Secretaría de Estado de la Presidencia
Gobierno de la República

MANUAL DE POLITICAS DE TECNOLOGÍA

UNIDAD DE COMUNICACIÓN Y TECNOLOGÍA (UCIT)

Versión
MPT-001

INDICE

INTRODUCCIÓN

El Manual de Políticas de Tecnología de la Información (MPT) de la Secretaría de Estado de la Presidencia (SEP) representa una importante herramienta que servirá para garantizar el buen funcionamiento de los procesos, para contribuir con su eficiencia, para optimizar los sistemas internos y garantizar la calidad en la gestión, con el objetivo de asegurar la seguridad de la información.

Se define Tecnología de la Información (TI), a las herramientas y métodos utilizados para recabar, retener, manipular o distribuir información, la cual se encuentra por lo general relacionada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

En los sistemas de información la ética debe estar presente, por lo que la SEP como institución promotora de la ética y la transparencia, espera que el establecimiento de este manual de políticas pueda transparentar y dar idoneidad a los métodos que son utilizados para manejar el uso de la tecnología de la información que dispone la institución.

Con este manual, se pretende trazar los lineamientos bajo la responsabilidad del área de Tecnología de la Información, como de los usuarios del uso de la misma, a fin de que toda administración en este contexto se realice de una manera clara, precisa, transparente y lo más real posible, donde se respeten los principios éticos que, dentro del marco normativo aceptado por la sociedad, produciendo así una escala de valores de hechos y formas de comunicación dentro de la institución.

Para definir las políticas de TI, es necesario analizar procesos tomando en cuenta las necesidades presentes y futuras de la institución, considerando como factor principal al capital humano con que cuenta la organización. De esta manera se busca que sus funcionarios y empleados se identifiquen con las políticas establecidas, encausando sus esfuerzos en el fomento del trabajo en equipo, en la integración y en la coordinación de todas las áreas en una misma dirección.

Conscientes de que el uso de la tecnología electrónica ha transformado a toda la humanidad, pretendemos encausar la administración de la tecnología de la información de nuestra organización, estableciendo políticas enfocadas a los procesos de la institución y orientadas

al logro de los planes, metas y objetivos de la misma, por lo que esperamos que nuestros mayores esfuerzos estén centrados en nuestra Misión y Visión, razón de nuestra esencia como Institución y en reforzar nuestros valores éticos y morales para que inspiren nuestros actos.

1. ASPECTOS GENERALES

1.1. OBJETIVOS DEL MANUAL

Los objetivos del Manual de Políticas de Tecnología de la Información de la Secretaría de Estado de la Presidencia, son los siguientes:

a) Crear y definirlas políticas generales y específicas que faciliten la ejecución de las actividades de tecnología de la información en las diferentes áreas de la Institución.

b) Promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos adecuados.

c) Normar los procesos de información con la finalidad de mejorar el rendimiento de la SEP.

d) Establecer las políticas para resguardo y garantía de acceso apropiado de la información de la SEP.

1.2. ALCANCE

El presente manual abarca las políticas que serán aplicadas en la Secretaría de Estado de la Presidencia, a través de la Unidad de Comunicación Institucional y Tecnología (UCIT).

1.3. PROPÓSITO

Dejar establecidas las políticas de TI que regirán el uso y mantenimiento de la plataforma tecnológica de la institución, para asegurar su operatividad, de manera que los responsables del uso de las tecnologías disponibles, aseguren el cumplimiento de las mismas, con miras al desarrollo de un trabajo óptimo y de calidad.

1.4 AUTORIZACIÓN

El Manual de Políticas de Tecnología de la Información (MPT) de la SEP, es aprobado, previa revisión y verificación.

