UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escola Tècnica Superior d'Enginyeria **Informàtica**

2. Ataques a soluciones móviles y cuidados a adoptar

Ciberseguridad en Dispositivos móviles
DISCA – ETS de Ingeniería informática (UPV)

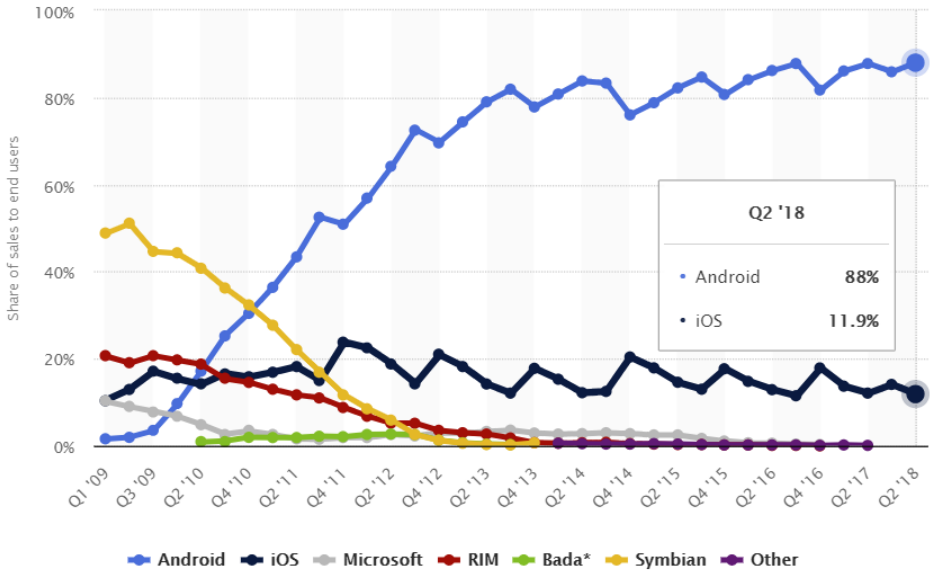
Indice

- Situación actual del parque móvil
- Ataques a dispositivos y aplicaciones móviles
- Listado de cuidados (no exhaustivo y, de momento, poco técnico) que podemos adoptar

Situación actual

Technology & Telecommunications › Telecommunications › Global market share held by smartphone operating systems 2009-2018, by qua... PREMIUM

Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 2nd quarter 2018



DOWNLOAD SETTINGS SHARE

PNG PDF XLS PPT

CITATION (FAQ)

Select citation

DESCRIPTION SOURCE MORE INFORMATION

This statistic shows the global market share held by the leading smartphone operating systems, in terms of sales to end users, from 2009 to 2018. In the second quarter of 2018, 88 percent of all smartphones sold to end users were phones with the Android operating system.

