SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME MES DE JUNIO 2025

DE : Matías Estay Esquivel
Departamento de Informática
SECPLA

A : Miguel Muñoz Verdugo
Secretario Comunal de Planificación

Padre Hurtado, junio del 2025
En función del cometido descrito en antecedente, señalado:

1. **Enseñar practicas seguras de uso de internet y herramientas digitales para proteger la privacidad y seguridad de línea de los vecinos.**

2. **Colaborar en la creación y distribución de materiales educativos.**

A continuación, se presentan las acciones concretadas durante el periodo indicado, para los distintos cometidos asignados, perteneciente al programa de alfabetización digital:

1. **Enseñar practicas seguras de uso de internet y herramientas digitales para proteger la privacidad y seguridad de línea de los vecinos.**

Este manual es crucial porque, en nuestra comuna, todos usamos celulares y tablets para casi todo, desde comunicarnos hasta manejar nuestras finanzas. Esto nos hace vulnerables a ciberataques que pueden afectar nuestra información personal, nuestro dinero o nuestra privacidad. Este documento nos da las herramientas y el conocimiento para protegernos de estafas, virus y robos de datos, convirtiéndonos en usuarios digitales más conscientes y seguros. Es la clave para que, como vecinos de Padre Hurtado, podamos disfrutar de la tecnología sin preocupaciones.

2. **Colaborar en la creación y distribución de materiales educativos.**

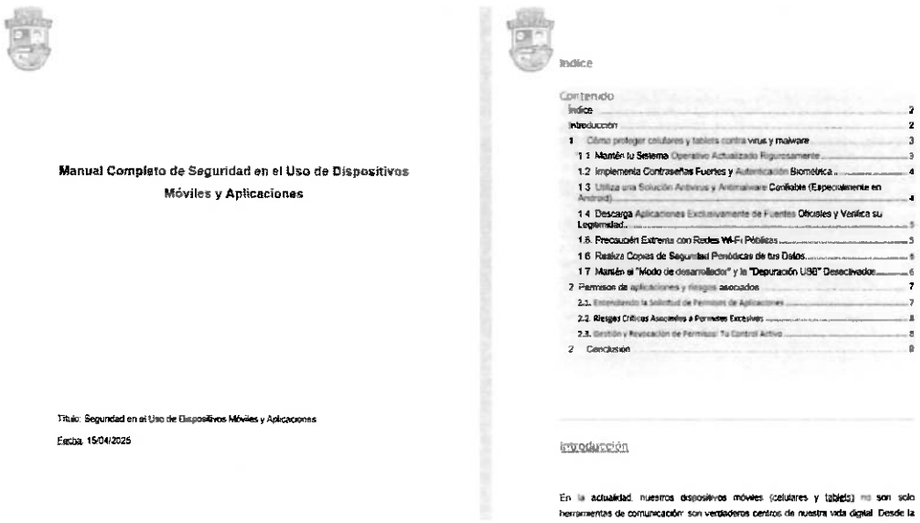
Mi rol es llevar esta información a nuestros hogares en Padre Hurtado de forma sencilla y directa.

- Enseñar prácticas seguras: Voy a mostrarles cómo mantener sus celulares actualizados, usar contraseñas robustas y huellas digitales, y descargar apps solo de las tiendas oficiales. También les advertiré sobre los peligros del Wi-Fi público y les enseñaré a revisar los permisos de sus aplicaciones para proteger su privacidad (ubicación, fotos, etc.).

- Crear y distribuir materiales: Para que el mensaje llegue, diseñaré infografías y videos cortos y atractivos, perfectos para compartir en nuestros grupos de WhatsApp y redes sociales vecinales. La idea es que la seguridad digital sea algo fácil de entender y aplicar por todos en la comuna.

[redacted]

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática



Manual Completo de Seguridad en el Uso de Dispositivos Móviles y Aplicaciones

Título: Seguridad en el Uso de Dispositivos Móviles y Aplicaciones

Fecha: 15/04/2025

Índice

Contenido

Introducción

En la actualidad, nuestros dispositivos móviles (celulares y tablets) no son solo herramientas de comunicación; son verdaderos centros de nuestra vida digital. Desde la

Los virus, el malware, el phishing y la suplantación de identidad no son exclusivos de las computadoras. Los dispositivos móviles son objetivos cada vez más atractivos para los ciberdelincuentes, quienes buscan explotar vulnerabilidades en el sistema operativo, en las aplicaciones o en los hábitos de los usuarios. Las consecuencias de una brecha de seguridad pueden ser devastadoras, incluyendo la pérdida de datos, el robo de identidad, el fraude financiero o la exposición de información privada.

Este manual completo ha sido diseñado para ser tu guía esencial en la protección de tus dispositivos móviles. Abordaremos en profundidad cómo blindar tus celulares y tablets contra el software malicioso y cómo entender y gestionar los permisos de las aplicaciones, un aspecto crucial a menudo subestimado. Al seguir estas directrices paso a paso, estarás equipando tus dispositivos y a ti mismo con las defensas necesarias para navegar por el ecosistema móvil de manera segura y confiada. La seguridad no es un acto único, sino una práctica continua.

1 Cómo proteger celulares y tablets contra virus y malware

Los virus y el malware (software malicioso) son programas diseñados con intenciones dañinas: robar información, dañar el sistema, espiar tus actividades o tomar control de tu dispositivo. Protegerte de estas amenazas requiere una combinación de buenas prácticas y herramientas de seguridad.

1.1 Mantén tu Sistema Operativo Actualizado Rigurosamente

Uno de los pilares de la seguridad móvil es mantener el **sistema operativo (SO)** de tu dispositivo al día. Los fabricantes (Apple para iOS, Google y fabricantes de Android) liberan constantemente **actualizaciones** que no solo añaden nuevas funciones, sino que, crucialmente, **corrigen vulnerabilidades de seguridad** descubiertas.