1.5 EDICIÓN Y DISTRIBUCIÓN

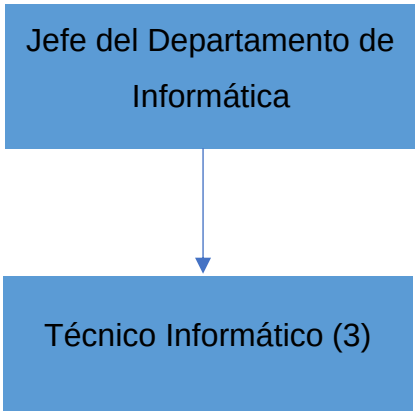
La edición se realizará en formato digital, la versión en físico será encuadernada, a fin de que permita realizar la sustitución de las páginas cuando ocurran revisiones y modificaciones. Recibirán un ejemplar completo del Manual:

- **Unidad de Comunicación Institucional y Tecnología**
- **Unidad de Planificación y Evaluación de la Gestión**

1.6 REVISIONES Y MODIFICACIONES

Cualquier cambio, corrección o recomendación se comunicará al Departamento de Planificación (UPEG), responsable de llevar a cabo revisiones periódicas al documento.

1.7 ORGANIGRAMA



.

2. POLÍTICAS TECNOLÓGICAS

La Unidad de Comunicación Institucional y Tecnología, como área de servicio interno, se encarga de resguardar, velar por el uso y funcionamiento de la plataforma tecnológica de la institución y asegurar permanente asistencia a los usuarios de la Institución, constituyéndose además en:

a) El reformador y operador de la Infraestructura Informática de la Institución y sus funciones deberán unificarse sin importar la localidad, a partir de la fecha de aprobación de estas políticas.

b) A su vez está autorizado, para delimitar o definir los equipos y programas existentes y a ser adquiridos que conforman los activos informáticos adecuados para la ejecución de los procesos.

2.1 INFRAESTRUCTURA DE HARDWARE (EQUIPOS, DISPOSITIVOS, APARATOS).

2.1.1 RESPONSABILIDADES DE TI

La responsabilidad de **TI** ante la adquisición, instalación, mantenimiento y buen funcionamiento de los equipos, dispositivos de la Institución son las siguientes:

a) Deberá vigilar y llevar un inventario detallado de la infraestructura de Hardware de la Institución, acorde con las necesidades existentes de la misma.

b) Será la única responsable de hacer requerimientos de los activos informáticos que hayan sido proyectados, según las necesidades que se presenten en cada área de trabajo, estas bajo una previa revisión y aprobación de la unidad solicitante.

c) Deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.

d) Deberá participar en los procesos de adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros a fin de dar una opinión técnica del equipo tecnológico.

e) Deberá confirmar que los equipos de informática cumplan con las especificaciones indicadas en las solicitudes de compra.

f) Deberá realizar el mantenimiento técnico preventivo de todos los equipos informáticos de la Institución.

g) Será responsable de instalar los equipos y programas informáticos utilizados en la Institución.

h) Será responsable de evaluar el área física donde se instalará un nuevo equipo informático, confirmando que el área este óptima para la instalación de los mismos.

i) Verificará que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, entre otros.

j) Deberá solicitar a la Gerencia Administrativa las infraestructuras o servicios de disponibilidades eléctricas, previamente a la instalación de los equipos informáticos requeridos.

k) Velará por el adecuado uso de las instalaciones eléctricas requerida para el funcionamiento de los equipos tecnológicos.

l) Verificará el inventario de los equipos y programas informáticos que sean instalados, con la finalidad de llevar un control de los mismos.

m) Instruirá al Usuario sobre el uso y manejo adecuado de los equipos y programas informáticos instalados.

n) Verificará que los suplidores de programas de computadoras suministren los manuales correspondientes al funcionamiento de los equipos o programas especializados.