Smartphone operating systems - additional information

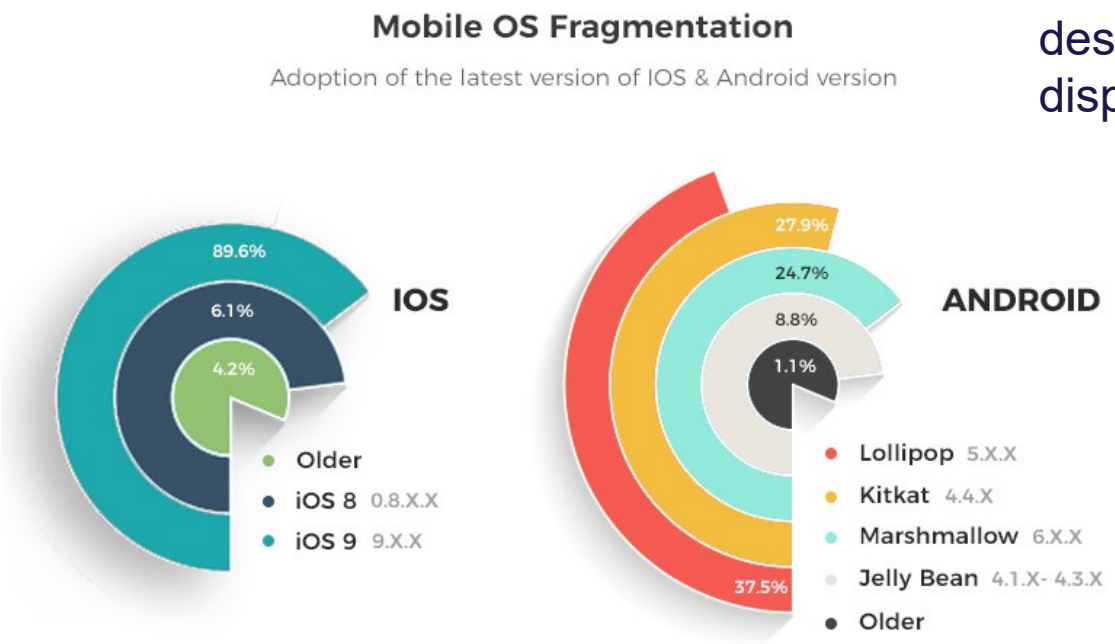
Smartphone operating systems, often referred to as smartphone OS, are operating systems that operate smartphones, PDAs, tablets and other mobile devices.

Additional Information: Worldwide; Gartner; 2009 to 2018

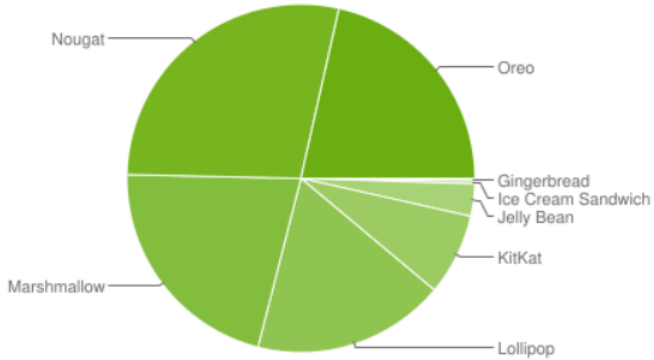
Source: Gartner

Android vs iOS

- La fragmentación supone todo un desafío para la seguridad de los dispositivos móviles



(Actualización de datos para 2018 en el caso de Android)

