

Espiar y atacar a un organismo
a través de los móviles:
mucho más sencillo de lo que pensamos.
Solo existe una forma eficaz de evitarlo



Daniel González

dgonzalez@mobileiron.com

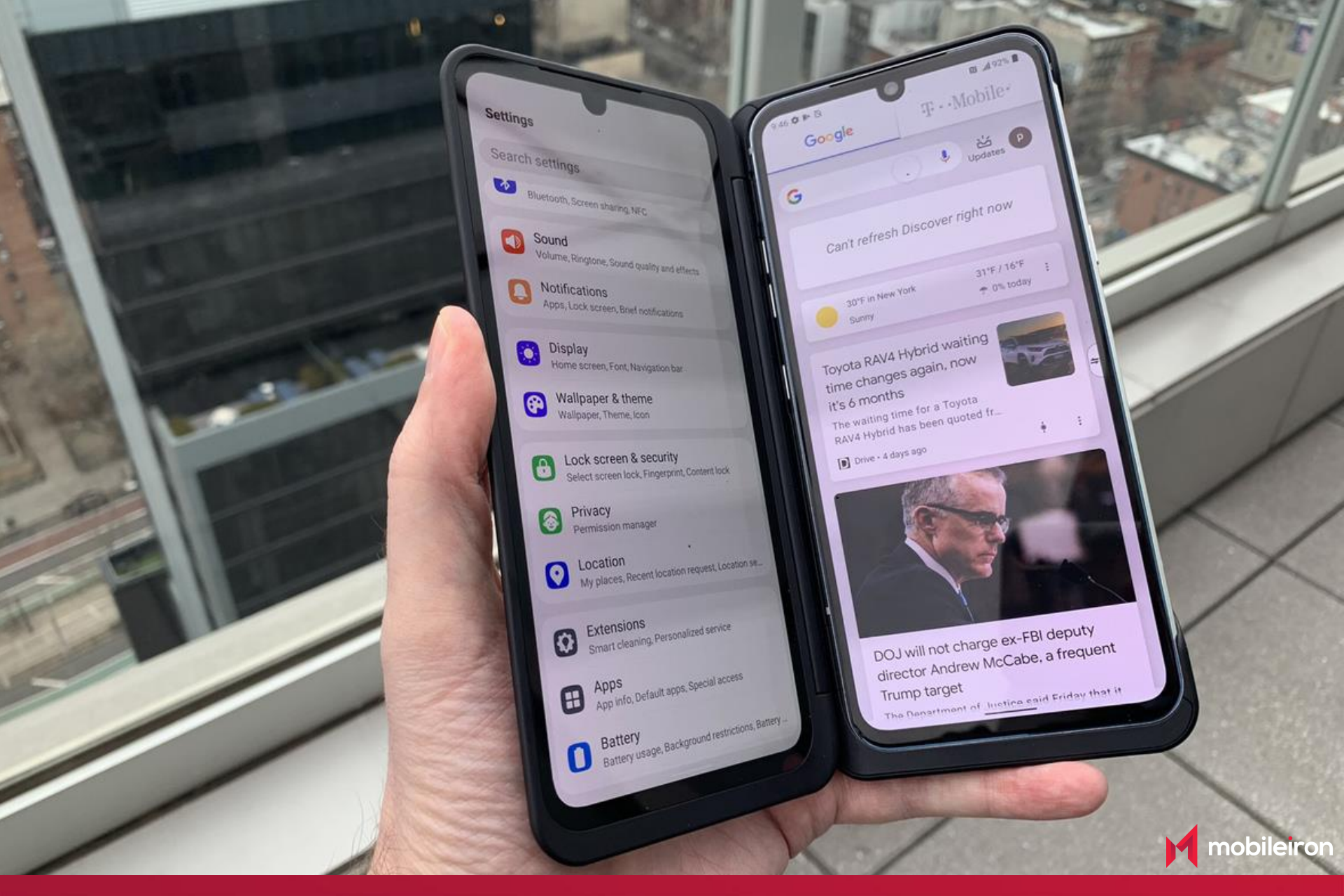
[606.64.55.00](tel:606.64.55.00)



An aerial, high-angle photograph of a busy city intersection at night. The scene is filled with a large crowd of pedestrians crossing the street, illuminated by streetlights. Several cars are visible on the roads, and the surrounding buildings are lit up, creating a vibrant urban atmosphere. The image serves as a background for the text.

¿ Teléfono móvil ?

¿ Smartphone ?



Settings

Search settings



Bluetooth, Screen sharing, NFC



Sound

Volume, Ringtone, Sound quality and effects



Notifications

Apps, Lock screen, Brief notifications



Display

Home screen, Font, Navigation bar



Wallpaper & theme

Wallpaper, Theme, Icon



Lock screen & security

Select screen lock, Fingerprint, Content lock



Privacy

Permission manager



Location

My places, Recent location request, Location se...



Extensions

Smart cleaning, Personalized service



Apps

App info, Default apps, Special access



Battery

Battery usage, Background restrictions, Battery ...