2.1.2 RESPONSABILIDADES DE LOS USUARIOS

Los recursos informáticos asignados a los usuarios, deben usarse adecuadamente, con responsabilidad acorde a los siguientes lineamientos:

a) Solo podrán utilizar los equipos asignados para ejecutar las actividades o tareas Institucionales.

b) No podrán usar equipos tecnológicos personales como: laptops, dispositivo informático, etc., en el área de trabajo salvo excepciones de las unidades que lo requieran previamente justificado.

c) No podrá traer ni efectuar solicitudes a **TI**, de reparación de equipos tecnológicos personales.

d) Solicitará a TI un levantamiento de los equipos informáticos necesarios que requiera el área.

2.2 INFRAESTRUCTURA DE SOFTWARE (PROGRAMAS DE COMPUTADORA)

TI, es responsable ante la institución de la instalación, actualización y modificación de los programas de computadoras utilizados por la misma.

2.2.1 RESPONSABILIDAD DE TI

a) Llevará inventario del software (programas) instalados en la Institución.

b) Velará porque todo el software instalado en la SEP, este legalmente licenciado.

c) Tendrá la custodia y almacenamiento de todos los programas informáticos de la Institución.

d) Definirá los discos portátiles de todas las áreas, para poder fragmentar el acceso a la información y una mejor organización.

e) Establecerá configuraciones automatizadas para que los usuarios guarden toda su información en los discos portátiles y se puedan facilitar las copias de seguridad (backup).

2.2.2 RESPONSABILIDADES Y/O PROHIBICIONES DE LOS USUARIOS

El software existente en los equipos asignados a los usuarios estará regido por los siguientes lineamientos:

a) Evitar instalar y/o descargar juegos, videos, música ni aplicaciones de ningún tipo de las páginas del Internet, que no guarden relación con la SEP.

b) Evitar tener en los discos portátiles archivos que no tengan o guarden relación con la SEP, salvo aquellas áreas que por la naturaleza de sus funciones lo requieran, Tales como:

- MP3 (u otro formato de música)
- EXE (archivos ejecutables)
- MSI (archivos de instalación)
- JPG; JPEG, GIF, BMP, PNG, ETC (imágenes)
- INI (Archivos de configuración de instalación)
- INF (Archivos de configuración de instalación)
- DLL (librerías de archivos)
- ZIP (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
- RAR (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
- Entre otros

c) Prohibido desinstalar el Antivirus de su equipo, ya es de alto riesgo para la seguridad ante el peligro de los virus.

d) Deberá informar a TI, en caso de presentarse cualquier problema de virus en su equipo informático.

2.3 SEGURIDAD DEL ÁREA DE INFORMÁTICA

a) Todos los sistemas de informática deberán estar resguardados dentro del área asignada a TI.

b) Los Usuarios o visitantes externos no podrán acceder al área destinada a TI, sin la previa autorización del Encargado o acompañados de un empleado de la misma.

c) Solo podrán acceder al área de infraestructura informática los empleados de TI.

2.4 CUSTODIA Y TENENCIA DE ACTIVOS INFORMÁTICOS

2.4.1 RESPONSABILIDAD DE TI

El uso indebido de los recursos informáticos puede afectar negativamente el funcionamiento de los equipos de oficina (PC), la red, los servidores por tanto TI:

a) Custodiará todos los activos informáticos de la SEP.

b) Emitirá un dictamen técnico de los equipos informáticos para su previa asignación de acuerdo con los requerimientos de las áreas.

c) Verificará que no le sea asignado un mismo activo informático a más de un Usuario.

d) Verificará que los Usuarios sean empleados regulares de la SEP.

e) Llevará el control de los equipos informáticos portátiles (Laptop) asignados al personal.

2.4.2 RESPONSABILIDAD DE LOS USUARIOS

Al ser asignado un activo a un usuario todo lo concerniente al mismo será de su responsabilidad por lo cual:

a) Será responsable de la custodia de los equipos informáticos asignados (PC´s, monitores, teclados, impresoras, USB, etc.)

b) Notificará, vía electrónica o cualquier otra vía los inconvenientes o anomalías presentada con los equipos, accesorios, impresoras, sistemas, entre otros, para su revisión.

