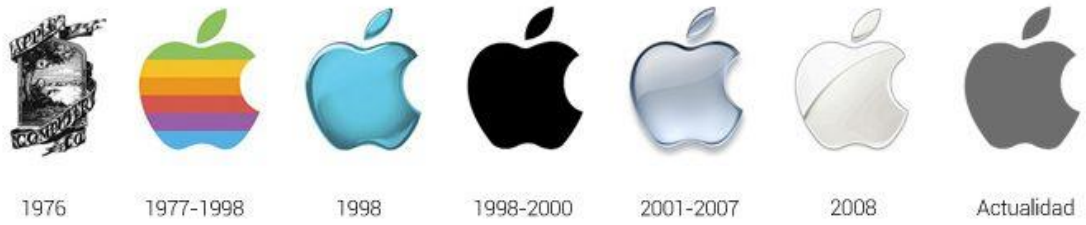
RESUMEN FINAL DEL CURSO: PUNTOS MÁS RELEVANTES

A lo largo de este curso hemos visto diferentes aspectos relacionados con dispositivos iOS. Hemos conocido la historia de Apple y la evolución del sistema operativo iOS. Aquí se destacan hitos importantes desde la fundación de Apple en 1976, el lanzamiento de productos icónicos como el iPod y el iPhone, hasta las diversas versiones del sistema operativo iOS, cada una con sus características y mejoras.



De igual forma se ha profundizado en medidas de seguridad específicas para dispositivos iOS. Estas medidas incluyen el uso de métodos de bloqueo (Face ID y Touch ID), activación de actualizaciones automáticas, utilización de aplicaciones de seguridad, realización de copias de seguridad, desactivación de conexiones inalámbricas cuando no se usan, revisión de permisos de aplicaciones, evitar el jailbreak, y restaurar los valores de fábrica antes de deshacerse del dispositivo.

A lo largo de los diferentes módulos hemos analizado las medidas de seguridad y protección de la privacidad integradas en los dispositivos iOS, con un enfoque en evitar el acceso no autorizado a la información almacenada.

Algunos aspectos que han sido analizados han sido medidas de seguridad y protección:

1. **Protección de Acceso Físico**: Uso de códigos, Touch ID y Face ID para proteger el acceso al dispositivo.
2. **Seguridad del Apple ID**: Importancia de una contraseña segura y la autenticación de doble factor.
3. **Buscar mi iPhone**: Uso de la aplicación para localizar, bloquear o borrar remotamente un dispositivo perdido o robado.
4. **Cómo Actuar en Caso de Robo**: Pasos a seguir, incluyendo el bloqueo remoto y la notificación a las autoridades.
5. **Borrado Remoto**: Funcionalidad para eliminar toda la información del dispositivo de forma remota.

Medidas de acceso físico al dispositivo:

- **Mediante Código**: Configuración y cambio de códigos en el dispositivo.
- **Touch ID**: Uso del sensor de huella dactilar para acceder al dispositivo y realizar compras.
- **Face ID**: Reconocimiento facial para desbloquear el dispositivo y acceder a servicios.

Medidas de seguridad del Apple ID:

- **Definición y Funciones**: El ID de Apple permite el acceso a diversos servicios de Apple, protegiendo la privacidad y sincronizando datos entre dispositivos.
- **Consejos de Seguridad**: No compartir el ID de Apple, usar autenticación de doble factor y crear contraseñas seguras.

De igual forma se han analizado aspectos como usar la aplicación “Buscar mi iPhone” o pasos a seguir en caso de pérdida o robo. El borrado remoto del dispositivo también ha sido objeto de interés en el curso.

El uso y la configuración segura de iCloud, el servicio de almacenamiento en la nube de Apple son aspectos que también han sido tratados en diversos módulos.

Ya en el ecuador del contenido se realiza una exposición completa sobre la creación, gestión y protección de contraseñas. A continuación, se presenta un resumen de los puntos clave abordados:

- **Importancia de las Contraseñas**: Las contraseñas son esenciales para proteger nuestra información personal y evitar el acceso no autorizado a servicios como redes sociales, correos electrónicos y banca online.
- **Reglas Básicas para Contraseñas Seguras**:
  - Crear contraseñas robustas con minúsculas, mayúsculas, números y caracteres especiales.
  - Usar frases largas y fáciles de recordar (mínimo 10 caracteres).
  - Evitar contraseñas fáciles de adivinar (fechas de nacimiento, nombres, secuencias comunes).
  - No reutilizar contraseñas en diferentes servicios.