Google

T-Mobile

Updates

Can't refresh Discover right now

30°F in New York
Sunny

31°F / 16°F
0% today

Toyota RAV4 Hybrid waiting
time changes again, now
it's 6 months
The waiting time for a Toyota
RAV4 Hybrid has been quoted fr...

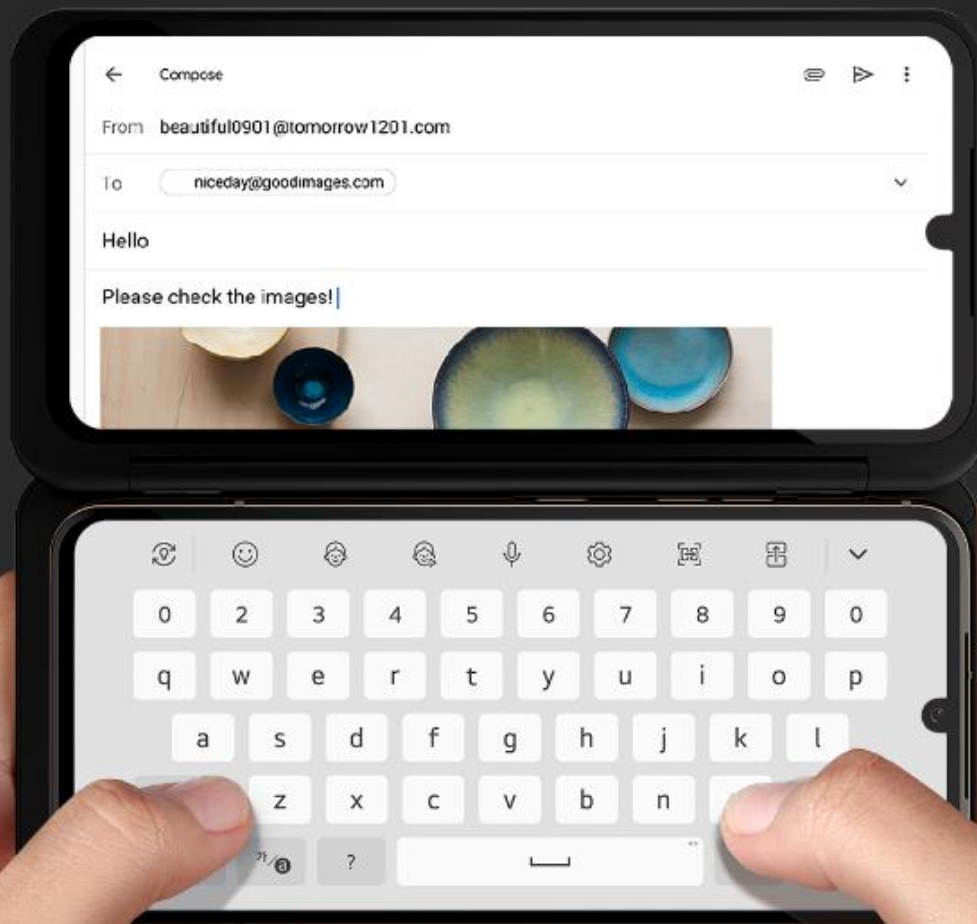


Drive • 4 days ago



DOJ will not charge ex-FBI deputy
director Andrew McCabe, a frequent
Trump target

The Department of Justice said Friday that it





¿ Teléfono móvil ?

¿ Smartphone ?



¿Cuántos ordenadores tiene
en su organismo sin protección?

El “ordenador de bolsillo” tiene acceso a ...

CRM

Intranet

Correo electrónico

Directorio corporativo

ERP

Mensajería instantánea

Multi-conferencia

Servidor de ficheros



**Qué nos ha llevado
a estas situaciones**

¿Qué tienen en común todos estos casos?

EL PAÍS ESPAÑA

WhatsApp confirma el ataque al móvil del presidente del Parlamento catalán

La aplicación de mensajería acreditada por primera vez que el teléfono de Roger Torrent fue víctima de un "intento de acceso no autorizado" en 2019

PERIODISTAS Y POLÍTICOS PODRÍAN HABER SIDO ESPIADOS EN LA JOYA DE LA CORONA DE CIUDADANOS

Escrito por TransMurcia | Mar 28, 2019 | ACTUALIDAD, NACIONAL | 0 | ★★★★★

El error deja a los iPhones vulnerables a los piratas informáticos que roban el contenido del correo electrónico

Una falla en la aplicación de correo incorporada podría permitir a los atacantes leer, modificar o eliminar correos electrónicos, dicen los expertos

El Confidencial

Fallo de ciberseguridad en Palacio: Strava revela las rutas de 'running' en La Zarzuela

Un buen 'zoom' al mapa de calor global publicado por la empresa estadounidense muestra con precisión las rutas que se realizan dentro de la residencia de los reyes de España



BUSINESS INSIDER

La policía detecta intentos de ciberdelincuentes por atacar el sistema informático de hospitales en plena crisis del coronavirus