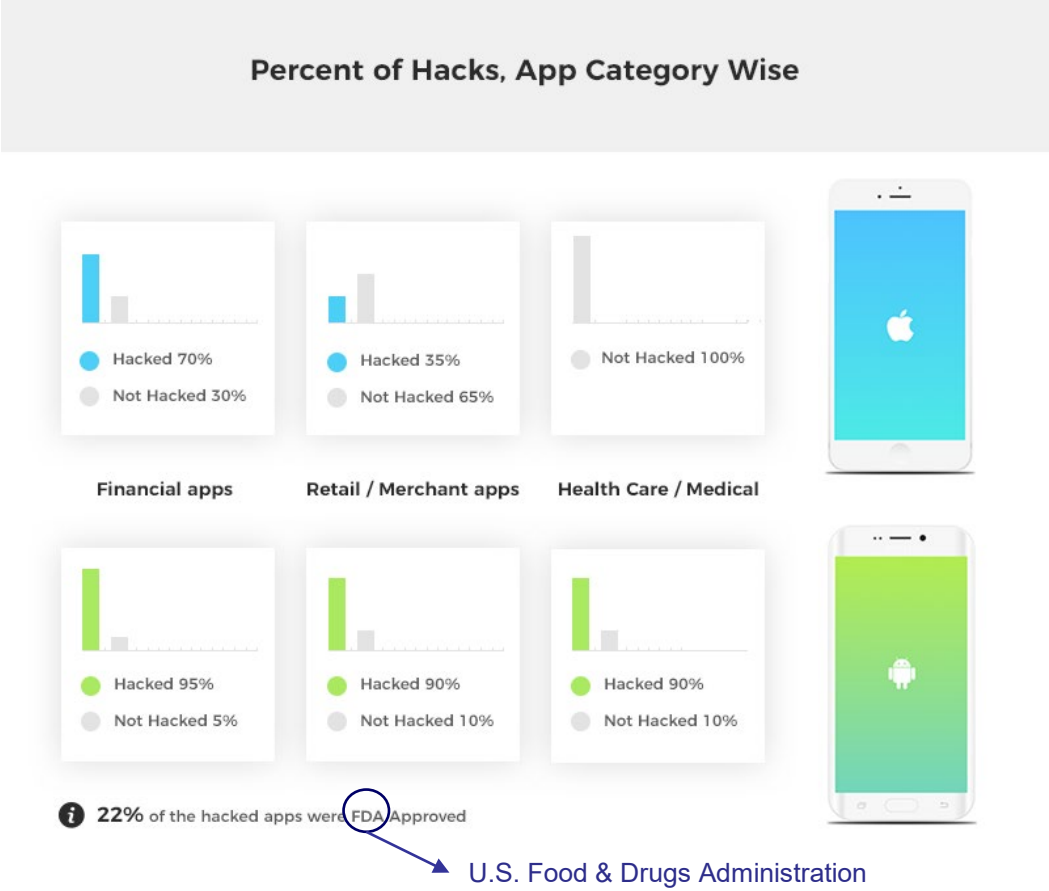


Datos recopilados durante un período de 7 días hasta 26/10/2018.
No se muestran versiones con una distribución inferior al 0,1%.

- Contrariamente a iOS, en Android las actualizaciones dependen de los fabricantes de dispositivos

Android vs iOS

Android vs iOS

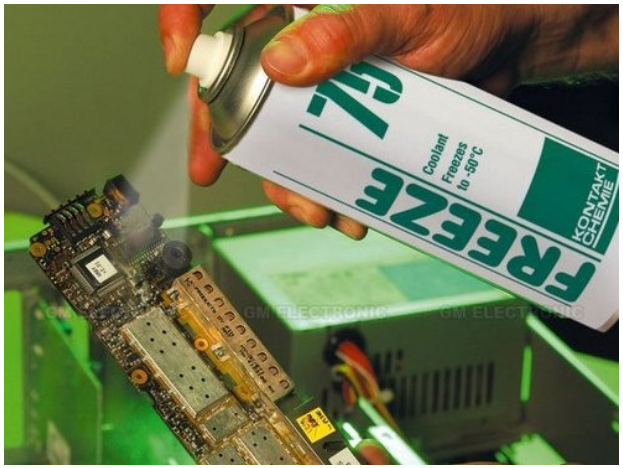


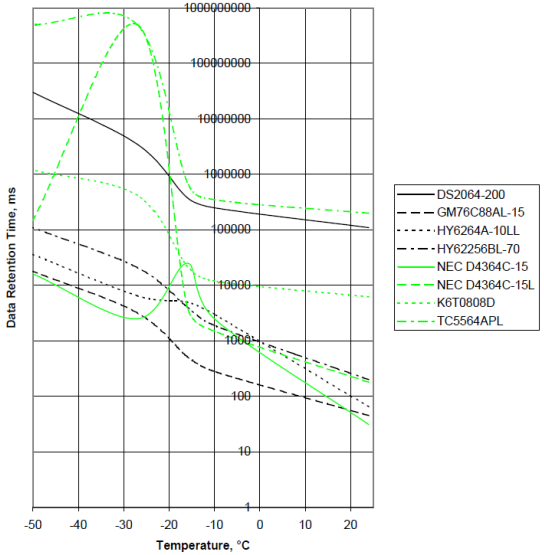
Indice

- Situación actual del parque móvil
- **Ataques a dispositivos y aplicaciones móviles**
- Listado de cuidados (no exhaustivo y, de momento, poco técnico) que podemos adoptar

Cool Boot Attack

- La memoria RAM de un dispositivo necesita de electricidad para su persistencia
  - Cuando el dispositivo se apaga, la corriente eléctrica deja de fluir por el circuito y los datos se pierden poco a poco
- Se aprovecha un hecho físico: la temperatura del dispositivo tiene un gran efecto sobre la velocidad de borrado de la RAM (a menor temperatura más tiempo tarda en borrarse)
- Aplica a memorias SRAM, EEPROM y Flash





Android *Cool Boot Attack*

Se introduce el teléfono bloqueado en un congelador a -15 ºC durante 1 hora.