- **Paso 1: Habilita las actualizaciones automáticas.**
  - **En Android:** Navega a **"Configuración" > "Sistema" > "Actualización** asegura que recibas los parches de seguridad tan pronto como estén disponibles.
  - **En iOS (iPhone/iPad):** Ve a **"Configuración" > "General" > "Actualización de software"**. Dentro de esta sección, activa **"Actualizaciones automáticas"**. Podrás elegir si quieres descargar e instalar automáticamente o solo descargar y ser notificado para instalar manualmente. Se recomienda la opción de instalación automática.
- **Paso 2: Reinicia tu dispositivo regularmente.**
  - Aunque parezca trivial, un **reinicio periódico** (al menos una vez a la semana) no solo puede ayudar a aplicar actualizaciones que estén pendientes de instalación, sino que también limpia la memoria RAM, cierra procesos innecesarios y puede resolver pequeños fallos, contribuyendo a un mejor rendimiento y una mayor estabilidad del sistema operativo, lo que indirectamente mejora la seguridad.

1.2 Implementa Contraseñas Fuertes y Autenticación Biométrica

El acceso no autorizado a tu dispositivo es **la puerta de entrada** para cualquier ataque. Una buena estrategia de bloqueo es tu primera **línea de defensa**.

- **Paso 1: Configura un método de bloqueo robusto.**
  - **Evita el "deslizar para desbloquear"**. Utiliza siempre un **PIN** (de 6 dígitos o más, complejo, no secuencias como "123456" ni fechas de nacimiento), un **patrón** (que no sea obvio como una "L" o una "Z" y que no se vea fácilmente por manchas en la pantalla) o, idealmente, una **contraseña alfanumérica** compleja (que combine letras mayúsculas y minúsculas, números y símbolos).
  - Para configurarlo:
    - **En Android:** **"Configuración" > "Seguridad y privacidad" > "Bloqueo de pantalla"** o **"Tipo de bloqueo de pantalla"**.
    - **En iOS:** **"Configuración" > "Face ID y código"** o **"Touch ID y código"**.
- **Paso 2: Habilita la autenticación biométrica.**
  - La mayoría de los dispositivos modernos ofrecen **lector de huellas dactilares** o **reconocimiento facial (Face ID/Touch ID)**. Estas tecnologías son rápidas, convenientes y, lo más importante, mucho más seguras que los métodos tradicionales si se configuran correctamente. Asegúrate de que estén activadas y funcionando eficientemente como complemento o alternativa a tu código.

1.3 Utiliza una Solución Antivirus y Antimalware Confiable (Especialmente en Android)

Aunque iOS es conocido por su ecosistema más "cerrado" y, por lo tanto, menos vulnerable al malware directo, los dispositivos Android, debido a su naturaleza más abierta, pueden beneficiarse enormemente de una **aplicación antivirus y antimalware de buena reputación**.

Sin otro particular, se despide atentamente,

[redacted]

varro
l.t.s
LT
tado

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME FINAL ENERO-JUNIO 2025

DE : **Matías Estay Esquivel**
Departamento de Informática
SECPLA

A : **Miguel Muñoz Verdugo**
Secretario Comunal de Planificación

En función del cometido descrito en antecedente, señalado:

1. **Enseñar practicas seguras de uso de internet y herramientas digitales para proteger la privacidad y seguridad de línea de los vecinos.**

2. **Colaborar en la creación y distribución de materiales educativos.**

A continuación, se presentan las acciones concretadas durante el periodo entre **ENERO – JUNIO**, para los distintos cometidos asignados, perteneciente al programa de alfabetización digital:

Enero: El mes de enero se realizó un manual de prevención de fraudes donde se explicaba la importancia de tener verificaciones, ocultar bien los datos personales y evitar entrar a sitios sospechosos.

Febrero: En febrero se llevó a cabo un manual sobre la seguridad de los datos personales en sí, ya que muchos adultos mayores dentro de nuestra comuna pueden llegar a pasar por alto alguna información o que tienen que hacer en caso de que se les llegue a filtrar algún tipo de información.

Marzo: En Marzo se realizó un manual el cual se explica y se mensiona la importancia de crear una contraseña segura para prevenir filtraciones, que tenga problemas de privacidad entre otras cosas, una contraseña segura puede ayudar bastante al momento de tener tus datos bien seguros.

Abril: En Abril se realizó un manual de cómo prevenir las estafas que suelen ocurrir ya sea telefónicamente como las que podemos encontrar en correo electrónico, aplicaciones móviles como Instagram, whatsapp, etc.

Mayo: En mayo se realizó un manual explicativo sobre el buen uso de las redes sociales, ya que para un usuario que no esté muy entendido de las redes, puede ser algo muy peligroso, ya sea por filtración de información o los mismos fraudes que anteriormente se realizaron manuales.

Junio: En el mes de junio se realizó un manual el cual nos ayuda ha explicar y dar a entender que la seguridad ya sea de teléfonos y tablets es importante, evitar la piratería, descargar aplicaciones de sus tiendas o paginas oficiales, además de tener cierta segurdad financiera ya que a dia de hoy todo el mundo o la gran mayoría cuenta con sus tarjetas en los teléfonos.

Teniendo en cuenta todos los meses, se realizaron diversos manuales en relación a la ciberseguridad y el uso seguro de la información de cada uno, de las redes sociales y de los mismos dispositivos, estos manuales todos han sido subidos en la intranet de la municipalidad.

[redacted]

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Sin otro particular, se despide atentamente,

[redacted]

[redacted]