

Protección de dispositivos, y seguridad de contenidos digitales

01 Utilizar contraseñas seguras y autenticación de dos factores

Disminuye la probabilidad de que alguien logre acceder a la información que se tiene en el dispositivo móvil, correo o equipo de cómputo.

También se recomienda activar el doble factor de autenticación, agregando una capa adicional de protección a través de dos distintos métodos, para validar tu identidad.



02 Realizar copias de seguridad



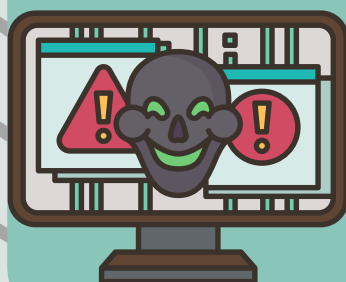
Permitirá tener la información disponible y actualizada, en caso de que el dispositivo móvil se extravíe, sea hurtado o dañado. Este proceso se puede realizar en la nube o en ordenadores de escritorio.

03 Gestión de permisos de aplicaciones móviles

Otorgar permisos puede dar acceso a ciberdelincuentes, a información privada, y a la de tus contactos. Por ello es importante verificar los datos asociados con tu identidad que te solicitan en las aplicaciones que descargas.



Evitar abrir archivos adjuntos y enlaces sospechosos 04



Ya que son una de las principales maneras en que un software malicioso puede entrar en dispositivos de todo tipo. Duda siempre de los enlaces que te envían. ¡No des clic!

05 Actualizar regularmente el sistema operativo y las aplicaciones móviles

Una versión obsoleta puede tener como consecuencia un dispositivo vulnerable a ciberataques que podrían poner en riesgo la seguridad del mismo.



06 Establecer la seguridad de correo electrónico

Este es una de las principales herramientas que utilizan los ciberdelincuentes para llevar a cabo ciberataques. Mantén una política de seguridad rigurosa, activando la protección avanzada para detectar, resolver amenazas y proteger la información confidencial, evitando así la pérdida de datos.