Una vez extraído, se enchufa a un equipo mediante una conexión USB y se reinicia

Antes de cargar el sistema operativo principal, mediante la conexión USB se carga el un módulo de arranque que lee los contenidos de la memoria RAM y permite extraer contraseñas y cualquier otro dato almacenado en la memoria.

Más información en: https://www1.informatik.uni-erlangen.de/frost

iPhone Passcode bypass

- El borrado automático del dispositivo no siempre funciona …

Hardware

https://www.youtube.com/watch?v=meEyYFISahk

- A través de la conexión USB se prueban todas las claves de 4 dígitos.
- Un sensor de luz detecta si la clave introducida es correcta.
- Si no lo es, se apaga el dispositivo rápidamente para que no se borre automáticamente tras llegar al límite de intentos.
- 40 segundos por clave, hasta 111 horas para probar todas las claves.

Software

http://www.iphonehacks.com/2015/03/iphone-passcode-bypassed-bruteforce-tool.html

- Solución similar, pero que funciona únicamente en dispositivos con *jailbreak* y versiones del operativo que soporte códigos de acceso de 4 dígitos.
- En este caso, necesita únicamente 5 segundos por clave.

Vulnerabilidad UPnP

- Vulnerabilidad de aplicación

Las librerías UPnP se utilizan para el *streaming* de vídeo entre dispositivos.
Existen más de 6 millones de dispositivos con estas librerías en sus aplicaciones: TV, *smartphones*, etc.
La vulnerabilidad permitía ejecutar código arbitrario en un dispositivo con una de estas librerías instalada.

- Vulnerabilidad corregida en 2012
- En Diciembre de 2015 existían dispositivos que seguían utilizando la versión vulnerable de la librería (fuente: blog.trendmicro.com) → 547 apps de las que 326 disponibles en Google Play

http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability

Aplicaciones de parking

- Vulnerabilidad de aplicación

Una auditoria de seguridad detectó que múltiples aplicaciones para el pago del parking en Reino Unido tenían vulnerabilidades que permitían conocer la localización y credenciales del usuario. Al parecer, aunque la mayoría de las apps comprometidas utilizaban como protocolo a nivel de transporte TLS (Transport Layer Security), ninguna de ellas verificaba el certificado utilizado por el servidor, lo que las hacía vulnerables a ataques de tipo man-in-the-middle. Es cierto que, al no servir conexiones WiFi, sino GSM, la superficie de ataque no era tan amplia, pero un atacante podría utilizar una estación base GSM falsa y perpetrar el ataque.

http://www.theregister.co.uk/2015/12/11/mobile_parking_apps_audit

Aplicaciones móviles Bancarias

- Sector financiero

Análisis de 40 aplicaciones bancarias en 2014 para iOS disponible en https://ioactive.com/personal-banking-apps-leak-info-through-phone

Resultados muy significativos:

- Menos del 20% no contaban con mecanismos de protección de pila (Stack smashing protection) ni aleatorización (ALSR) de memoria o PIE (Position Independent Executable) con lo que eran altamente sensibles a fallos de corrupción de memoria
- El 20% enviaba información sensible (códigos de activación de las cuentas) sin cifrar a través de la red
- El 30% tenía las credenciales escritas directamente en el código.
- El 40% filtraba información sensible a través de los log
- El 40% no validaba correctamente los certificados SSL
- El 50% de las aplicaciones analizadas eran vulnerables a *Cross-Site Scripting* en el lado del cliente
- El 90% comunicaban usando enlaces sin cifrado SSL lo que permitía ataques de man-in-the-middle

