UPAM
UNIVERSIDAD POLITÉCNICA DE AMOZOC

Amozoc de Mota, Puebla a 29 de agosto de 2022
ANEXO 1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PERSONAL ADMINISTRATIVO, DOCENTE Y EXTERNO
P R E S E N T E

Con fundamento en los artículos 17 fracciones V, X y 18 fracciones XV, XII del Reglamento Interior de la Universidad Politécnica me permito informar que:

La Universidad Politécnica de Amozoc depende de los Sistemas de Tecnologías de Información (TIC) y Comunicaciones, para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, garantizando su resiliencia tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Alcance:

Esta política se aplica a todos los sistemas TIC de la Universidad Politécnica de Amozoc y a todos los miembros de la comunidad universitaria, sin excepciones.

- Personal administrativo
- Personal docente
- Personal externo (cafetería, papelería, limpieza y vigilancia)

Política de Seguridad de la Información

"La Universidad Politécnica de Amozoc reconoce que la información de su propiedad y la de sus clientes, así como, los activos de información y la infraestructura que la soporta, son esenciales para la continuidad de las labores diarias; por lo que es fundamental protegerlos, restringiendo el acceso, uso y revelación, conforme a sus intereses institucionales".

Por lo anterior se establece los siguientes:

a) Funciones Generales

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Universidad Politécnica de Amozoc, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

UPAM
UNIVERSIDAD POLITÉCNICA DE AMOZOC

Las directivas institucionales en conjunto con el Comité de Tecnologías de la Información y Comunicación (CTIyC) aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Tecnologías de la Información y Comunicación de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución.

Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.

El Coordinador del Comité de Tecnologías de la Información y Comunicación será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El grupo responsable de Seguridad Informática será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGC y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Tecnologías de la Información y Comunicación.

Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de la Oficina de sistemas en coordinación con el jefe de Departamento de Servicios Informáticos debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la Universidad. Corresponde a dichas jefaturas determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios.

El Abogado General verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información. Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

UPAM
UNIVERSIDAD POLITÉCNICA DE AMOZOC

b) Respaldo de información

Todos los mandos medios y superiores de las áreas dentro de la Institución son responsables de identificar la información que sea sensible para la operación de su área de acuerdo a su criticidad y deben dar aviso a Departamento de Servicios Informáticos para gestionar su respaldo y periodicidad.

El Departamento de Servicios Informáticos debe:

1. Implementar procedimientos para respaldar la información de la Institución.
2. Respaldar periódicamente toda la información (configuraciones, logs, file systems, bases de datos, etc.) que resida en los sistemas de la Institución, considerando su criticidad.
3. Asegurar que el respaldo de la información de los sistemas, en lo posible no degrade su operación.
4. Los respaldos deben llevarse a cabo preferentemente fuera de los horarios de operación y se documentan las excepciones.
5. Proveer espacios suficientes para almacenamiento y resguardo de la información del negocio que será respaldada periódicamente, siendo responsabilidad de cada usuario el manejo de la información a respaldar.
6. Revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que cumple con los principios de integridad y disponibilidad.
7. Evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.
8. Almacenar los respaldos generados en un sitio protegido contra el medio ambiente y con controles estrictos de acceso, que debe ubicarse a una distancia razonable fuera del alcance de un evento en la zona principal.
9. Mantener un registro actualizado, con acceso controlado, que contenga los datos de todos los archivos respaldados, fuera de las instalaciones de la Institución, indicando la fecha más reciente en que la información fue modificada y la naturaleza de la misma.

c) Almacenamiento de información

El Departamento de Servicios Informáticos debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su información institucional. Asimismo, debe contar con un inventario de usuarios autorizados en los recursos de almacenamiento de cada área. Queda prohibido la utilización de recursos de almacenamiento institucional para archivos de uso personal.

El Departamento de Servicios Informáticos debe contar con procedimientos y mecanismos de borrado o destrucción y de la información de la Institución, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

ATENTAMENTE

DRA. MARÍA ROCÍO TORRES SOTO
RECTORA
UNIVERSIDAD POLITECNICA DE AMOZOC
COMITÉ DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CTIyC