Alberto R. Aguilar | 23 Mar 2020 13:39h



Alerta por 'phishing': el CNI investiga el hackeo de los móviles de varios ministros y altos cargos del Gobierno

Sofía Sánchez | 20 Ago 2020 11:25h

LA VANGUARDIA | Política

Defensa comunica a la Fiscalía un posible ataque a su red informática interna

En 2018 se registraron aproximadamente 34.000 ciberincidentes de diverso tipo en entidades del sector público y empresas de interés estratégico

EL PAÍS

ANDALUCÍA CATALUÑA C. VALENCIANA GALICIA MADRID PAÍS VASCO ÚLTIMAS NOTICIAS

El ataque a los móviles de Torrent y Maragall con un programa espía israelí desata una tormenta política

Interior, Policía y Guardia Civil aseguran que no contrataron los servicios de la empresa NSO



El Confidencial

La ministra de Exteriores también fue víctima de 'hackeo' del móvil

Arancha González Laya sufrió el mismo ataque a su teléfono que otros altos cargos y el ministro de Justicia, Juan Carlos Campo



Vulnerabilidad en WhatsApp permite instalar spyware en teléfonos con solo realizar una llamada

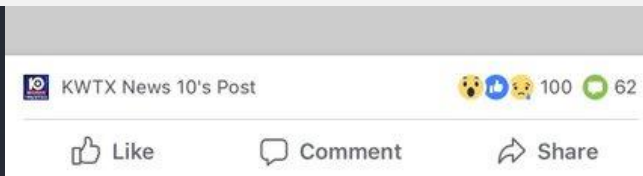
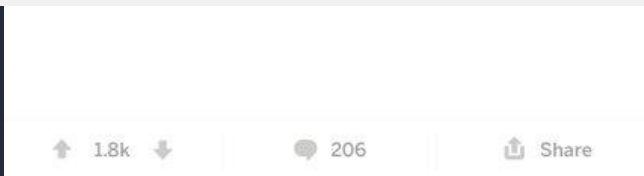
El fallo, que afecta tanto a usuarios de Android como de iOS, ya fue reparado en la última actualización que lanzó WhatsApp



Juan Manuel Harán 14 May 2019 - 04:01PM



Ejemplo de suplantación del departamento de seguridad de Apple



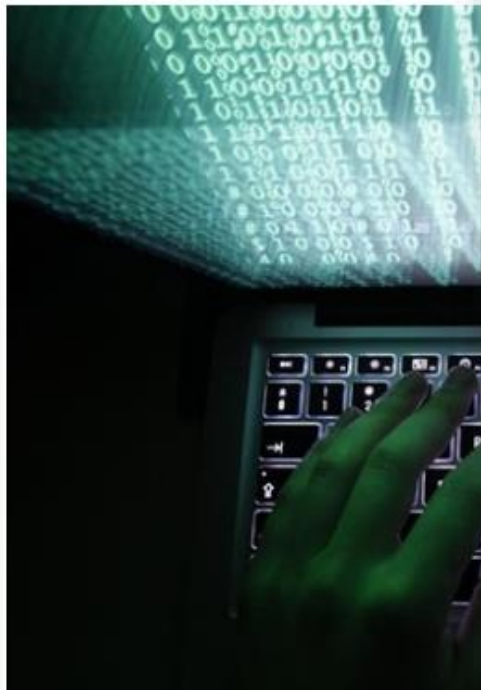
¿Cómo pueden ser espiados políticos, periodistas o famosos a través de sus móviles?



Las amenazas más peligrosas para los dispositivos móviles en la actualidad son:

- **Trojanos móviles de acceso remoto (mRATs):** Dan la capacidad de obtener de forma remota el acceso a todo lo almacenado, pudiendo infectar tanto sistemas Android como iOS. En dispositivos Android se infectan a través de las aplicaciones del 'marketplace' de Google y los iOS son igualmente vulnerables a través del método 'jailbreak'.
- **Ataques WiFi Man-in-the-Middle (MitM):** Ocurren cuando un dispositivo se conecta a un punto de acceso WiFi que ha sido infectado. El atacante se hace con las comunicaciones y puede escuchar de forma secreta e incluso alterar la comunicación de la red.
- **Ataques de día cero:** Suponen la explotación de ciertas vulnerabilidades, tanto en iOS como Android, que aún no han sido publicadas. Una vez en el dispositivo, el atacante puede robar contraseñas, datos corporativos y correos electrónicos, así como recoger información de actividad del teclado y pantalla.
- **Explotación de privilegios en Android:** Las vulnerabilidades de Android pueden ser explotadas para obtener altos privilegios sin dejar rastro, como sucedió con la vulnerabilidad 'Certifi-gate' que afectó a cientos de millones de dispositivos el pasado verano. Los ataques se aprovechan de las oportunidades creadas por la fragmentación de Android.
- **Certificados iOS falsos:** Usan certificados de distribución para hacer 'sideloading' de una aplicación, dejando a un lado el proceso de validación oficial de la tienda de aplicaciones de Apple mediante una descarga directa en el dispositivo.
- **Perfiles iOS maliciosos:** Utilizan los permisos de perfil para eludir los mecanismos de seguridad típicos, permitiendo, por ejemplo, que el atacante modifique el recorrido del tráfico de un usuario desde el dispositivo móvil a un servidor controlado por él.
- **Vulnerabilidades en WebKit de iOS:** Permiten a los navegadores web renderizar las páginas de forma correcta para un usuario. Los ciberdelincuentes las explotan para ejecutar 'scripts' propios, dejando a un lado las robustas medidas de seguridad implementadas por Apple.

