Hoja

"Decálogo sobre Seguridad Digita"

Instrucciones para un mayor nivel de seguridad

- ✓ Elije una **contraseña** segura. Usa una combinación de al menos seis números, letras y signos de puntuación (como ! y &). La contraseña debe ser distinta de las otras que use en Internet.
- ✓ Cambia tu contraseña regularmente, sobre todo si ves un mensaje que te pide que lo hagas. Si la red social detecta que tu contraseña puede haber sido robada, cambiarla en ella y otros sitios te ayuda a proteger tu cuenta y prevenir ataques en el futuro.
- ✓ Nunca reveles tu contraseña a alguien que no conoces y en quien no confías.
- ✓ Asegúrate de que tu cuenta de correo está protegida. Puede que la gente que puede leer tu correo también pueda acceder a tu cuenta.
- ✓ Sal desconectándote (con *log-out*) de las redes sociales cuando uses un ordenador o teléfono inteligente que compartas con otros. No aceptes "Recuérdame" cuando inicias sesión en un ordenador público, dado que tu acceso se mantendrá incluso cuando cierres la ventana del navegador.
- ✓ Personaliza las opciones de privacidad de las redes sociales que usas.
- ✓ En algunas ocasiones puede ser útil seleccionar un modo de navegación anónimo o privado para proteger información bancaria para pagos o información personal, como detalles de inicio de sesión a las redes sociales, cuando el ordenador es usado para varias personas o tiene un riesgo grande de robo.
- ✓ Asegúrate de saber si tu cuenta es pública o privada y cómo se difunde el contenido.
- ✓ Apaga la función de geolocalización de tu teléfono inteligente si no quieres que otros sepan dónde estás.

Comportamientos adecuados

- ✓ Si alguien comparte fotos o vídeos que te hacen sentir incómodo, puedes dejar de seguir o bloquear a la persona que lo ha hecho. También pueden informar de contenido no adecuado directamente desde la aplicación si crees que viola sus principios.
- ✓ Asegúrate de que no tienes problemas si las fotos y vídeos que compartes muestran quién eres a mucho público, lo que incluye por ejemplo, tus padres, profesores o posibles jefes (futuros).
- ✓ Piensa con cuidado antes de autorizar terceras aplicaciones.
- ✓ Nunca aceptes hacer o compartir algo que te haga sentir incómodo.
- ✓ Si te están acosando, pide ayuda a un miembro de la familia o a un profesor en quien confíes. También puedes eliminar un comentario de una foto que compartas informar de actos de acoso e intimidación en las redes sociales (Centro de Ayuda)
- ✓ Pide permiso antes de publicar fotos con otras personas.