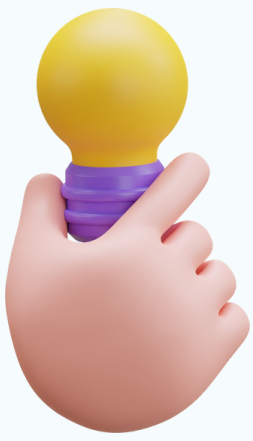
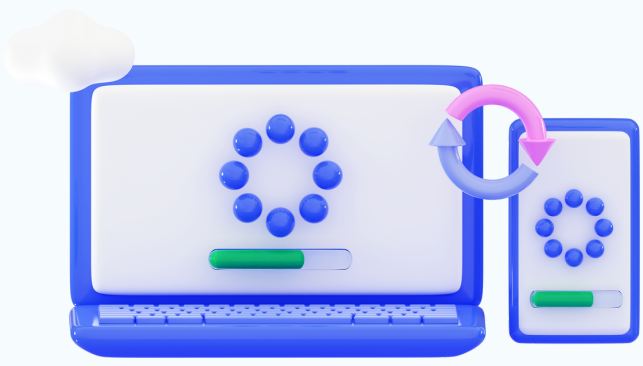


MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

CIBERSEGURIDAD PARA DISPOSITIVOS PORTÁTILES: MANTÉN TUS LAPTOPS Y MÓVILES PROTEGIDOS

BLOQUEA TU COMPUTADORA Y LAPTOP CUANDO NO ESTÉN EN USO

Establece contraseñas o utiliza métodos de autenticación biométrica, como el reconocimiento facial o la huella dactilar, para evitar el acceso no autorizado a tu laptop cuando no la estés utilizando.



MANTÉN TUS APLICACIONES Y SISTEMAS OPERATIVOS ACTUALIZADOS

Las actualizaciones regulares de software incluyen mejoras de seguridad importantes. Configura tu laptop para que se actualice automáticamente o verifica manualmente las actualizaciones disponibles y aplícalas tan pronto como sea posible.

UTILIZA UN SOFTWARE ANTIVIRUS CONFIABLE

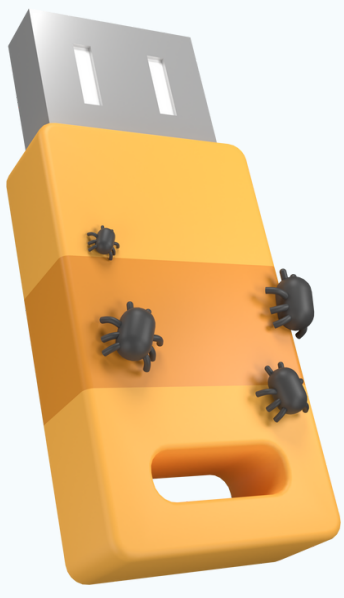
Instala un programa antivirus confiable en tu laptop y manténlo actualizado. Realiza análisis periódicos para detectar y eliminar posibles amenazas de malware.

DESCARGA E INSTALA PROGRAMAS SOLO DESDE FUENTES DE CONFIANZA

Evita descargar e instalar programas de origen desconocido o sitios web no confiables. Opta por fuentes oficiales y verificadas para reducir el riesgo de descargar software malicioso.

EVITA CONECTAR DISPOSITIVOS PORTÁTILES O DE ALMACENAMIENTO SIN PERMISO

No conectes dispositivos extraños, como unidades USB o discos duros externos, a tu laptop sin autorización. Estos dispositivos podrían contener malware que podría comprometer la seguridad de tu sistema.



CONFIGURA UN BLOQUEO DE PANTALLA SEGURO EN TU MÓVIL

Establece un PIN, patrón o contraseña para desbloquear tu dispositivo móvil. Esto brindará una capa adicional de seguridad en caso de pérdida o robo.

MANTÉN TUS APLICACIONES ACTUALIZADAS

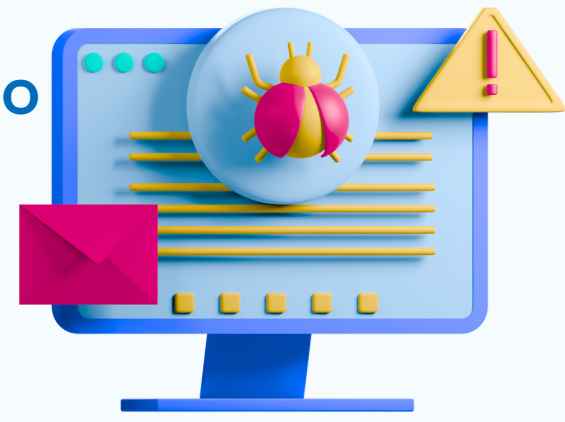
Las actualizaciones de las aplicaciones móviles a menudo incluyen correcciones de seguridad cruciales. Asegúrate de instalar las actualizaciones tan pronto como estén disponibles.

DESCARGA APLICACIONES SOLO DESDE TIENDAS OFICIALES Y CONFIABLES

Utiliza tiendas de aplicaciones oficiales, como Google Play Store o Apple App Store, para descargar aplicaciones en tu móvil. Estas plataformas suelen tener medidas de seguridad más rigurosas para proteger a los usuarios de aplicaciones maliciosas.

EVITA HACER CLIC EN ENLACES SOSPECHOSOS O ABRIR ARCHIVOS ADJUNTOS DE ORIGEN DESCONOCIDO

No hagas clic en enlaces sospechosos que recibas por correo electrónico, mensajes de texto o redes sociales. Del mismo modo, evita abrir archivos adjuntos de remitentes desconocidos, ya que podrían contener malware.



UTILIZA UNA SOLUCIÓN DE SEGURIDAD MÓVIL, COMO UN ANTIVIRUS O UNA APLICACIÓN DE SEGURIDAD

Evita descargar e instalar programas de origen desconocido o sitios web no confiables. Opta por fuentes oficiales y verificadas para reducir el riesgo de descargar software malicioso.

UTILIZA UNA RED WI-FI SEGURA

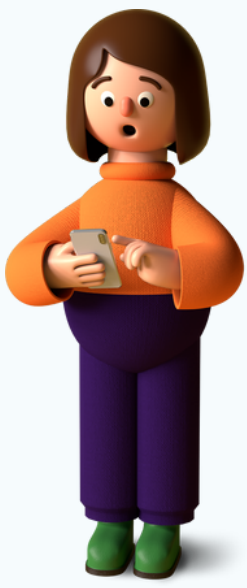
Evita conectarte a redes Wi-Fi públicas y no seguras, ya que pueden ser vulnerables a ataques cibernéticos.

SÉ CAUTELOSO CON LOS PERMISOS DE LAS APLICACIONES

Antes de descargar e instalar una aplicación, revisa cuidadosamente los permisos que solicita. Asegúrate de que los permisos sean coherentes con las funciones y características de la aplicación. Si una aplicación solicita permisos innecesarios o excesivos, considera no instalarla o buscar una alternativa más segura.

CONFIGURA EL BLOQUEO REMOTO Y LA ELIMINACIÓN DE DATOS

En caso de pérdida o robo de tu dispositivo móvil, habilita las opciones de bloqueo remoto y eliminación de datos. Esto te permitirá bloquear tu dispositivo de forma remota para evitar el acceso no autorizado y, si es necesario, borrar todos los datos de manera segura para proteger tu información personal.



www.micitt.go.cr

Más información

(506) 2539-2200

csirt@micitt.go.cr