# Circular

**Estimados empleados**

Con el fin de fortalecer la seguridad de nuestros sistemas y proteger la integridad de la información confidencial del IHTT, se implementarán las siguientes políticas de seguridad:

1. **Sistema de directorio que organiza y administra los usuarios a nivel de Computadoras.**

   a) Sistema de directorio que organiza y administra los usuarios a nivel de Computadoras.
   b) Bloqueo de USB
   c) Monitoreo de las computadoras en el dominio Transporte.gob.hn, permitiendo la supervisión del estado de las computadoras y la integridad de la información.
   d) Cambio de contraseñas de uso obligatorio cada 90 días para todos los usuarios.
   e) Bloqueo de Acceso a Panel de Control y Configuraciones del Sistema Operativo.

**2. Antivirus y Firewall:**

   a) Se configurará el antivirus para realizar análisis de sistema completos periódicamente en todas las computadoras.

   b) El antivirus será configurado para controlar la ejecución de aplicaciones y el acceso a dispositivos periféricos.

   c) Filtrado de Correo Electrónico mediante el antivirus para detectar y bloquear correos electrónicos de phishing y malware.

   d) Todos los Dispositivos Móviles de la institución es obligatorio instalar el antivirus.

**3. Seguridad de Red:**

   a) Acceso Remoto para Trabajo en Casa deberán solicitarse mediante un memorando que incluya una justificación adecuada.

   b) Manipulación de switches de red, accesos WiFi y cámaras de seguridad: Únicamente el personal de soporte TICCA está autorizado para manipular.

   c) En caso de necesitar realizar alguna modificación, es imprescindible contar con la autorización por parte de la autoridad competente.

4. **Políticas de Comunicación y Operaciones:**
   a) Gestión de Actualizaciones se mantendrán todos los sistemas operativos y aplicaciones actualizados por lo que periódicamente se estarán aplicando en las PC.
   b) Copias de Seguridad regulares para todos los datos esenciales.
   c) Implementaremos capacitaciones para garantizar que todos los empleados estén preparados y actualizados en cuanto a las mejores prácticas de seguridad en línea.

      Esto significa que estaremos ofreciendo capacitación regularmente, con el objetivo de enseñarles cómo proteger nuestra información y sistemas contra posibles amenazas cibernéticas, como virus, ataques de phishing o robo de datos, todo esto nos fortalecerá la seguridad de la Institución.

Es fundamental que todos los empleados conozcan y cumplan estas políticas de seguridad para garantizar la protección de nuestros activos digitales.


Lic. Rafael Barahona
Comisionado Presidente