

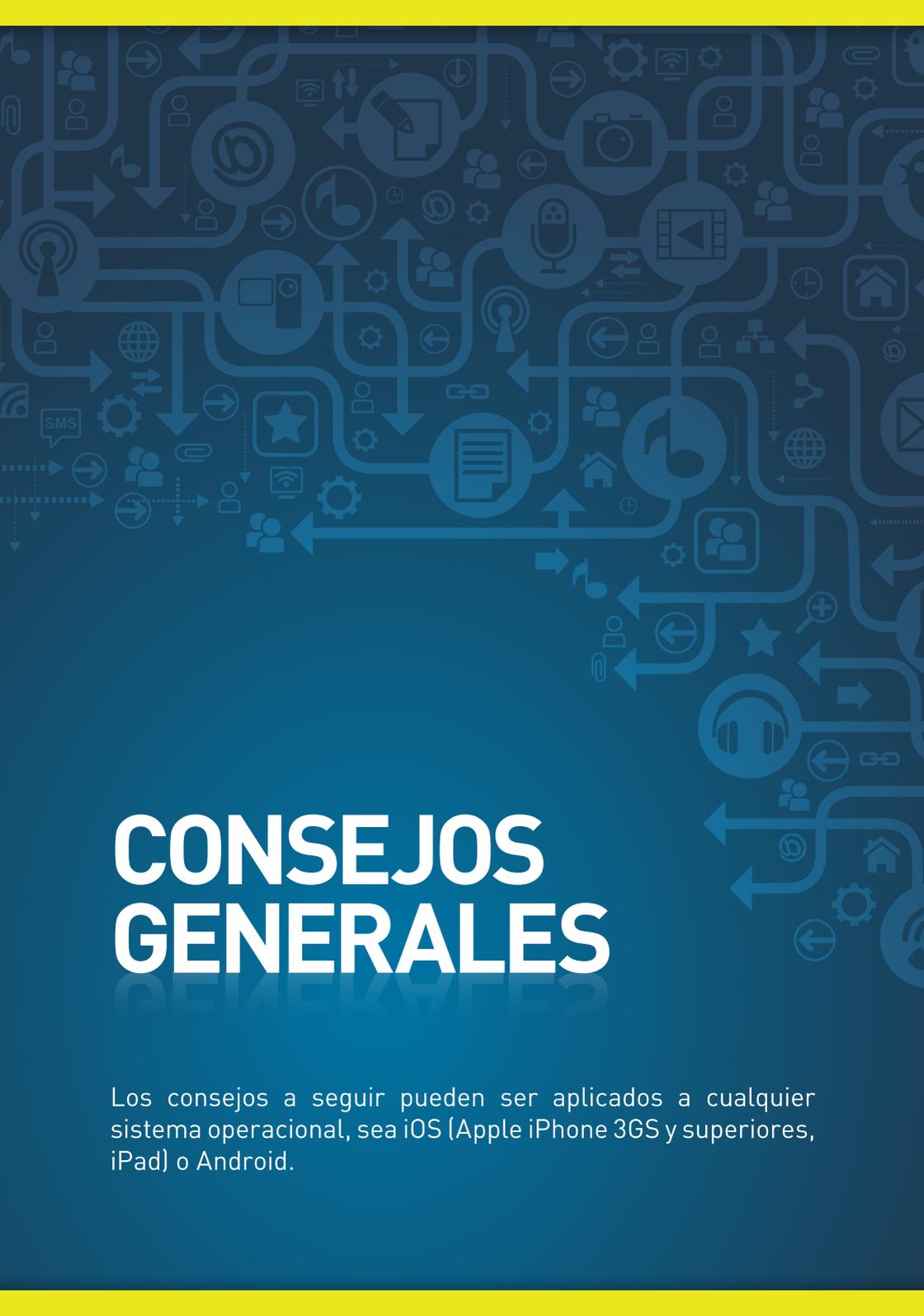
© 2012, CAIS/RNP - Centro de Atendimento a Incidentes de
Segurança da Rede Nacional de Ensino e Pesquisa.

É permitida a reprodução parcial ou integral e a
distribuição deste material, desde que citada a fonte
e para fins educacionais e de conscientização.



Tablets y smartphones están cada vez más presentes en la vida de las personas. Diferente de las computadoras personales, estos dispositivos tienen menor poder de procesamiento, menor capacidad de memoria e interfaces de comunicación con el usuario diferenciadas. Dispositivos diferentes deben contar con estrategias de protección contra amenazas de seguridad diferentes.

CAIS/RNP preparó este guía para auxiliarte en el mundo relativamente nuevo de los dispositivos móviles, dando consejos simples y eficaces para usarlos de forma más segura.