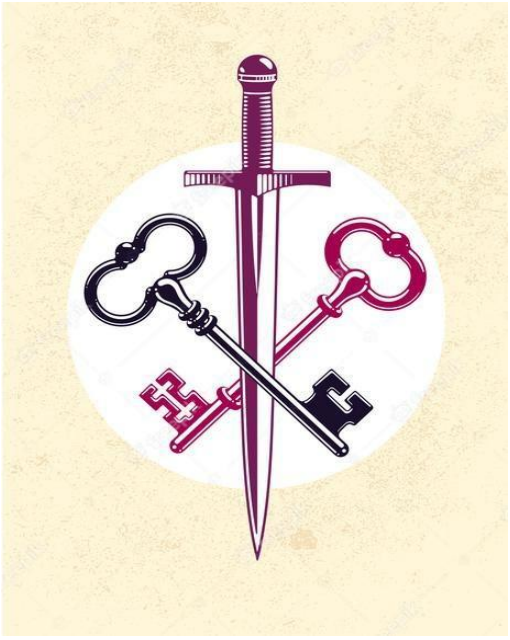
- **No Compartir Contraseñas**: Mantener las contraseñas en secreto para proteger la privacidad.
- **Contraseñas Robustas**: Deben tener al menos 8 caracteres y una combinación de diferentes tipos de caracteres.
- **Preguntas de Seguridad**: Usar respuestas complejas o falsas que solo el usuario conozca.

- **Función del Llavero de iCloud**: Almacena contraseñas, números de tarjetas de crédito, contraseñas Wi-Fi, cuentas de Internet y formularios web. Se sincroniza entre dispositivos Apple con el mismo ID de Apple.

- **Protección de la Información**: Usa cifrado completo y autenticación de dos factores para proteger los datos.
- **Desactivación del Llavero**: Implica que las contraseñas no se sincronizarán entre dispositivos, pero seguirán protegidas localmente.
- **Activación del Llavero**: Se puede activar desde la aplicación Ajustes en el dispositivo iOS.
- **Configuración en Dispositivos Adicionales**: Requiere aprobación desde otro dispositivo con el llavero activo o mediante el código de seguridad de iCloud.

- Aplicaciones que almacenan y gestionan credenciales en una base de datos cifrada accesible mediante una contraseña maestra.
- **Funciones Comunes**:
    - Acceso online y offline.
    - Verificación en dos pasos.
    - Sincronización multidispositivo.
    - Generación automática de contraseñas.
    - Alertas de vulnerabilidad.

- **Ver y Editar Contraseñas Guardadas**: Accesible desde Ajustes > Contraseñas en dispositivos iOS.
- **Recomendaciones de Seguridad**: Alertas sobre contraseñas débiles o reutilizadas.



También ha centrado la atención del curso las amenazas cibernéticas comunes que enfrentan los usuarios de dispositivos móviles y cómo protegerse de ellas.

Aspectos como la ciberdelincuencia, gestión de malware, técnicas de ingeniería social, jailbreak y el uso seguro de aplicaciones de pagos como Apple Pay son importantes y han centrado la atención del curso.

Otro de los aspectos tratados son las diferentes tecnologías inalámbricas disponibles en dispositivos iOS, cómo utilizarlas de manera segura y prácticas recomendadas para proteger la información personal.

La gestión segura de aplicaciones y permisos en dispositivos iOS es otro de los temas importantes que debes recordar, ya que te ayudará a conocer cuáles son las mejores recomendaciones para dar permisos a aplicaciones y los riesgos asociados en cada caso.

También habrás conocido los pasos a seguir para la configuración de la actualizaciones automáticas y manuales y la importancia de desinstalar las aplicaciones que no uses habitualmente.

La protección de la privacidad en dispositivos iOS, y cómo gestionar la información personal y los permisos de aplicaciones es también considerado al final del curso, junto con el control de la privacidad.

Confiamos en que este curso te haya ayudado a tener un mejor conocimiento de tu dispositivo iOS, y sobre todo hacer un uso responsable y seguro del mismo.