



POLÍTICAS O LINEAMIENTOS PARA LA ADQUISICIÓN, MANTENIMIENTO, SOPORTE, DESARROLLO, USO Y DESECHO DE LAS TIC

1 Introducción

1.1 Objetivo y Propósito

La gestión estandarizada y profesional de las tecnologías de la información (TI) es un pilar fundamental para la eficiencia operativa, la seguridad de los datos y la prestación de servicios públicos de calidad en el ITSOEH. Una administración tecnológica coherente y planificada permite optimizar recursos, mitigar riesgos y alinear la infraestructura digital con los objetivos estratégicos del Instituto.

El objetivo principal de esta política es establecer un marco normativo claro y de obligado cumplimiento para gobernar el ciclo de vida completo de los activos tecnológicos del Instituto, desde su adquisición hasta su desecho. Este documento define los lineamientos que aseguran una toma de decisiones informada, una gestión responsable y un uso seguro de la tecnología en todas las áreas. A continuación, se detallan las directrices para cada fase del ciclo de vida tecnológico.

1.2 Alcance y Aplicabilidad

Esta política es de aplicación general y obligatoria para todas las áreas y personal del ITSOEH que adquieran, utilicen, gestionen o desechen cualquier tipo de tecnología de la información propiedad del tecnológico.



2. Lineamientos para la Adquisición de Tecnologías de la Información

Un proceso de adquisición riguroso y estratégico es el primer paso para construir una infraestructura tecnológica sólida y sostenible. Una compra bien planificada previene incompatibilidades, optimiza el gasto público y garantiza que la tecnología adquirida responda verdaderamente a las necesidades funcionales del ITSOEH, sentando las bases para su operación eficiente y segura.

2.1 Evaluación de Necesidades

Es requisito indispensable la identificación clara y documentada de los requerimientos funcionales, técnicos y de seguridad antes de iniciar cualquier proceso de compra tecnológica. Esta evaluación previa garantiza que la inversión se alinee con las necesidades reales de la operación institucional.

2.2 Estándares y Compatibilidad

Toda nueva tecnología deberá garantizar la compatibilidad con los sistemas existentes y apegarse estrictamente a los estándares tecnológicos previamente aprobados por el instituto. Este lineamiento es crucial para asegurar la interoperabilidad, facilitar la integración y evitar la fragmentación tecnológica que genera costos ocultos y complejidades operativas.

2.3 Análisis de Costo-Beneficio

Se exige la realización de un análisis que considere el Costo Total de Propiedad (TCO). Este análisis debe incluir no solo el precio de compra, sino también los costos asociados a licencias, mantenimiento, capacitación y el eventual reemplazo del activo, proporcionando una visión completa del impacto financiero a largo plazo.



2.4 Proceso de Selección Transparente

Se mandata el uso de procesos de selección formales (licitaciones, cotizaciones, etc.) para todas las adquisiciones tecnológicas. Este requisito tiene como fin garantizar la transparencia en el uso de los recursos públicos, promover la competitividad entre proveedores y asegurar la obtención de las mejores condiciones de calidad y precio para el instituto.

2.5 Formalización de Contratos y Acuerdos

Toda adquisición deberá formalizarse a través de contratos o acuerdos por escrito. Dichos documentos deberán especificar, como mínimo, las garantías aplicables, los niveles de servicio comprometidos y las condiciones del soporte técnico que proporcionará el proveedor.

Una vez que la tecnología ha sido adquirida conforme a estos lineamientos, su correcto mantenimiento se convierte en el siguiente paso crítico para maximizar su valor y vida útil.

3. Lineamientos para el Mantenimiento de Tecnologías de la Información

El mantenimiento proactivo de la infraestructura tecnológica no es un gasto, sino una inversión estratégica. Un programa de mantenimiento adecuado alarga la vida útil de los equipos, previene fallos críticos que podrían interrumpir servicios esenciales y garantiza la continuidad operativa de las funciones del instituto.