CONSEJOS GENERALES

Los consejos a seguir pueden ser aplicados a cualquier sistema operacional, sea iOS (Apple iPhone 3GS y superiores, iPad) o Android.

EN AMBIENTE CORPORATIVO



La plataforma considerada con los mejores recursos de seguridad para empresas es BlackBerry.

- **Hace muchos años la RIM (fabricante de estos dispositivos) ofrece soluciones para gerenciamiento remoto de los dispositivos** por medio de BlackBerry Enterprise Server, más conocido como BES. A través de este servicio, el administrador de sistemas de la empresa puede forzar el uso de contraseñas fuertes, prohibir el uso de Wi-Fi, prohibir la instalación de Apps de redes sociales, entre otros.
- **Los mecanismos de criptografía de los BlackBerry son reconocidos por ser superiores**, desde transferencia de datos seguros hasta almacenamiento de datos seguros, ofrecidos por el propio dispositivo, sin la necesidad de instalación de Apps adicionales.

Google Android y Apple también poseen recursos orientados a la administración remota de dispositivos que son parte de una corporación. Ellos son:

- **iOS Security – Mobile Device Management (MDM)**
http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf
- **Device Policy Administration for Android**
<http://support.google.com/a/bin/answer.py?hl=en&answer=1056433>

CONSEJOS DE COMPRA



Prefiera los principales y más promisoros sistemas operacionales para smartphone. En el momento actual, estas opciones son Google Android, Apple iPhone y el más reciente Windows Phone.

Históricamente, se ha registrado una mayor incidencia de Apps maliciosos para Google Android del que para Apple iPhone / iPad – los dos sistemas dominantes en el mercado. Sin embargo, a pesar de ese histórico favorecer la elección de dispositivos Apple, ningún sistema está libre de amenazas.

Si fuera posible, contrate seguro o la garantía extendida del fabricante o del establecimiento comercial. Estas son algunas de las opciones disponibles en el Brasil:

- <http://www.pitzi.com.br>
- <http://www.portoseguro.com.br/seguros/seguro-para-equipamentos-portateis>

CONEXIÓN SEGURA



- **Evite proporcionar datos personales/financieros a sitios sin conexión segura (SSL/TLS).** Esta recomendación es particularmente importante cuando el usuario usa Wi-Fi (802.11a, 802.11b, 802.11g, 802.11n). Para verificar si un sitio ofrece conexión segura, busque por la imagen de un candado en el navegador. Otra manera de verificar es conferir si la dirección comienza con `https://` . O “s” al final de `http` significa que el servidor está utilizando SSL/TLS.
- **Si fuera posible, evite usar cualquier App que tenga que ver con datos personales en redes Wi-Fi abiertas** – redes sin contraseña, normalmente disponibles en aeropuertos y cafés. Algunos ejemplos son Apps de bancos y sitios de compras.
- **VPN:** Smartphones tienen la opción de usar 3G como link de Internet, que actualmente es mucho más seguro que usar una red Wi-Fi abierta en términos de posibilidad de interceptaciones de los datos por terceros. Sin embargo, también recomiéndase el uso de VPN, que crea un canal seguro de comunicación, aún que la red usada para acceso a la Internet no lo sea. Para más informaciones, por favor, consulte la página 25 (Laptops).

SEGURIDAD FÍSICA



● En caso de robo de su smartphone o tablet:

- En primer lugar, reconozca que su mayor problema es garantizar que sus informaciones estén a salvo.
- La viabilidad de recuperar su smartphone robado o perdido en Brasil es mínima, por eso se prepare para poder perderlo sin grandes impactos en su vida personal / profesional.
- En dispositivos iPhone e iPad, hay un recurso que localiza el dispositivo perdido / robado. Hay también la opción de bloquear, borrar todos los datos o simplemente enviar un mensaje (con destaque) para el celular. Consulte la página 18 (Buscar iPhone) para más informaciones.
- En dispositivos Android hay diversas maneras de localizar y realizar acciones en el dispositivo perdido o robado. Una de las opciones es Android Lost (<http://www.androidlost.com>).
- Prohíba el acceso de su smartphone perdido a sus redes sociales. Es posible realizar esta acción remotamente. Algunos ejemplos:

Twitter:

<https://twitter.com/settings/applications>

Facebook:

<https://www.facebook.com/settings?tab=applications>

Gmail:

<https://accounts.google.com/b/0/IssuedAuthSubTokens>

● Como descartar dispositivos móviles con seguridad:

Usó su smartphone por años y ahora es hora de deshacerse del modelo antiguo. ¿Qué hacer antes de dar a él un destino, sea venderlo o donarlo?