¿Cómo pueden ser famosos a través de



Las amenazas más peligrosas para los dispositivos móviles en la actualidad son:

- **Trojanos móviles de acceso remoto (mRATs):** Dan la capacidad de obtener de forma remota el acceso a todo lo almacenado, pudiendo infectar tanto sistemas Android como iOS. En dispositivos Android se infectan a través de las aplicaciones del 'marketplace' de Google y los iOS son igualmente vulnerables a través del método 'jailbreak'.
- **Ataques WiFi Man-in-the-Middle (MitM):** Ocurren cuando un dispositivo se conecta a un punto de acceso WiFi que ha sido infectado. El atacante se hace con las comunicaciones y puede escuchar de forma secreta e incluso alterar la comunicación de la red.
- **Ataques de día cero:** Suponen la explotación de ciertas vulnerabilidades, tanto en iOS como Android, que aún no han sido publicadas. Una vez en el dispositivo, el atacante puede robar contraseñas, datos corporativos y correos electrónicos, así como recoger información de actividad del teclado y pantalla.
- **Explotación de privilegios en Android:** Las vulnerabilidades de Android pueden ser explotadas para obtener altos privilegios sin dejar rastro, como sucedió con la vulnerabilidad 'Certifi-gate' que afectó a cientos de millones de dispositivos el pasado verano. Los ataques se aprovechan de las oportunidades creadas por la fragmentación de Android.
- **Certificados iOS falsos:** Usan certificados de distribución para hacer 'sideloading' de una aplicación, dejando a un lado el proceso de validación oficial de la tienda de aplicaciones de Apple mediante una descarga directa en el dispositivo.
- **Perfiles iOS maliciosos:** Utilizan los permisos de perfil para eludir los mecanismos de seguridad típicos, permitiendo, por ejemplo, que el atacante modifique el recorrido del tráfico de un usuario desde el dispositivo móvil a un servidor controlado por él.
- **Vulnerabilidades en WebKit de iOS:** Permiten a los navegadores web renderizar las páginas de forma correcta para un usuario. Los ciberdelincuentes las explotan para ejecutar 'scripts' propios, dejando a un lado las robustas medidas de seguridad implementadas por Apple.



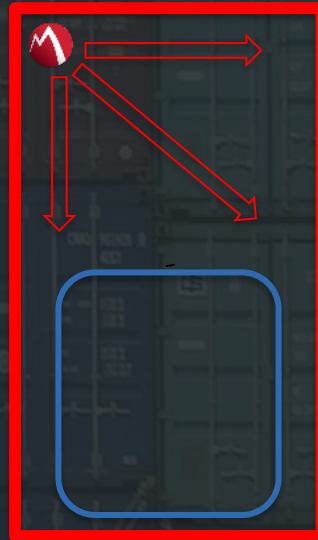
¿Proteger los datos corporativos y la privacidad del usuario?

Los sistemas operativos están preparados para separar contenido personal y laboral.