2.5 TRASLADO DE ACTIVOS INFORMÁTICOS

2.5.1 RESPONSABILIDAD DE TI

Al momento de recibir una solicitud de las áreas, para el traslado de un equipo informático fuera de la institución, el compromiso de **TI**, es el siguiente:

a) Verificará el estado de los equipos tecnológicos a ser entregados a las áreas, a través del Formulario Movimientos de Activos (Equipos), aprobado por el Gerencia Administrativa, para comprobar su salida.

b) Verificará con el Dpto. Administrativo y Financiero que el plazo otorgado a los equipos tecnológicos que serán utilizados fuera de la Institución no sea mayor de cinco (5) días.

2.5.2 RESPONSABILIDAD DE LOS USUARIOS

El compromiso de los usuarios al momento de solicitar el traslado de un equipo informático fuera de la institución son los siguientes:

a) Deberá llenar completamente hasta la casilla “Descripción del Equipo” en el Formulario Traslado de Activos el cual debe ser aprobado por el Dpto. Administrativo y Financiero.

2.6 ROBO O PÉRDIDA DE EQUIPO

a) A partir de las políticas definidas por la Gerencia Administrativa, determinara los pasos a seguir para el inventario de los equipos que se reporten como sustraídos.

b) El usuario de un equipo asignado deberá reportar dentro de veinticuatro (24) horas cualquier pérdida o sustracción del mismo, tanto a la Gerencia Administrativa como a la UCIT y Bienes Nacionales, con el fin de inhabilitar accesos de usuario.

c) La Gerencia Administrativa y Bienes Nacionales se encargará de realizar los procesos pertinentes para que se establezca responsabilidad ante dicha pérdida.

d) Ante el caso de que se determine responsabilidad por parte del usuario de dicha perdida, se notificará a la Unidad de Bienes Nacionales de la institución para que se proceda con la aplicación de las medidas que se consideren correspondientes.

2.7 SOFTWARE (PROGRAMAS DE COMPUTADORA)

La procedencia del software utilizado y adquirido por la Institución deberá estar acorde a las especificaciones técnicas que requiera la disponibilidad de la tecnología que disponga la institución.

2.7.1 RESPONSABILIDAD DE TI

a) Velará que el software incluya información de instalación y mantenimiento, para facilitar la labor del personal de soporte técnico.

b) Deberá requerirle a los proveedores, el entrenamiento en el uso del software.

2.8 MODIFICACIÓN O INSTALACIÓN DE SOFTWARE (PROGRAMAS)

Para satisfacer las necesidades de la Institución en cuanto a las modificaciones o Instalaciones de Software, que cumplan con los atributos de calidad adecuados, se definen las siguientes responsabilidades.

2.8.1 RESPONSABILIDAD DE TI

a) Evaluará todas las modificaciones propuestas al software (programas) actuales, tomando en cuenta el buen funcionamiento y costo en beneficio de la Institución.

b) Modificará o Instalará los sistemas de Información acorde a las necesidades de los usuarios, que busquen mejorar los procesos automatizados de la SEP.

2.9 SOPORTE TÉCNICO A LOS EQUIPOS ASIGNADOS

Las responsabilidades descritas constituyen la normativa ante las solicitudes recibidas para la asistencia de soporte técnico a los equipos asignados a los usuarios.

2.9.1 RESPONSABILIDAD DE TI

a) Todas las solicitudes de Soporte Técnico deberán ser remitidas vía correo electrónico, verbal, chat institucional, llamada telefónica o cualquier otro medio al Jefe del Departamento de Informática, quien le dará las instrucciones necesarias al personal técnico bajo su cargo.

b) Deberá dar un tiempo de respuesta a cada una de las solicitudes que hayan sido notificadas por los usuarios en un plazo no mayor de dos (2) días laborables dependiendo el inconveniente reportado.

c) Cuando TI considere que el reporte de avería es mínimo, se podrá proceder con la reparación de inmediato.

d) Deberá de asegurar que el usuario este satisfecho con el servicio prestado.

e) Deberá recibir e instalar los equipos tecnológicos solicitados por las diferentes áreas de la Institución.

f) Se encargará de revisar todos los equipos, accesorios, programas, entre otros.

g) Dará soporte técnico solamente a los equipos informáticos de la SEP.