3.1 Planes de Mantenimiento Preventivo y Correctivo

Se establece la obligación de diseñar e implementar rutinas periódicas de mantenimiento preventivo para todos los sistemas y equipos críticos. Adicionalmente, se deberá contar con un protocolo de actuación para el mantenimiento correctivo que permita resolver fallos de manera eficiente y minimizar el tiempo de inactividad.



3.2 Gestión de Actualizaciones

Se ordena asegurar la instalación oportuna de parches de seguridad y actualizaciones de software en todos los sistemas y aplicaciones. Esta práctica es fundamental para mitigar vulnerabilidades, proteger la información del ITSOEH contra amenazas cibernéticas y garantizar el óptimo funcionamiento de las herramientas tecnológicas.

3.3 Documentación Técnica

Se exige mantener actualizada y accesible toda la documentación técnica relevante de los activos tecnológicos. Esto incluye diagramas de red, manuales de operación, registros de configuración, información de licencias y cualquier otro documento necesario para la correcta administración y soporte de la infraestructura. Un mantenimiento efectivo depende de una estructura de soporte técnico bien organizada y capacitada para responder a las necesidades de los usuarios.

4. Lineamientos para el Soporte Técnico

Un sistema de soporte técnico eficiente y centralizado es crucial para la productividad del instituto. Este servicio es el punto de contacto directo con los usuarios para resolver incidencias rápidamente, minimizar la interrupción del trabajo y maximizar la adopción y el aprovechamiento de las herramientas tecnológicas disponibles.

4.1 Mesa de Ayuda

Se ordena la implementación de un canal centralizado como único punto de contacto para la atención, registro y seguimiento de todas las incidencias y solicitudes de soporte técnico. Esta centralización permite una gestión ordenada de los requerimientos y la generación de métricas para la mejora continua del servicio.



4.2 Niveles de Atención

Se instruye sobre la necesidad de definir y comunicar claramente los niveles de atención. Esto implica establecer tiempos de respuesta y resolución de problemas basados en la prioridad y el impacto de cada incidencia, garantizando que los problemas más críticos reciban atención prioritaria.

4.3 Capacitación del Personal de Soporte

Se establece como un requisito permanente **garantizar la actualización y capacitación constante del equipo de soporte técnico**. El personal de soporte debe poseer las habilidades y conocimientos necesarios para atender eficazmente las tecnologías vigentes en el instituto y resolver problemas de manera competente. Más allá de mantener la infraestructura existente, el instituto debe gestionar adecuadamente el desarrollo de nuevas soluciones tecnológicas.

5. Lineamientos para el Desarrollo de Sistemas

La adopción de un enfoque disciplinado y metódico para el desarrollo de software es fundamental. Una metodología clara y el cumplimiento de estándares de calidad y seguridad aseguran la creación de sistemas robustos, seguros, escalables y verdaderamente alineados con los objetivos estratégicos y las necesidades operativas del instituto.

5.1 Metodologías de Desarrollo

Todo proyecto de desarrollo de sistemas deberá adoptar una metodología de trabajo clara, ya sea ágil o tradicional, la cual será seleccionada en función de la naturaleza, el alcance y los requisitos específicos del proyecto para garantizar una gestión eficiente y resultados de alta calidad.



5.2 Ciclo de Vida del Software

Es obligatorio seguir las etapas formales del ciclo de vida del desarrollo de software: requerimientos, diseño, desarrollo, pruebas, implementación y mantenimiento. El cumplimiento de cada una de estas fases asegura un proceso ordenado y reduce los riesgos de fracaso del proyecto.

5.3 Seguridad y Privacidad desde el Diseño

Se mandata la integración de los principios de "privacy by design" (privacidad desde el diseño) y "security by design" (seguridad desde el diseño) como un requisito no negociable en todas las etapas del desarrollo. La seguridad y la protección de datos deben ser consideradas desde la concepción inicial del sistema, no como un añadido posterior.