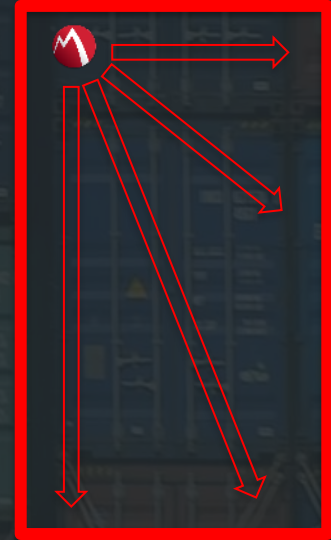
BYOD



COPE



COSU



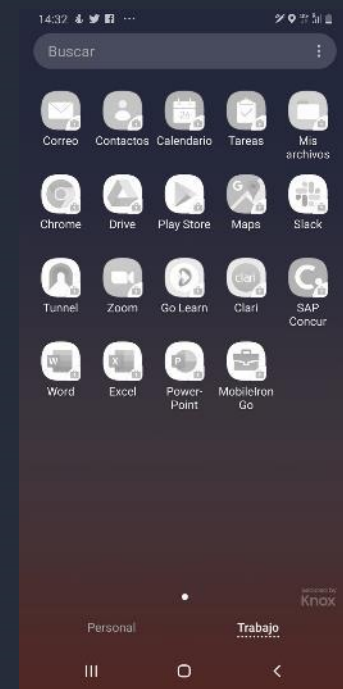
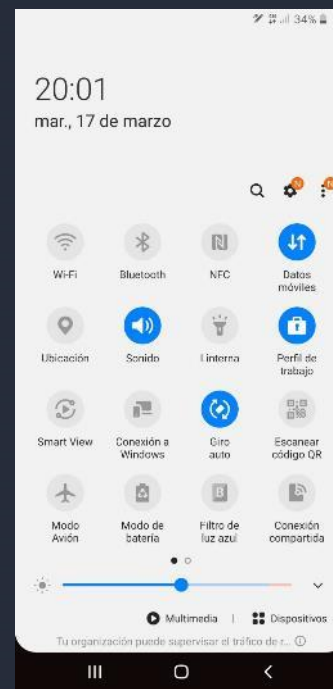
 Usuario