2.9.2 RESPONSABILIDAD DE LOS USUARIOS

La responsabilidad de los usuarios ante la solicitud de asistencia del área de informática es la siguiente:

a) Solicitará, vía correo electrónico, verbal, chat institucional, llamada telefónica o cualquier otro medio a **TI** las solicitudes de modificaciones o servicio técnico, así como cualquier anormalidad en su equipo, con copia a su superior inmediato.

2.10 PLAN DE CONTINGENCIA

El propósito de un Plan de Contingencia en la informática, busca reanudar las actividades ante un desastre a fin de que la institución pueda mitigar los efectos del mismo, para lo cual **TI**:

2.10.1 RESPONSABILIDAD DE TI

a) Deberá tener siempre en caso de fallas un Plan de Contingencia que permita recuperar en corto tiempo todas las informaciones contenidas en la Red.

2.10.2 RESPONSABILIDAD DE LOS USUARIOS

a) Deberán respetar los lineamientos establecidos en el Plan de Contingencia y abocarse a colaborar con el mismo.

b) Ante la advertencia de un desastre deberá apoyar a TI en la protección de los equipos.

2.11 ASIGNACIÓN DE USUARIO

El objetivo de la asignación de usuarios corresponde a establecer el acceso a los equipos informáticos de la institución, a aquellas personas que forman parte de esta, otorgándole el derecho y el privilegio de inicio de sesión en la red de la institución.

2.11.1 RESPONSABILIDAD DE TI

a) Recibirá las informaciones requeridas para evaluar las solicitudes de creación o modificación de usuarios en los sistemas de información por parte del área de Recursos Humanos.

b) Deberá crear el usuario de los nuevos empleados, con la finalidad de otorgarle el acceso al dominio de la red de la Institución.

c) Deberá informar a la Sección de Recursos Humanos la creación de nuevos usuarios en el dominio de la red.

d) Velará por que los datos de los usuarios en el dominio de la data serán los siguientes: el primer nombre seguido del signo de punto y luego el primer apellido del empleado. Ej.: Ignacio.Torres-Área-SEP

e) Deberá monitorear toda anomalía detectada en la aprobación de creación o modificación de usuarios en el sistema de información.

f) Los empleados en disfrute de vacaciones o licencias médicas, no serán deshabilitados de la data.

g) Se deshabilitará los usuarios de los empleados que hayan finalizado su contrato de trabajo, según información remitida, vía correo electrónico por parte de Recursos Humanos, previo a la elaboración de un Manual de Procedimiento para Entrada y Salida de Personal.

h) Suspenderá el permiso a la red a todo empleado que se encuentre bajo investigación interna por haber cometido alguna infracción en el uso de la tecnología e informará al superior inmediato de dicha suspensión.

2.11.2 RESPONSABILIDAD DE LOS USUARIOS

a) Ningún usuario podrá solicitar directamente a TI, la creación de acceso a la red de la institución.

b) Deberá asegurarse del cierre de manera correcta de la sesión de usuario al momento de finalizar sus labores.

c) No permitirá a persona ajena a la institución el acceso a su Equipo informático asignado.

2.12 SEGURIDAD DE LA INFORMACIÓN

Se prevén medidas de seguridad a ser seguidas por todos los miembros que componen la institución con el propósito de proteger la información y normar los niveles de acceso y confidencialidad, a ser observadas y cumplidas por los involucrados en el uso y mantenimiento de los activos de informáticas de la organización.