Fake WhatsApp

- Hacer dinero mediante publicidad

A finales del 2017, un app llamada “Update WhatsApp Messenger”, clasificada con una puntuación de 4.2 estrellas, obtuvo más de 1.000.000 de descargas. La app utilizaba el logo oficial de WhatsApp y en su descripción aparecía desarrollada por WhastApp Inc. Esto se consiguió utilizando como nombre de la app el string “WhatsApp+Inc%C2%A0” (C2A0 = No-break Space). Sólo solicitaba permisos de accesos a internet para su instalación y se comportaba como un cargador que instalaba la apk “whatsapp.apk”. Una vez instalada esta apk se obtenían las credenciales de WhastApp de los usuarios e instalaba en el dispositivo un servicio (sin icono, ni título en la pantalla lanzadera) que mostraban publicidad con cierta frecuencia.

https://lifehacker.com/watch-out-for-this-fake-whatsapp-app-in-the-google-play-1820222637

CryptoHacking en Apps

- Uso de apps para minar criptomonedas

En 2017 y 2018, se encontraron apps que reducían (a veces) significativamente la duración de la batería de los dispositivos en los que se instalaban. Tras analizarlas se comprobó que estas apps se servían de la CPU de los dispositivos en los que se instalaban para minar criptomonedas, es decir verificar transacciones de criptomonedas dentro de un blockchain. Como recompensa, los nodos recibían una cantidad concreta de la criptomoneda que estén minando. Obviamente los beneficiarios no eran los propios dispositivos, sino el nodo que designaba el atacante que ha diseñado el troyano.
Señalar que el minado de criptomonedas no es ilegal, lo que es ilegal es hacerlo fraudulentamente, es decir, sin el consentimiento del usuario. Aunque en Julio del 2017 Google prohibió este tipo de apps, a lo largo de 2018 aún se han detectado varias de ellas todavía disponibles en Google Play en apps de Juego y entretenimiento. A esto se le llama **cryptohacking**.

https://computerhoy.com/noticias/internet/que-es-cryptohacking-como-evitar-que-minen-bitcoins-tu-pc-71675

CopyCat

- Infección masiva de malware

Malware que instala apps sin permiso y genera beneficios a sus creadores instalando apps de terceros y modificando el código de identificación utilizado por el Adware de las apps. Así es como los se generaban ingresos ilícitos para sus creadores.
El malware se propagó desde tiendas de apps no oficiales, camuflado bajo la denominación de apps desconocidas.
Infectó 14 millones de dispositivos (sólo el 7% de ellos son europeos), de los cuales 8 millones resultaron finalmente rooteados
Se estima que los responsables ganaron 1,5 millones de dólares

https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world

Versión Copycat de Wannacry

- Ransomware en dispositivos móviles

De nombre *Wannalocker*, se trata de un malware que en 2017 infectó a muchos móviles Android en China. Se distribuyó a través de foros de juegos como un plugin para el popular juego Chino *King of Glory* (un clon de *League of Legends*). El malware ocultaba su icono y reemplazaba el fondo de pantalla por una imagen animada. No sólo cifraba la información almacenada en el dispositivo, sino la de cualquier dispositivo de almacenamiento externo al que éste se conectara. El método de cifrado era AES. Se solicitaba un rescate de sólo 5 a 6 USD, que se podían pagar por QQ, Alipay y WeChat, con lo que los pagos eran rastreables. Es un ejemplo de ransomware en el que se busca hacer dinero rápidamente.

https://blog.avast.com/wannacry-wannabe-targeting-android-smartphones
https://androidphoria.com/juegos/descargar-king-of-glory-clon-league-of-legends-android

