

"2022, Año de Ricardo Flores Magón"

Reglamento para el uso de equipos de cómputo Institucionales, portátiles y de escritorio

1. Todo empleado que requiera para sus labores un equipo de cómputo portátil o de escritorio, éste deberá contar con las siguientes características:
 - Sistema Operativo: Windows o en su caso IOS (MAC)
 - Herramientas Administrativas: Paquetería completa de Office, Adobe Reader, Chrome, Mozilla Firefox, Antivirus de uso Libre
 - Asignación de cuenta para correo electrónico Institucional
 - Asignación de Cuenta para acceso a Intranet (Sistemas Institucionales Internos)
 - Asignación de Cuenta para Acceso a Internet
2. El equipo de cómputo debe de usarse como una herramienta de apoyo relacionada con las funciones asignadas al cargo de cada trabajador.
3. El usuario final no deberá de mantener información personal dentro del Equipo Institucional
4. Es responsabilidad del usuario, hacer buen uso del equipo de Cómputo Asignado, así como la conservación, integridad y contenido de la información que se encuentra en los discos duros de los equipos asignados.
5. El uso del equipo de cómputo contempla emplear hardware y software que se encuentre instalado en los mismos, incluyendo el acceso a Internet, cuando se disponga de conexión a la red.
6. No instalar software sin licenciamiento o de fuentes desconocidas, ya que de ello derivan los principales ataques cibernéticos.
7. No compartir carpetas con información a menos que estas tengan algún tipo de cifrado o en su caso una VPN, que proteja la información dentro de la red.
8. Cada equipo de cómputo institucional debe de tener una contraseña asignada. No deben de estar sin contraseña para los inicios de sesión al mismo.

"2022, Año de Ricardo Flores Magón"

9. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones.
10. Mantener las cuentas de uso de sistemas internos resguardadas.
11. El uso de internet queda reservado solo para las actividades de trabajo que así lo requieran.
12. No guardar los inicios de sesión de los diferentes sistemas usados o páginas consultadas, ya que dicha información se puede extraer del equipo fácilmente. (Correo Electrónico, IMSS, INFONAVT, SIHAE, MICROSIP, REDES SOCIALES, ETC).
13. No acceder a sitios que marquen error de certificados o en su caso una página de color rojo indicando riesgo de seguridad.
14. Con respecto a los correos institucionales tener la cautela antes de abrir cada correo recibido, sobre todo verificar el remitente. El SPAM regularmente se identifica por ser correos con propagandas o iniciar con símbolos en el mensaje. Verificar asunto y Remitente.
15. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos como medida de seguridad de información y preferentemente asignarles una contraseña como capa adicional de seguridad.
16. El responsable de cada equipo de cómputo debe de reportar a la Subdirección de Tecnologías de la Información, Comunicación y Redes si detecta alguna anomalía con su equipo.
17. Permitir al personal de la Subdirección de Tecnologías de la Información, Comunicación y Redes llevar a cabo los mantenimientos programados a las áreas, estos pueden ser de Software y Hardware, así como de Respaldos de Información para evitar incidentes de pérdida de información

"2022, Año de Ricardo Flores Magón"

Atentamente

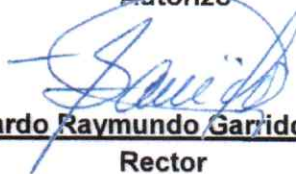
*"La causa de la educación tecnológica es una,
con el desarrollo sustentable"*

Elabro



Ing. Oscar Paulino Valdiviezo Trujillo
Subdirector de Tecnologías de la
Información, Comunicación y Redes

Autorizo



Dr. Eduardo Raymundo Garido Ramírez
Rector

