Amozoc de Mota, Puebla a 3 de marzo de 2026
CIRCULAR NO. SPLAN/002/2026
Asunto: Lineamientos generales de seguridad de la información, respaldo, almacenamiento y uso de equipos de cómputo institucionales

PERSONAL DIRECTIVO, ADMINISTRATIVO Y DOCENTES
P R E S E N T E

La Universidad Politécnica de Amozoc reconoce que la información de su propiedad, la información de sus usuarios, los activos de información y la infraestructura tecnológica que los soporta constituyen elementos esenciales para la continuidad de las labores académicas, administrativas y operativas de la Institución.

Por tal motivo, resulta indispensable proteger dichos activos mediante controles adecuados de acceso, uso, respaldo, almacenamiento, conservación, revelación y eliminación segura, conforme a los intereses institucionales, la normatividad aplicable y las mejores prácticas en materia de seguridad de la información.

En consecuencia, se establecen los siguientes lineamientos de observancia obligatoria para todo el personal de la Universidad Politécnica de Amozoc.

A. Funciones generales y responsabilidades

1. Obligatoriedad

La presente Política es de aplicación obligatoria para todo el personal de la Universidad Politécnica de Amozoc, cualquiera que sea su situación contractual, el área de adscripción, el cargo que desempeñe o el nivel de responsabilidad asignado.

Asimismo, será aplicable a toda persona que, con motivo de sus funciones, actividades, prestación de servicios, prácticas profesionales, servicio social o colaboración institucional, tenga acceso a información, sistemas, equipos de cómputo, redes, plataformas, archivos o infraestructura tecnológica de la Universidad.

2. Aprobación y modificaciones

Las directivas institucionales, en coordinación con el Comité de Tecnologías de la Información y Comunicación, en adelante CTIyC, serán las responsables de aprobar la presente Política.

Cualquier modificación, actualización, ampliación o ajuste a estos lineamientos deberá ser revisado y autorizado por las instancias competentes, con la finalidad de asegurar su vigencia, pertinencia y correcta aplicación institucional.

3. Responsabilidades del CTIyC

El CTIyC será responsable de revisar, proponer y recomendar a las directivas institucionales el contenido de la presente Política, así como de definir las funciones generales en materia de seguridad de la información.

De igual manera, le corresponderá estructurar, recomendar, dar seguimiento y promover la mejora continua del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, de la Institución.

El CTIyC también deberá proponer estrategias de capacitación, concientización y difusión interna, con el propósito de fortalecer la cultura institucional en materia de protección de la información, uso adecuado de los recursos tecnológicos y prevención de riesgos informáticos.

4. Coordinación del CTIyC

La persona titular de la Coordinación del CTIyC será responsable de organizar, convocar y coordinar las acciones del Comité en materia de seguridad de la información.

Asimismo, deberá impulsar la implementación, cumplimiento, seguimiento y mejora de la presente Política, procurando la participación de las áreas involucradas y la atención oportuna de los riesgos identificados.

5. Grupo responsable de seguridad informática

El grupo responsable de seguridad informática será el encargado de cumplir las funciones relacionadas con la protección de los sistemas de información de la Universidad.

Sus actividades comprenderán la operación, seguimiento y supervisión técnica del SGSI, así como la vigilancia del cumplimiento de los presentes lineamientos, de acuerdo con las capacidades institucionales, el personal disponible y los recursos autorizados.

El nivel de supervisión, intervención y alcance de dicho grupo deberá ser avalado por el CTIyC.

6. Propietarios de activos de información

Las áreas propietarias de activos de información serán responsables de clasificar, mantener, actualizar y resguardar la información que se encuentre bajo su administración.

Deberán documentar la clasificación de dicha información, definir los usuarios autorizados para acceder a ella y establecer los permisos correspondientes, de acuerdo con las funciones, atribuciones y competencias de cada persona.

Asimismo, tendrán la responsabilidad de procurar que los activos de información se mantengan íntegros, confidenciales y disponibles durante su creación, desarrollo, producción, mantenimiento, uso, respaldo y conservación.