2.12.1 RESPONSABILIDAD DE TI

a) Velará para que los equipos estén libres de vulnerabilidades a fin de reducir los riesgos a que puedan someterse.

b) Velará por la seguridad de la información que se genere día a día.

c) Deberá almacenar en un lugar seguro todos los backup’s o copia de seguridad ejecutados.

d) Se encargará de monitorear el uso indebido de todos los equipos tecnológicos por parte de los usuarios de la institución.

e) Velará por la instalación de programas que garanticen la seguridad de la información en los archivos compartidos.

f) Asegurará que los encargados de áreas que manejan plataformas de datos electrónicos, se rijan por las políticas establecidas en este manual.

g) Realizará auditorías continuas a las carpetas con informaciones compartidas en el disco público, lo que permitirá determinar responsabilidad cuando sean reportadas informaciones como borradas.

2.12.2 RESPONSABILIDAD DE LOS USUARIOS

a) Solo utilizará el correo electrónico Institucional para recibir y/o enviar correspondencia relacionadas con su trabajo.

b) Los usuarios deberán revisar y responder día a día todos los correos electrónicos internos como externos relacionados con las actividades de la Institución.

c) Deberá manejar todas las informaciones institucionales exclusivamente a través de los correos internos que dispone la organización.

d) Se asegurará de salvar y proteger la información que maneja.

e) No podrá transferir a terceros información considerada como confidenciales sin autorización previa.

f) Guardará la información de trabajo en los discos de red asignados por usuario, garantizando así la integridad de la información.

g) Deberá borrar todos aquellos correos que no deban permanecer en los buzones ni en la papelera.

h) Deberá crear una contraseña privada, con la finalidad de acceder a los datos, servicios y programas de su equipo, asegurándose que tenga las siguientes características:
- Ocho (8) ó más caracteres
- Combinar letras mayúsculas, minúsculas y números.
- Fácil de recordar y difícil de adivinar

i) No deberá compartir la contraseña creada para acceder al Equipo Informático asignado.

j) No hará uso indebido de la información institucional que maneja.

2.13 MANEJO DE IMPRESORAS

Buscando regular la impresión de documentos innecesarios por parte de los usuarios de las impresoras asignadas y establecer un control interno, se han establecido los siguientes lineamientos:

2.13.1 RESPONSABILIDAD DE TI

a) Se encargará de monitorear el uso de las impresoras de red.

b) Coordinara con los encargados de área, el personal que puede tener acceso a las impresoras de red como a las impresoras disponibles en los departamentos.

c) Las impresoras a color solo serán utilizadas para imprimir documentos que exclusivamente requieran ser impresos a color, no para hacer pruebas ni borradores.

d) No se imprimirán trabajos que no tengan relación con la institución

e) Cada área solicitará el papel de impresión a utilizar y será responsable del uso del mismo.

f) Solo se utilizarán para impresiones, tóneres y tintas originales.

g) Solo tendrán acceso al uso de impresoras en red fuera de horario de trabajo, los encargados de áreas y el personal autorizado por ellos.

h) Reportara bajo informes el uso indebido de las impresoras.

2.13.2 RESPONSABILIDAD DE LOS USUARIOS

a) No podrán imprimir documentos personales, ni a terceras personas en los equipos de la institución.

b) Deberá contar con la previa autorización de su superior inmediato vía correo electrónico, para utilizar impresoras fuera de horario de trabajo.

c) Deberá triturar los borradores impresos de trabajos considerados como confidenciales.

d) Los “borradores” de trabajos serán impresos bajo el mandato de economía de tinta.

e) Podrá utilizar para borradores de trabajo, hojas recicladas que no contengan información considera como confidencial

f) Hará buen uso del material de trabajo disponible en el área para sus impresiones.