 Empresa

BYOD – Dispositivo propiedad del usuario

Coxx – Dispositivo propiedad del organismo

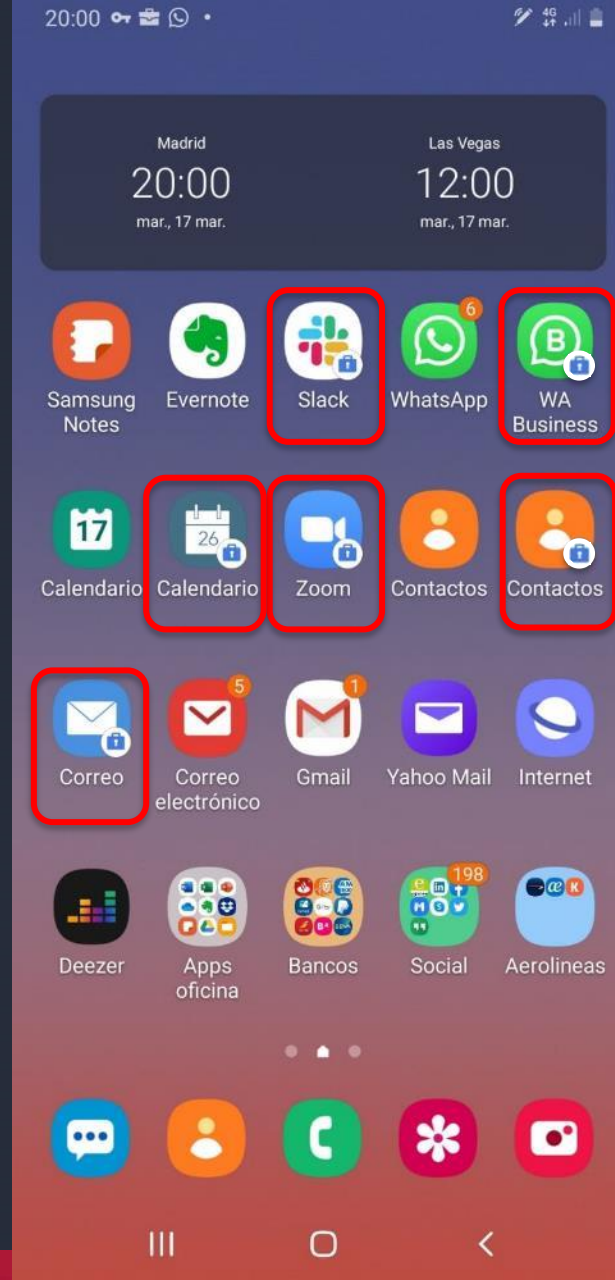
Veamos un ejemplo



Escritorio principal

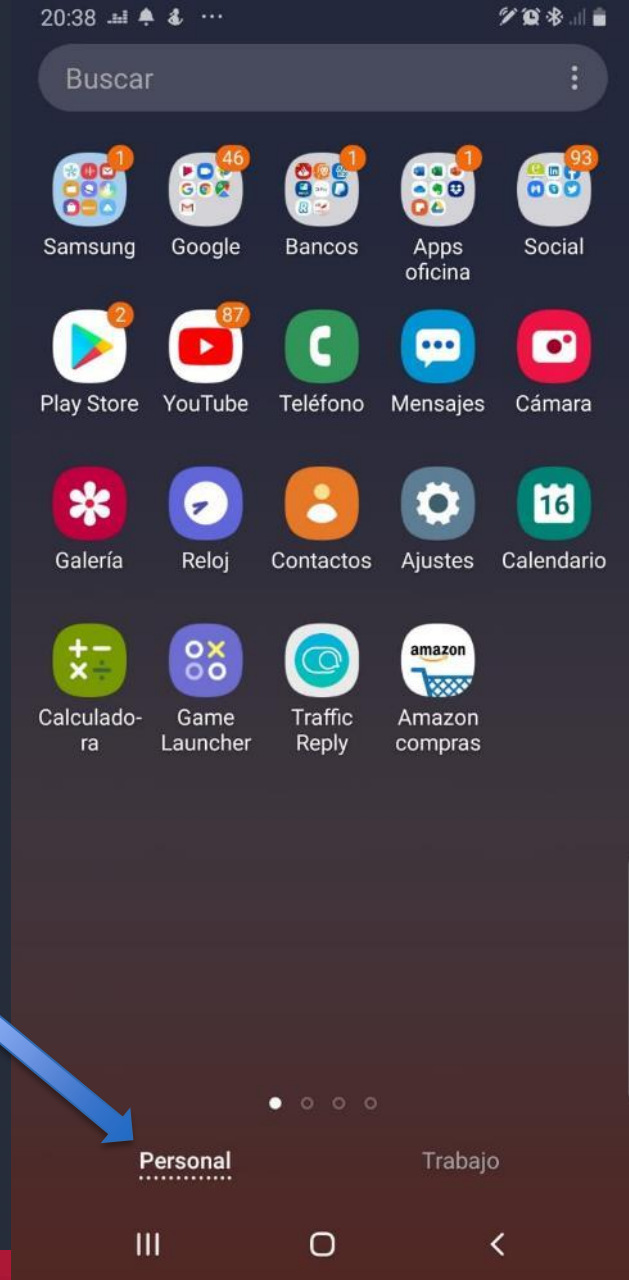


Escritorio principal

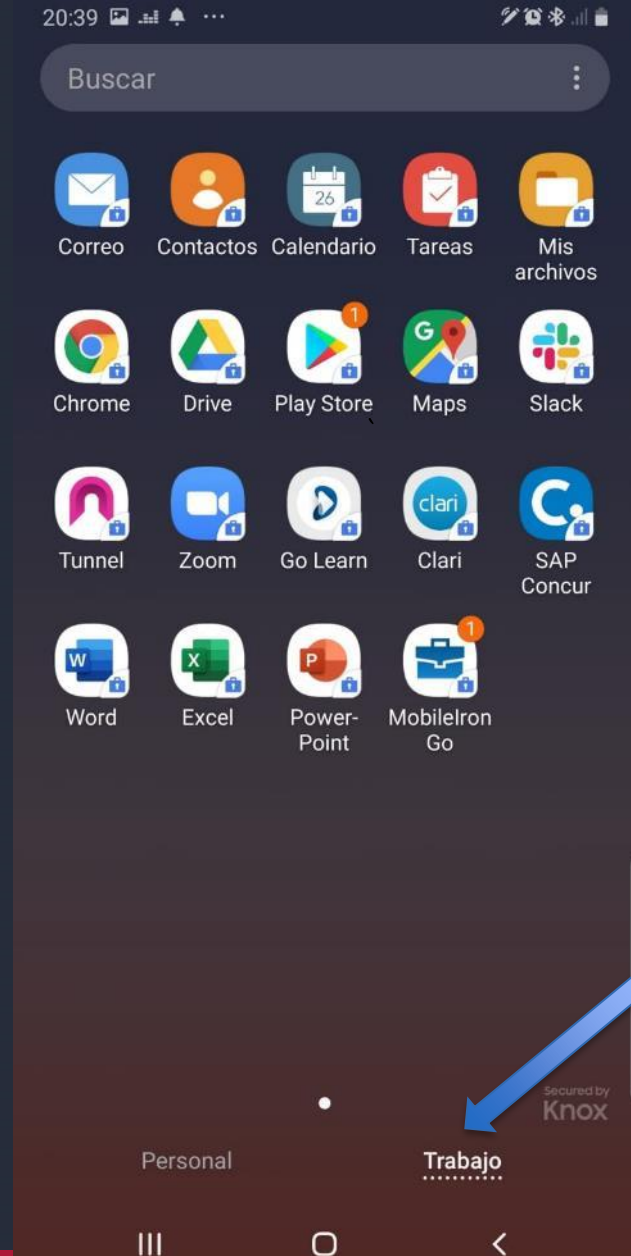


Apps Corporativas

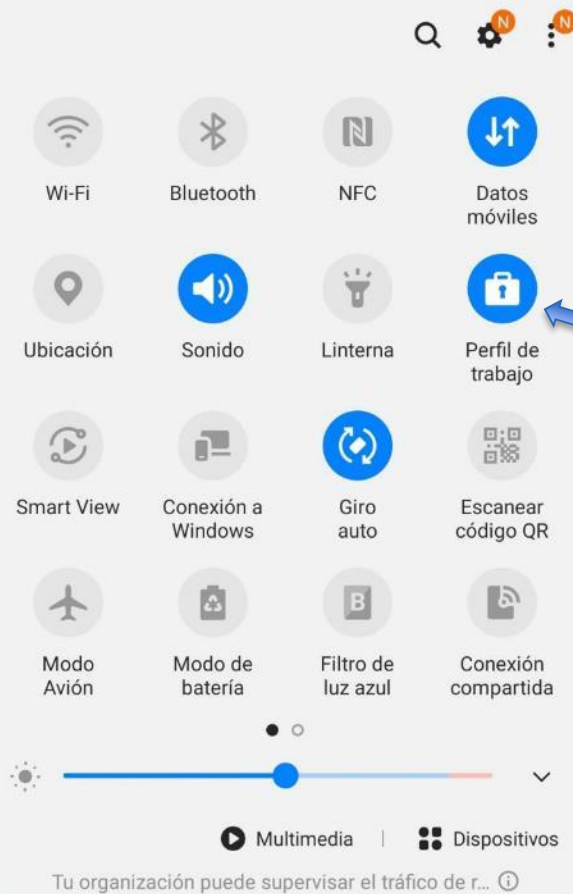
Escritorio de Aplicaciones Personales



Escritorio de Aplicaciones de trabajo



20:01
mar., 17 de marzo



Activación del
perfil de trabajo

20:02

mar., 17 de marzo



Wi-Fi



Bluetooth



NFC



Datos
móviles



Ubicación



Sonido



Linterna



Perfil de
trabajo



Smart View



Conexión a
Windows



Giro
auto



Escanear
código QR



Modo
