Políticas de Tecnologías de la información

Alcance

El presente documento es aplicable a todos los empleados de los SSEP, consultores, contratistas, colaboradores, practicantes o residentes, incluyendo a todo el personal externo (Usuarios Finales) que en algún momento cuente con acceso a los recursos informáticos propios o arrendados, o información de los Servicios de Salud del Estado de Puebla (SSEP).

Sobre la asignación y el uso de los recursos

1. El personal debe hacer **uso adecuado de los recursos informáticos** para actividades relacionados con los objetivos y metas de la institución (PC, impresoras, programas, correo, etc.). Además, todo el personal deberá informar al **Departamento de Tecnologías de la Información y Telecomunicaciones (DTIyT)** sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento. Se cuenta con una mesa de ayuda, para dar seguimiento a todas sus peticiones.
2. Todo el personal podrá tener una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades, si se **solicita** al área de DTIyT de **manera oficial** a través de memorándum de su titular. Estas cuentas de correo, sólo son para uso oficial, con dependencias gubernamentales o particulares, sólo para procesos propios de su área, no deberán ocuparse para uso personal o cualquier otro motivo que no sea expresamente dado.
3. Para el **desarrollo y/o implementación** de un sistema se deberá evaluar el impacto social y económico, la mejora de productividad o la seguridad que se espera obtener con cada sistema. Además, las necesidades de infraestructura que se requieren para el éxito de cada proyecto, las cuales pueden ser: Equipo de Cómputo actualizado, conexión y velocidad de internet, servidores, dispositivos especiales (lectores de códigos de barra, celulares, gps, etc) licencias. Cada Área que requiera un sistema deberá presentar un proyecto en el formato que el DTIyT les entregue, en caso de información técnica podrá solicitar ayuda al DTIyT.

Sobre la seguridad de la información

4. Diariamente se realizan respaldos automáticos a la base de datos según los mecanismos establecidos en los sistemas considerados críticos. Los usuarios finales podrán justificar ante el DTIyT, de cualquier Sistema para que sea considerado crítico y sea respaldado, si la valoración y requerimientos lo permitieran.
5. Para los **respaldos en equipos personales** se asignará una cuenta y una cuota a cada Departamento o Unidad Administrativa, dicha cuota deberá ser distribuida de la manera que indique el titular entre todo su personal, pudiéndose dar el caso donde el 100% esté en una sola cuenta y a través de ella se comparta a su personal o de manera equitativa se reparta; al compartir espacio sólo se le contabiliza al que comparte y no a los invitados (Actualmente es **NextCloud** la solución con que se trabaja).
6. Para solicitar una cuenta de **NextCloud** cada área deberá **solicitar de manera oficial** al DTIyT, para que este último realice un análisis completo del requerimiento: cantidad de espacio, número de usuarios, crecimiento y de acuerdo a la capacidad instalada en los servidores centrales se crearan los accesos correspondientes.
7. Al igual que el equipo propietario o arrendado, con respecta a la utilización de este espacio de respaldos, deberá ser únicamente para actividades relacionadas con los objetivos y metas de la institución. Por lo que no se deberá respaldar la siguiente información, de manera enunciativa más no limitativa: fotos personales, música, videos que no sean institucionales, software sin licencia.

8. El usuario final deberá almacenar la información que desee respaldar en las carpetas que le hayan sido asignadas y verificar que el respaldo se realizó con éxito, en caso de cualquier problema deberá informar a la Mesa de Ayuda establecida por la DTIyT para su atención.
9. Es **responsabilidad de cada usuario al que se le haya asignado una cuenta el buen uso** y confidencialidad de ella y en su caso notificar al DTIyT de su baja, recuperación o cambio si sospechara o se hubiera comprometido la seguridad de los accesos, además de notificar cuando haya algún movimiento de personal para dar de baja o modificar la cuenta.
10. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows de administradores estarán protegidas con contraseña. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas, sistemas o sesiones de Windows. Así como cualquier intento de vulnerar esta seguridad. El usuario final a cargo del equipo de cómputo deberá, en caso de detectar alguna modificación en claves, informar a la Mesa de Ayuda para su atención. Cuando exista un cambio en el personal deberán notificar al DTIyT de esto para que se realicen los cambios necesarios de accesos.
11. El DTIyT mensualmente realizará respaldos de las configuraciones de los conmutadores y firewalls de oficinas centrales.
12. Para el control de acceso a los sites y administración de los firewalls de oficinas centrales, se realizará cada 6 meses una depuración de accesos. Así mismo la baja inmediata cuando un elemento con acceso deja de laborar en el DTIyT.
13. Todos los archivos que viajen por correo y que contengan **información sensible** deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.
14. En caso de uso de memorias USB o discos externos, el usuario final deberá hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además, los usuarios pueden pedir apoyo al DTIyT para el uso de antivirus. En caso de no contar con antivirus el usuario deberá pedir a través de la Mesa de Ayuda su instalación o actualización.
15. El usuario deberá evitar conectar por iniciativa propia, algún dispositivo a la red (modem, Access point, switch, teléfono), que no esté autorizado y configurado por el personal del DTIyT.
    a. El DTIyT es el único autorizado para conectar cables UTP a la red. En caso de que el usuario compre o arme un cable, deberá informar al DTIyT para validar que esté bajo la norma establecida.
    b. Anualmente el DTIyT solicitará a la Dirección de Operación de Obra, Bienes, Servicios Generales y Procesos de Gestión se le otorgue mantenimiento preventivo (pintura, retenidas, anclas, dados, luces de destrucción) a las torres que tienen instalado equipo de comunicaciones de oficinas centrales.

Sobre el mantenimiento y buen uso de la infraestructura

16. Se podrá solicitar la instalación de software que cuente con **licencia adquirida** o si el software es Open Source o Freeware que su licencia permita su uso, el usuario final deberá informar al DTIyT de cualquier software que no cumpla con estos características, si requiriera algún software particular deberá presentar de manera oficial vía memorándum la solicitud de dictamen técnico al DTIyT para su valoración y si procediera, el usuario final deberá realizar la requisición para el proceso de adquisición.
17. Los equipos de toda los SSEP deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad. El usuario final en caso de no contar con ello deberá solicitar la vía oficial VoBo del DTIyT y una vez autorizado, elaborar su requerimiento al área encargada de compras.
18. Todos los servidores deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías. El DTIyT es el responsable de garantizar la operatividad de dichos equipos.

Sobre uso de Internet y Telefonía

19. El uso de internet queda reservado solo para **actividades propias de la institución**, por lo que no deberá realizar lo siguiente, de manera enunciativa más no limitativa: transmisión de video y/o música (streaming) páginas no oficiales, actividades personales, redes sociales siempre y cuando sea para difundir información oficial.
20. El DTIyT administra en oficinas centrales el filtrado de contenidos a través de un firewall, empleando niveles de privilegios mismos que son asignados previa autorización y justificación de jefes inmediatos.
21. Los aparatos telefónicos deberán emplearse única y exclusivamente para actividades relacionadas con los objetivos y metas de la institución.
    a. Cualquier desperfecto de aparato telefónico deberá notificarlo al DTIyT; el cual no reemplazará el equipo, en caso que en el diagnóstico se detecte mal uso o descuido del mismo.
    b. Se cuenta con tres niveles de privilegios mismos que son asignados acordes a las funciones y previa autorización del jefe superior inmediato

22. Toda actividad elaborada por el DTIyT deberá de estar debidamente registrada a través de la Mesa de Ayuda para darle seguimiento y que sirva como evidencia en los procesos de auditoria interna.