Android/TimpDoor

- Malware que transforma los dispositivos móviles en proxies ocultos
  - Uso de Smishing, es decir de ataques de tipo Phishing utilizando mensajes de texto, o SMS, en lugar de emails
    - En el mensaje se informa a los usuarios sobre la existencia de dos mensajes en el buzón de voz
    - Al acceder al mismo se instala una app de mensajería (VoiceApp.apk) fraudulenta
    - Al escuchar los mensajes se instala un servicio (malware) en segundo plano. Este servicio instala una alarma en el dispositivo para, regularmente, subir información del mismo a la red, filtrando así Contactos, SMSs, localizaciones, imágenes, logs, etc.
    - El código ejecutado es el que se muestra

```
this.mHandler.postDelayed(new Runnable() {
    public void run() {
        AppService.this.startSsh();
        AppService.this.startNetworkConnectionMonitor();
        AppService.this.setupAlarmManager();
        AppService.this.startPoolSshConnection();
    }
}, 3000);
```

  - El malware puede evadir algunas medidas de seguridad instaladas en el dispositivo al redireccionar tráfico cifrado a un servidor saltándose el firewall y el IDS existente
  - Malware actualmente en desarrollo … con lo que la historia continuará
    - https://medium.com/@sapnagupta279796/be-aware-android-timpdoor-turns-androids-into-cryptic-proxies-a1591f5bcfc0
    - https://exchange.xforce.ibmcloud.com/collection/AndroidTimpDoor-Turns-Mobile-Devices-Into-Hidden-Proxies-a82dde9a4383fd3ac55f653c4b60b3cf

FaceTime

- Violación de privacidad

Un error en la programación de sistema de video-llamada FaceTime permitía a cualquiera escuchar a su interlocutor antes de que éste aceptara la comunicación.
Esto ocurría si el que llamaba se añadía a la conversación antes de que el llamado descolgara.
Si además el llamado colgaba al audio transmitido se le añadía vídeo.

https://www.theverge.com/2019/1/29/18201667/apple-group-facetime-disabled-server-side-major-security-flaw-fix

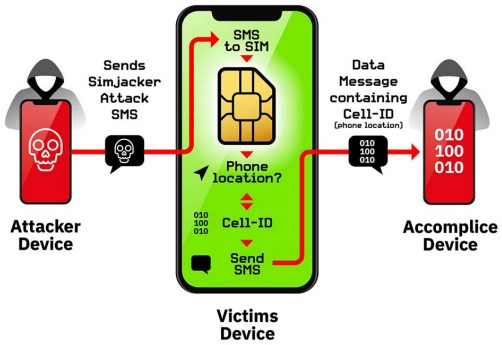
Apps con geolocalización

- Los datos de geolocalización, obtenidos tanto por las plataformas móviles como por apps de terceros, siguen siendo un **elemento muy preciado** para múltiples propósitos, incluyendo
  - Servicios que utiliza el usuario y sus funcionalidades extra (mapas, navegación, servicios en redes sociales, actividad física, fotografías, localización y estado de negocios cercanos, navegación en interiores, etc.),
  - Comercialización de anuncios personalizados y basados en la ubicación,
  - Comercialización de los propios datos de localización, etc.
- En 2018, la app de actividad física y deportiva Strava, que se vio expuesta y permitió identificar numerosas localizaciones sensibles, como las utilizadas por los servicios de inteligencia y operativos militares en todo el mundo, incluyendo bases militares secretas

https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

SIMJacker

- **Vulnerabilidad crítica en nuestras tarjetas SIM** que permite a un atacante remoto hackear móviles y espiarnos tan sólo enviando un SMS
  - El estándar de las tarjetas SIM lleva 10 años sin actualizarse
  - Ataca a una parte del software llamada S@T Browser (SIMalliance Toolbox Browser).
    - Esta herramienta añade diversas funcionalidades para los operadores, pudiendo gestionar servicios, suscripciones u otros servicios
    - Para operar, contiene una serie de instrucciones, como enviar un mensaje corto, establecer una llamada, lanzar el navegador, ejecutar un comando o enviar datos, los cuales pueden ser activados enviando un SMS al dispositivo
    - Gracias a ello, un atacante tiene un entorno de ejecución a su disposición para ejecutar órdenes



