiva de los usuarios: docentes, empleados y estudiantes de la UTMACH, para lo cual:

- a) El usuario debe asegurarse de ingresar su contraseña cuando esté seguro de que no es observado por otra persona.
- b) Se recomienda actualizar periódicamente la contraseña y de manera inmediata cuando sospeche que ha sido vulnerada su seguridad.
- c) En caso de olvido o no poder hacer el cambio de su contraseña deberá acercarse personalmente a la Dirección de TIC y solicitar su reseteo. Si el usuario es un estudiante deberá escoger la opción *Olvidó su contraseña?*
- d) No está permitido:
 - Dar a conocer a terceras personas su contraseña, en caso de hacerlo, es de su absoluta responsabilidad todo lo actuado con dicha clave.



UNIVERSIDAD TÉCNICA DE MACHALA

- Escribir la contraseña y dejar el documento en un lugar visible: escritorio, monitor, bajo el teclado, etc.
- Guardar la contraseña en un celular, Tablet o computador.
- Usar contraseñas que resulten obvias y que sean fácil descubrir como: nombre personal, fecha de nacimiento, año actual, número de cédula, número de teléfono, etc. Para evitar que la contraseña sea quebrantada debe regirse al estándar establecido para la creación de claves y debe tener:
 - i. Mínimo 9 y máximo 15 caracteres
 - ii. Por lo menos una letra mayúscula
 - iii. Por lo menos una letra minúscula
 - iv. Por lo menos un número
 - v. Un carácter especial: \$. #. _ *

5.7 Copias de respaldo.

La Información es un activo que la Universidad Técnica de Machala debe proteger adecuadamente, por lo tanto es responsabilidad de la Dirección de TIC:


- a) Establecer los mecanismos adecuados a fin de obtener y mantener los respaldos de toda la información generada por los usuarios a través de las aplicaciones, así como también de la base de datos alojadas en los servidores garantizando la confiabilidad, seguridad e integridad de la información.
- b) Implantar procedimientos para un rápido y eficiente acceso a la información resguardada.
- c) Definir los medios de almacenamiento que contendrá la información, así como el lugar externo, donde se va resguardar tomando en consideración su ambiente, espacio y seguridad física.

5.8 Acuerdo de confidencialidad.

Todos los funcionarios de la Universidad Técnica de Machala y las personas que temporalmente realizan actividades en la institución deben aceptar y firmar un Acuerdo de Confidencialidad en donde refleje el compromiso de respetar, proteger y dar el uso correcto a la información, servicios y recursos tecnológicos que provee la UTMACH.

Dra. Leonor Illescas Zea, Esp.
Secretaria General de la Universidad Técnica de Machala
CERTIFICA:

Que, la presente **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE MACHALA** fue aprobada por Consejo Universitario en sesión ordinaria celebrada en enero 15 del 2015.


Dra. Leonor Illescas Zea, Esp.
Secretaria General UTMACH

Jessy