Avión



Modo de
batería



Filtro de
luz azul



Conexión
compartida



Multimedia



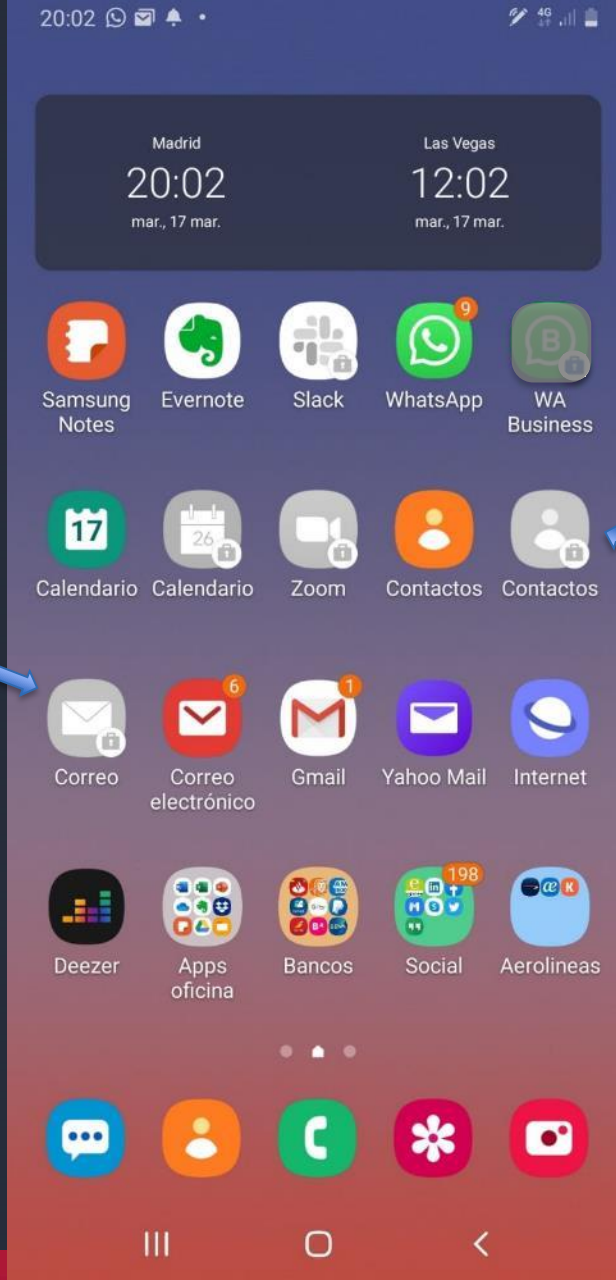
Dispositivos

Tu organización puede supervisar el tráfico de r... ⓘ

Desactivación del
perfil de trabajo

Escritorio principal

Aplicaciones de perfil de trabajo desactivadas



Aplicaciones de perfil de trabajo desactivadas

Escritorio de trabajo desactivado





Proteger los datos corporativos y la privacidad del usuario

Separando el contenido personal del corporativo, con un UEM certificado



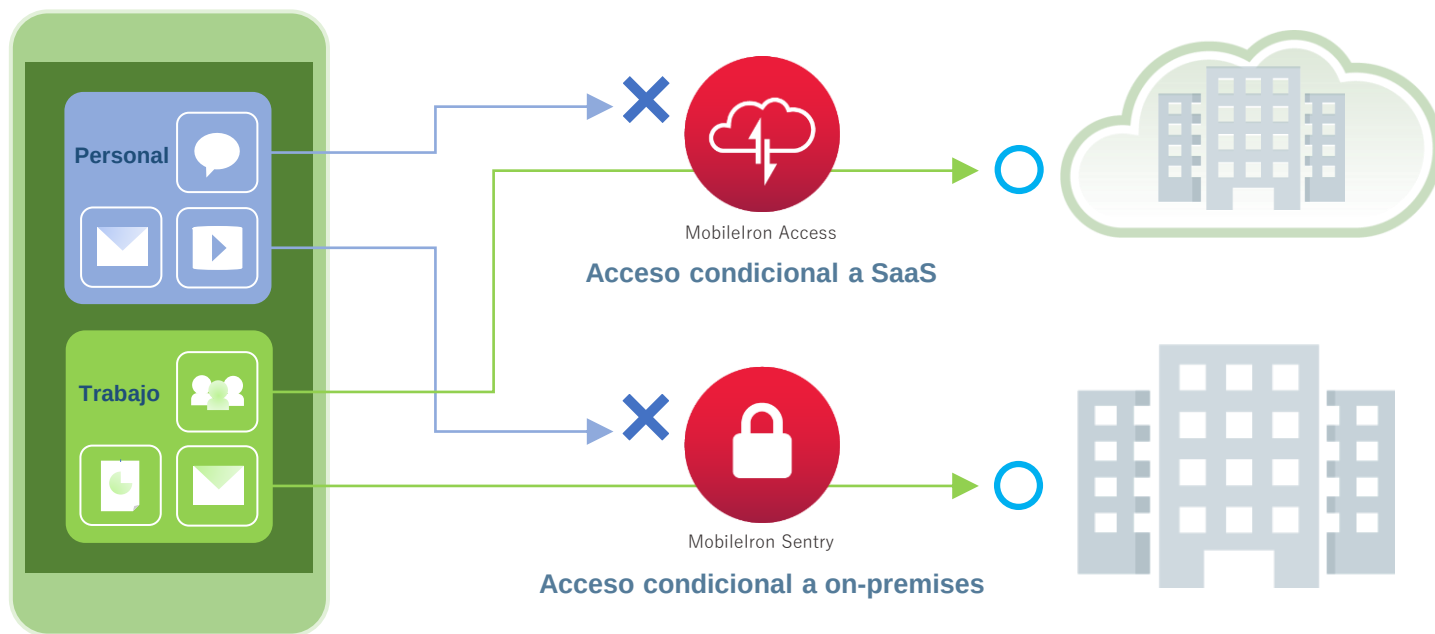
Arquitectura Mobileiron

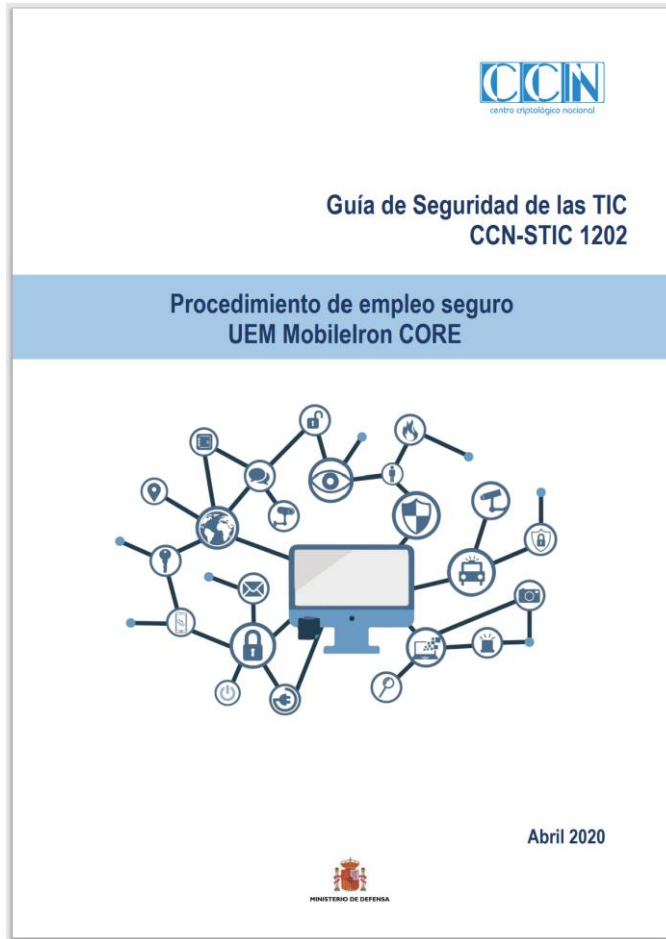
Seguridad centrada en dispositivos móviles para un mundo sin perímetro



Prevenir el acceso no autorizado a datos corporativos

Aplique políticas inteligentes basadas en riesgos en un mundo sin perímetro





Procedimiento de empleo seguro



<https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/4916-ccn-stic-1202-procedimiento-de-empleo-seguro-uem-mobileiron-core/file.html>

UEM

La base de la seguridad para dispositivos y aplicaciones



 **mobileiron**
UEM

Unified Endpoint Management

Threat Defense

Detectar y Remediar.
Cyberseguridad



 **mobileiron**
MTD

Mobileiron Threat Defense

Zero Password

Móvil y biometría como
identificador del usuario.



 **mobileiron**
ZSO

Zero Sign-on

Ha sido un placer. Muchas gracias por su atención