  - https://www.adslzone.net/2019/09/12/simjacker

Indice

- Situación actual del parque móvil
- Ataques a dispositivos y aplicaciones móviles
- **Listado de cuidados (no exhaustivo y, de momento, poco técnico) que podemos adoptar**

Necesidad de una higiene digital

- Se trabaja poco la higiene digital a nivel social → Muchos conocemos lo que hay que hacer, pero pocos lo hacemos
- ¿***Qué cuidados debemos tener en cuenta*** para poder estar seguros al utilizar un dispositivo móvil?

Antes de adquirir un dispositivo

- Observar los mecanismos de seguridad disponibles
  - Diferentes modelos y fabricantes
  - Incluir la seguridad en nuestra decisión
- En caso de escoger un dispositivo que ya ha sido usado restablecer las configuraciones de fábrica antes de utilizarlo
- No adquirir dispositivos:
  - desbloqueados ilegalmente (jailbreak)
  - con los permisos de acceso modificados
    - acción ilegal
    - violación de los términos de la garantía
    - seguridad comprometida
    - funcionamiento comprometido

Al usar un dispositivo (1/4)

- Instalar mecanismos de seguridad y mantenerlos actualizados
  - antivirus (se debe instalara antes que cualquier otra aplicación)
  - antispam
  - antimalware
  - firewall personal
- Mantener nuestro dispositivo seguro:
  - instalando las versiones más recientes de todos los programas
  - instalando todas las actualizaciones del sistema
- No hacer clic ni seguir enlaces recibidos en mensajes electrónicos
  - SMS, mensajes de correo electrónico, redes sociales, etc.

Al usar un dispositivo (2/4)

- Mantener el control físico del dispositivo
  - especialmente en lugares de riesgo
  - no dejar el dispositivo sobre la mesa
  - cuidado con los bolsos y las carteras en los lugares públicos
- Proteger nuestra privacidad → cuidado con:
  - publicar datos de geolocalización
  - permitir que una aplicación acceda a tus datos personales

Al usar un dispositivo (3/4)

- Protejamos nuestras contraseñas
  - utilicemos contraseñas bien elaboradas
  - de ser posible, configurar el dispositivo para que acepte contraseñas complejas (alfanuméricas)
  - utilizar contraseñas largas y con diferentes tipos de caracteres
  - No utilizar:
    - secuencias de teclado
    - datos personales, como nuestro nombre, apellido o fechas importantes
    - datos personales que se puedan obtener fácilmente

Al usar un dispositivo (4/4)

- Proteger nuestros datos:
  - Configurar el acceso al dispositivo con:
    - una contraseña de bloqueo en la pantalla de inicio
    - un código PIN
    - información biométrica
    - si es posible, con una combinación de mecanismos
  - Realizar copias de seguridad periódicas
  - almacenar la información sensible en formato encriptado
  - si la comunicación incluye datos confidenciales, utilizar una conexión segura
    - contraseñas
    - número de una tarjeta de crédito

Al instalar aplicaciones

- Buscar aplicaciones de fuentes confiables
  - tiendas confiables
  - sitio del fabricante
- Escoger aplicaciones:
  - bien evaluadas
  - con una gran cantidad de usuarios
- Antes de instalar la aplicación, verificarla con un antivirus
- Observar los permisos de ejecución
  - estos permisos deben ser coherentes con la finalidad de la aplicación
  - por ejemplo, la aplicación de un juego no necesariamente necesita acceder a nuestra lista de llamadas

Al conectarnos a una red

- Tener cuidado al utilizar redes Wi-Fi públicas
  - deshabilitar la opción de conexión automática
- Mantener desactivadas las interfaces de comunicación
  - bluetooth, infrarrojo y Wi-Fi
  - habilitarlas solo cuando sea necesario
- Configurar la conexión bluetooth para que el dispositivo no pueda ser identificado (o "descubierto") por otros dispositivos