7. Oficina de Sistemas y Departamento de Servicios Informáticos

La Jefatura de la Oficina de Sistemas, en coordinación con la Jefatura del Departamento de Servicios Informáticos, deberá observar los presentes lineamientos y atender los requerimientos técnicos necesarios para la operación, administración, comunicación, mantenimiento y protección de la infraestructura tecnológica institucional.

A dichas jefaturas les corresponderá determinar, actualizar y resguardar el inventario de activos de información, equipos de cómputo, sistemas, plataformas, licencias, redes, dispositivos y demás recursos tecnológicos de los cuales sean propietarios, responsables o custodios.

También deberán apoyar a las áreas en la implementación de controles técnicos para proteger la información institucional y prevenir accesos no autorizados, pérdida de datos, alteraciones indebidas o afectaciones a los servicios tecnológicos.

8. Abogado General

El Abogado General verificará que la presente Política sea considerada en la gestión de contratos, convenios, acuerdos, instrumentos jurídicos y demás documentación legal relacionada con empleados, proveedores, terceros o cualquier persona física o moral que tenga acceso a información o infraestructura tecnológica de la Universidad.

Asimismo, brindará asesoría legal en materia de seguridad de la información, protección de datos, confidencialidad, responsabilidades administrativas y demás disposiciones normativas aplicables.

9. Usuarios

Todas las personas usuarias de la información, sistemas, equipos de cómputo, redes, plataformas y recursos tecnológicos institucionales serán responsables de conocer, comprender y cumplir la Política de Seguridad de la Información vigente.

El desconocimiento de estos lineamientos no exime de responsabilidad a quienes hagan uso indebido de la información, equipos, sistemas o infraestructura tecnológica de la Universidad.

B. Respaldo de información

Todos los mandos medios y superiores de las áreas de la Institución serán responsables de identificar la información sensible, crítica o necesaria para la operación de sus respectivas áreas, considerando su importancia, confidencialidad, disponibilidad, valor institucional y riesgo de pérdida.

Dichas áreas deberán informar al Departamento de Servicios Informáticos sobre la información que requiera respaldo, así como sobre la periodicidad sugerida, los responsables de su administración y cualquier condición especial para su conservación.

El Departamento de Servicios Informáticos tendrá la obligación de:

1. Implementar procedimientos estandarizados para respaldar la información institucional.

2. Respaldar periódicamente la información crítica que resida en los sistemas institucionales, incluyendo configuraciones, registros de actividad, sistemas de archivos, bases de datos, documentos oficiales y demás información necesaria para la continuidad operativa.
3. Asegurar que la ejecución de los respaldos no afecte de manera significativa la operación, disponibilidad o rendimiento de los sistemas institucionales.
4. Realizar los respaldos preferentemente fuera de los horarios ordinarios de operación laboral, documentando formalmente cualquier excepción.
5. Proveer, administrar o gestionar los espacios de almacenamiento necesarios para el resguardo de la información institucional, conforme a la disponibilidad de recursos autorizados.
6. Orientar a las áreas usuarias respecto al manejo correcto de la información que deba respaldarse, sin que ello sustituya la responsabilidad de cada área sobre la organización, actualización y clasificación de sus archivos.
7. Revisar y validar periódicamente la integridad de los respaldos, a fin de verificar que la información sea recuperable, legible, vigente y útil para la operación institucional.
8. Evitar la obsolescencia tecnológica de los medios de almacenamiento utilizados para respaldo, procurando el uso de tecnologías adecuadas que permitan optimizar el espacio físico y lógico disponible.
9. Almacenar los respaldos generados en sitios protegidos contra riesgos ambientales, accesos no autorizados, daño físico, pérdida o destrucción.
10. Procurar que los respaldos críticos se conserven en una ubicación alterna razonablemente separada de la sede principal, cuando las condiciones institucionales lo permitan, con la finalidad de reducir el riesgo de pérdida total ante un siniestro.
11. Mantener un registro actualizado y con acceso controlado que contenga los datos generales de los archivos respaldados, incluyendo el área responsable, tipo de información, fecha de generación, fecha de modificación más reciente, periodicidad del respaldo y medio de almacenamiento utilizado.

