



CHECK LIST DIGITAL

REGRESO A CLASES

Club de Ciberseguridad

En el retorno a clases del 2025, invitamos al club de ciberseguridad, compartir con pancartas, entrega de volantes, pequeñas charlas en ciertos salones o un espacio en el acto cívico del retorno a clases, compartir el **“Check List Digital de Regreso a Clases.”**.

Para **concienciar** a los niños, adolescentes, padres y tutores, a través de este mensaje, que fomente una cultura en ciberseguridad en nuestro entorno estudiantil.

Lista de recomendaciones:

1_ FORTALECER LOS VÍNCULO DE CONFIANZA

Mantener una comunicación constante con nuestros padres y tutores, sobre la vida digital que vamos desarrollando mientras crecemos, esto involucra los amigos que hacemos en las redes sociales y plataformas de juegos online.

2_ HABLAR CLARAMENTE SOBRE LOS DIVERSOS RIESGOS EN INTERNET

Compartir los diversos riesgos presentes en internet (ciberacoso, fraude, extorsión) las alertas y consecuencias que estas pueden ocasionar. Ante dudas, pregunta y busca apoyo con tus padres o tutores.

3_ COMPRENDER EL USO DE APLICACIONES DE CONTROL PARENTAL

Estos aplicativos especializados, sirven de apoyo a evitar el acceso a elementos de riesgos confirmados en internet. Por ellos es importante que como jóvenes, entendamos la importancia de su uso en nuestras vida.

4_ VERIFICAR LAS POLÍTICAS DE USO DE DISPOSITIVOS EN LA ESCUELA

Nuestra escuela cuenta con normas y responsabilidades digitales, verifica las políticas de ciberseguridad y fomenta su buen uso.



5_ **UTILIZAR CONTRASEÑAS SEGURAS PARA SUS DISPOSITIVOS**

Recuerda, que tus contraseñas son privadas, no debes compartirlas. Debes utilizar diversas contraseñas para tus cuentas digitales y también utilizar el multifactor de autenticación.

6_ **CUIDAR SU IDENTIDAD DIGITAL Y LA DE SUS COMPAÑEROS.**

Ser consiente de lo que compartes en redes sociales, “Piensa antes de enviar información personal” y evita compartir contenido privado. Tú identidad digital eres tú, así que es importante.

7_ **MANTENER ACTUALIZADO EL SISTEMA OPERATIVO DE SUS DISPOSITIVOS**

Verificar regularmente que el dispositivos y las aplicaciones cuenten con su última versión de actualización, así garantizamos que tengamos los parches de seguridad.

8_ **VERIFICAR LAS APLICACIONES QUE MANTIENEN EN SUS DISPOSITIVOS Y LOS PERMISO DE LOS MISMOS.**

Verificar las aplicaciones que mantengo en mi celular y los permisos que están disponibles para ellos, en caso que no se utilice un aplicativo, es recomendable eliminarlo.

9_ **SER PRECAVIDOS CON EL WI-FI DE LIBRE ACCESO.**

Aunque sea divertido utilizar el WiFi publico, seamos precavidos al utilizarlo, no ingresar a aplicativos bancarios o herramientas de uso personal o medico.

10_ **CONTAR CON COPIAS DE SEGURIDAD DEL COMPUTADOR**

Nuestro computador se puede dañar o ser infectado con algún virus, guarda siempre una copia de seguridad de los archivos importantes.



520-2378



info@panamacibersegura.gob.pa



www.panamacibersegura.gob.pa