Al deshacerse del dispositivo

- Eliminar toda la información almacenada
- Restablecer la configuración de fábrica

En caso de pérdida o robo (1/2)

- De ser posible, configurar previamente el aparato:
  - para que permita localizarlo/rastrearlo y bloquearlo de manera remota, mediante servicios de geolocalización
  - para que en la pantalla muestre un mensaje que permita aumentar las probabilidades de devolución
  - para que aumente el volumen o salga del modo silencioso y facilitar así su localización en caso de extravío
  - para que los datos se borren después de un determinado número de intentos de desbloqueo fallidos
    - **Cuidado**: especialmente si hay niños pequeños a quienes les gusta "jugar" con el dispositivo

En caso de pérdida o robo (2/2)

- Informar:
  - al operador → solicitar el bloqueo del número (chip)
  - la empresa donde trabajamos → si el dispositivo haya información sensible (contraseñas, documentos, imágenes, etc.)
- Modificar las contraseñas que puedan estar guardadas en el dispositivo
- Bloquear las tarjetas de crédito cuyo número esté almacenado en el dispositivo
- Si está configurada, activar la localización remota → de ser necesario, borrar remotamente la información guardada en el dispositivo

Qué hace único a "*lo móvil*"…

Dispositivos móviles habitualmente compartidos

- Uso familiar de teléfonos y tables
- Uso de los dispositivos de la empresa entre distintos empleados
- Uso y organización de apps vs explorador de archivos

Uso de multiples perfiles

- Herramienta de trabajo
- Dispositivo de entretenimiento
- Organización personal
- ¿Perfil de seguridad por perfil?

Dispositivos diversos (fragmentación)

.

- Sector inmaduro para la gestión de empresa
- BYOD dicta el uso de distintos OSs
- Fabricantes/vende-dores /operadores controlan el mercado e imponen sus reglas

Utilización en multiples localizaciones

- Se puede disponer en una misma localización de conexiones publica, privada o celular
- Ubiquidad (Anywhere, anytime)
- Confianza creciente en la WiFi de la empresas

Se le da prioridad y protagonismo al usuario

- Se cuida la experiencia de usuario
- La arquitectura del OS proporciona el control al usuario
- Dificultad de imponer políticas o lista de apps

"Por qué iba alguien a limitar la funcionalidad de estos dispositivos?"

Aspectos positivos

1. Permite la integración de forma sencilla de plataformas ya existentes en las organizaciones. De esta manera se evitan acciones con riesgo para la organización cuando se trabaja desde un dispositivo móvil propio
   - Ejemplo: Uso de MS Office Mobile que permite sincronizar los documentos a través de OneDrive. Así no se necesita extraer los datos de la organización (mediante USB o email personal)
2. Los dispositivos móviles ya incluyen muchas características de seguridad por defecto que, en sistemas de escritorio, deben ser implementados mediante herramientas de terceros
   - Ejemplo: Mecanismos de cifrado de disco, autenticación biométrica …
3. El sistema operativo está diseñado para aislar unas aplicaciones de otras. De esta manera, si hay un problema de seguridad en una app, éste no debería afectar a las demás.

Aspectos negativos

1. Los smartphones suponen un nuevo vector de ataque a través del cuál es posible conseguir el acceso a una organización
   - Ejemplo: Almacenamos mucha información personal en nuestros dispositivos móviles, como credenciales de acceso → Necesidad de protección
2. Existe una dualidad entre dispositivos que pertenecen a la organización y los personales de los empleados
   - Ejemplo: Las políticas de BYOD intentan mitigar este problema
3. En el caso de que esté aprobado el uso del dispositivo personal en la organización, hay veces que el acceso por parte de terceros de confianza puede poner en riesgo la información de la organización
   - Ejemplo: Envío de información sensible a través de cuentas de trabajo por equivocación de miembros de la familia que utilizan el dispositivo esporádicamente