5.4 Control de Versiones y Pruebas

Se ordena el uso obligatorio de herramientas de versiones de código y la utilización de ambientes de pruebas diferenciados del ambiente de producción. Esto es esencial para llevar un control riguroso de los cambios, facilitar la colaboración y garantizar la calidad y estabilidad de las aplicaciones antes de su despliegue final. La forma en que se construyen los sistemas es tan importante como la forma en que el personal los utiliza en su día a día.

6. Lineamientos para el Uso de las Tecnologías de la Información

Regular el uso de los recursos tecnológicos es una responsabilidad compartida. La definición de normas claras es esencial para proteger la información y los activos del instituto, asegurar la disponibilidad de los recursos para fines laborales y promover un entorno de trabajo digital seguro, ético y eficiente para todo el personal.



6.1 Políticas de Uso Aceptable

Se ordena el establecimiento y la difusión de normas claras sobre el uso responsable de los recursos tecnológicos institucionales, incluyendo equipos de cómputo, redes, correo electrónico y sistemas de información. Estas políticas deben definir qué constituye un uso apropiado e inapropiado para fines laborales.

6.2 Capacitación y Sensibilización

Es un requisito permanente formar continuamente a los usuarios sobre el uso seguro y eficiente de las herramientas de TI. Los programas de capacitación deben incluir temas sobre ciberseguridad, protección de datos personales, mejores prácticas y los riesgos asociados a un uso inadecuado de la tecnología.

6.3 Control de Accesos

Se exige la implementación de controles de acceso a la información basados en roles, aplicando el principio de mínimo privilegio. Asimismo, se debe garantizar el uso de mecanismos de autenticación segura (como contraseñas robustas) y el monitoreo de las actividades en los sistemas para detectar y prevenir accesos no autorizados.

Finalmente, el ciclo de vida de la tecnología concluye con su retiro y desecho, una etapa que requiere la misma atención y rigor que su adquisición.

7 Lineamientos para el Desecho de Tecnologías de la Información

Un proceso de desecho formal y seguro tiene una doble importancia crítica: la protección de datos sensibles institucionales y la responsabilidad ambiental. Una gestión inadecuada en esta etapa final puede derivar en graves fugas de información, con consecuencias legales y de reputación, así como en el incumplimiento de la normativa ambiental vigente.



7.1 Política de Baja Tecnológica

Se ordena la definición de criterios claros y objetivos para dar de baja y reemplazar equipos y sistemas obsoletos. Estos criterios, basados en el rendimiento, la seguridad o el fin del soporte, permitirán una renovación tecnológica planificada y presupuestada, evitando el uso de tecnología riesgosa o ineficiente.

7.2 Eliminación Segura de Datos

Es un mandato crítico asegurar el borrado seguro y permanente de todos los datos institucionales almacenados en cualquier dispositivo antes de su desecho, donación o reciclaje. Se deben utilizar métodos certificados que garanticen que la información no pueda ser recuperada, previniendo así cualquier fuga de información sensible.

7.3 Gestión Ambiental

Se exige el cumplimiento estricto de las normativas ambientales vigentes para el reciclaje o disposición final de equipos electrónicos. Específicamente, se deberá seguir la normativa sobre Residuos de Aparatos Eléctricos y Electrónicos (RAEE) para asegurar una gestión responsable con el medio ambiente.

El cumplimiento integral de esta política es una responsabilidad de todo el personal y resulta esencial para la modernización, la eficiencia y la seguridad del ITSOEH.

ATENTAMENTE
Excelencia en Educación Tecnológica®

ING. IVAN RODRIGUEZ HERNANDEZ
ENCARGADO DE SOPORTE TÉCNICO

VALIDO

MTRO. ÁNGEL HERNÁNDEZ CABRERA
DIRECTOR DE PLANEACIÓN Y
VINCULACIÓN