2.14 ACCESO AL INTERNET

El Internet es un medio importante y eficiente de comunicación, por lo cual es importante lograr un uso equitativo y eficiente del mismo, por tanto, TI velará porque se cumplan los siguientes lineamientos:

2.14.1 RESPONSABILIDAD DE TI

a) Se asegurará de coordinar con los encargados de áreas, las páginas de Internet a las que puede tener acceso el personal bajo su cargo, bloqueando aquellas páginas que no sean relevantes para el desempeño de las funciones.

b) Deberá monitorear el acceso de las páginas de internet por parte del personal e informar cualquier violación de acceso, vía correo electrónico a los encargados de las áreas.

c) Deberá informar vía correo electrónico al encargado de área, los casos continuos de violación de acceso a internet a páginas no relacionadas con el trabajo institucional como, por ejemplo: de juegos, de música, descargas, videos, entre otras; con la finalidad de que se tomen las medidas de lugar.

d) Dará seguimiento a la plataforma de internet, notificando a las áreas los inconvenientes presentados en la misma.

2.14.2 RESPONSABILIDAD DE LOS USUARIOS

a) Está prohibido la transmisión y/o, descarga de material obsceno o pornográfico, que contenga amenazas o cualquier tipo de información que atente contra la moral o buenas costumbres.

b) No deberá acceder a las siguientes páginas:

- YouTube
- Facebook
- Twitter
- Hi5
- Bonche.com
- Uepa.com
- Megavideo.com
- Megaupload.com
- Rapidshare.com
- Gigasize.com
- Páginas de Warez
- Otras de igual finalidad

c) Solo tendrá acceso a las siguientes páginas de internet: bancarias, educativas, periodísticas e institucionales.

2.15 IMPREVISTOS

Los casos que se presenten y que estén vinculados al trabajo y no estén contemplados en este Manual de Políticas, serán atendidos o resueltos por Gerencia Administrativa según sea el caso.

2.16 VIGENCIA

Este Manual entrará en vigor a partir de la aprobación y socialización, permanecerá por tiempo indefinido introduciéndosele las revisiones y las mejoras que amerite el mismo.

Este documento ha sido revisado en el mes de octubre del 2022 y cualquier modificación se anexará y notificará a las áreas encargadas para su estricto cumplimiento.

ANEXO

SECRETARÍA DE ESTADO DE LA PRESIDENCIA
SOLICITUD TRASLADO DE BIENES

SOLICITUD NO. ULAB-STB-SEP-XXX-2023	**FECHA SOLICITUD:**

NOMBRE DEL SOLICITANTE	**UBICACIÓN ACTUAL DEL ACTIVO**	**TELÉFONO O EXTENSIÓN**
PARA SER TRASLADADO A:		
BIEN ASIGNADO A:		

DESCRIPCIÓN	**SERIE**	**INVENTARIO**	**SIAFI**

PARA USO EXCLUSIVO DE LA UNIDAD DE COMUNICACION INSTITUCIONAL Y TECNOLOGIA	
SALIDA DE ACTIVO	**DEVOLUCIÓN DE ACTIVO**
ENTREGADO POR:	**RECIBIDO POR:**
FECHA SALIDA: **FECHA P/ DEVOLUCIÓN:**	**FECHA Y HORA**
RECIBIDO POR (NOMBRE):	**ENTREGADO POR (NOMBRE):**
Observaciones:	

FIRMA Y SELLO AUTORIZACIÓN

Nota: Deberá asegurarse que la persona que recibe los activos, es la responsable y que al momento de la entrega estén en perfectas condiciones, exceptuando las salidas para fines de reparación.

Aprobación del Documento

Elaboró:	Revisó:	Aprobó:
Lic. Josué David Rivera Ramírez Jefe del Departamento de Informática	Lic. Josué David Rivera Ramírez Jefe del Departamento de Informática	Lic. Vanessa Elizabeth Maradiaga Gerente Administrativo

Tabla de Versiones

Versión	Fecha	Autor
MPT-001	31-10-22	Josué David Rivera Ramírez