C. Almacenamiento, uso de recursos tecnológicos y destrucción de la información

1. Asignación de recursos

El Departamento de Servicios Informáticos deberá proporcionar, administrar o gestionar espacios de almacenamiento suficientes para que las áreas resguarden copia de su información institucional, de acuerdo con la disponibilidad presupuestal, técnica y operativa de la Universidad.

2. Control de acceso

Se deberá contar con un inventario actualizado de usuarios autorizados para acceder a los recursos de almacenamiento de cada área.

Los accesos deberán asignarse conforme a las funciones y responsabilidades de cada persona, evitando permisos innecesarios, excesivos o no justificados.

3. Uso institucional

Los recursos de almacenamiento institucional deberán utilizarse exclusivamente para el resguardo de información relacionada con las actividades oficiales de la Universidad.

Queda estrictamente prohibido utilizar dichos recursos para almacenar archivos personales, música, fotografías privadas, videos ajenos a las funciones institucionales, software no autorizado, instaladores, copias de programas, archivos maliciosos o cualquier contenido que no corresponda a las actividades propias de la Institución.

4. Eliminación segura

El Departamento de Servicios Informáticos deberá contar con procedimientos y mecanismos para el borrado seguro o destrucción física de información institucional que ya no sea necesaria para la operación, siempre que no exista obligación legal, administrativa, fiscal, archivística o normativa que exija su conservación.

La eliminación de información deberá realizarse de manera controlada, documentada y autorizada por el área responsable, evitando pérdidas indebidas, eliminación accidental de información vigente o destrucción de documentos sujetos a conservación obligatoria.

D. Prohibiciones sobre equipos de cómputo institucionales

Con la finalidad de proteger la infraestructura tecnológica, las licencias institucionales, la información oficial y la continuidad de los servicios, queda estrictamente prohibido para todo el personal:

1. Formatear equipos de cómputo institucionales sin autorización expresa de la instancia competente.
2. Instalar, reinstalar, modificar, sustituir o eliminar software en los equipos de cómputo de la Universidad sin autorización del área responsable.
3. Instalar, reinstalar, cambiar, sustituir o modificar sistemas operativos en equipos de cómputo institucionales sin autorización expresa del Departamento de Servicios Informáticos o de la instancia que corresponda.
4. Eliminar, alterar, desactivar o modificar licencias de software adquiridas, asignadas o instaladas por la Universidad.
5. Descargar, instalar o ejecutar programas, aplicaciones, extensiones, herramientas, controladores, licencias, activadores o cualquier componente tecnológico no autorizado.
6. Realizar configuraciones que comprometan la seguridad, estabilidad, rendimiento o disponibilidad de los equipos, sistemas, redes o servicios institucionales.
7. Manipular componentes físicos de los equipos de cómputo, servidores, dispositivos de red, periféricos o infraestructura tecnológica sin autorización.
8. Deshabilitar antivirus, mecanismos de protección, configuraciones de seguridad, controles de acceso o herramientas institucionales de monitoreo.
9. Utilizar los equipos de cómputo institucionales para fines personales, comerciales, políticos, ilícitos o contrarios a los intereses de la Universidad.
10. Extraer, copiar, transferir o almacenar información institucional en medios personales o no autorizados.

El incumplimiento de estas disposiciones podrá hacerse del conocimiento de las autoridades competentes de la Universidad, a efecto de que se determinen las medidas administrativas, técnicas o legales que resulten procedentes conforme a la normatividad aplicable.

Sin otro particular, se solicita a todo el personal observar puntualmente los presentes lineamientos y contribuir al fortalecimiento de la seguridad de la información, la protección

de los recursos tecnológicos y la continuidad operativa de la Universidad Politécnica de Amozoc.

ATENTAMENTE
Coordinación de Sistemas
Departamentos de Servicios Informaticos
Subdirección de Planeación, Evaluación y Estadística
Universidad Politécnica de Amozoc