A seguir, ofrecemos algunos consejos básicos para descartar de forma segura sus dispositivos móviles:

- Smartphones y tablets almacenan muchos tipos diferentes de datos. Es posible afirmar que esos dispositivos almacenan una variedad mayor de datos personales del que computadoras personales, particularmente fotos personales. Usted debe garantizar que estos datos no lleguen a terceros.
- La principal acción que debe ser tomada es limpiar todos los datos y configuraciones del dispositivo. Esto tiene varios nombres, dependiendo del fabricante: wipe, reset, reiniciar, redefinir.
- Como realizar “wipe” en cada dispositivo:

iPhone / iPad:

App “Ajustes”, Opción “General”, Opción “Redefinir” (la última de la tela General). Escoja la opción “Borrar Todo el Contenido y Ajustes”.

Android:

Botón “Menú”, opción “Configuraciones del sistema”, opción “Hacer backup y redefinir”. Escoja la opción “Configuración original”.

BlackBerry:

- En la pantalla inicial o en una carpeta, haga clic en el ícono Opciones.
- Haga clic en Opciones de seguridad. Después haga clic en Configuraciones generales.
- Presione la tecla Menú.
- Haga clic en Limpiar dispositivo portátil.
- Para excluir todos los aplicativos de terceros del dispositivo, marque la caja de selección Incluir aplicativos de terceros.
- Haga clic en Continuar.
- Digite blackberry.

CONSEJO

Con excepción de iPhone y iPad, la mayoría de los smartphones y tablets poseen el recurso de expansión de memoria de almacenamiento por tarjeta MicroSD o SD. Esa tarjeta puede estar localizada en una puerta externa o atrás de la batería. Antes de donar o vender este dispositivo se certifique, que haya tarjetas de memoria, que ellos estén sin datos de cualquier tipo (fotos, archivos de sistema, documentos).



PREVÉNGASE DE ACCIDENTES



SINCRONIZACIÓN. Sincronice los contactos y agenda de su smartphone o tablet. De esta forma, usted no perderá contactos en caso de pérdida, robo o si el dispositivo se malogra. Los principales servicios de Webmail (ex: Gmail) permiten la sincronización con smartphone de manera muy fácil.

BACKUP! Todos los sistemas de smartphone ofrecen la opción de backup completo del dispositivo. Normalmente eso es hecho automáticamente (iPhone, BlackBerry) al conectarse el dispositivo al computador personal para sincronización de multimedia, contactos y apps.

¿USTED SABÍA?



- Es posible exigir dos contraseñas de acceso al Gmail. Para esto configure la “Verificación en dos etapas” en:

<https://accounts.google.com/b/0/SmsAuthConfig>

- Google también ofrece una App llamada “Google Authenticator”. Entretanto, sugerimos la verificación por SMS pues funciona solamente en caso de que la batería esté descargada.
- Caso su celular primario no pueda recibir SMSs por alguna razón es posible registrar un segundo número de celular. Para ello, configure la opción “backup phones”.
- Caso usted no tenga acceso a ninguno de los celulares que fueron configurados para recibir el SMS, es posible obtener un conjunto de contraseñas de emergencia. Para ello, basta acceder los códigos de backup (“backup codes”). Preventivamente, recomiéndase que una copia de tales códigos sea impresa y guardada en sigilo.

CÓDIGOS MALICIOSOS



Antivirus: instalar o no? La incidencia de virus para smartphones no es alarmante, pero significativa lo suficiente (particularmente en Google Android) para que las personas puedan comenzar a tratar smartphones como computadoras personales. A este respecto, es importante considerar lo siguiente.

- Soluciones de seguridad no tratan apenas de virus.
- Algunas funcionalidades son redundantes (ejemplo: localización y bloqueo / datos borrados remotamente).
- Algunas sugerencias de productos. No indicaremos una única solución para evitar parcialidad:

- **F-Secure Mobile Security**

http://www.f-secure.com/pt/web/operators_global/security-services/protection-for-mobile/overview

- **Kaspersky Mobile Security**

<http://brazil.kaspersky.com/produtos/produtos-para-usuarios-domesticos/mobile-security>

- **McAfee Mobile Security**

<http://home.mcafee.com/store/mobile-security>

- **Trend Micro Mobile Security**

<http://br.trendmicro.com/br/products/enterprise/mobile-security/>

INSTALE APPS SOLAMENTE A PARTIR DE LAS FUENTES OFICIALES



En el caso de iPhone y iPad, sólo es posible instalar Apps de fuentes alternativas si el dispositivo hubiera pasado por el proceso de “jailbreak”. Caso contrario, su dispositivo es impedido de acceder fuentes no oficiales de Apps, garantizando la procedencia de las mismas.

Fuentes oficiales de cada plataforma:

- **Android:** Google Play
- **iPhone / iPad:** Apple iTunes App Store
- **BlackBerry:** BlackBerry App World

TARJETAS DE MEMORIA Y DISPOSITIVOS DE ALMACENAMIENTO USB



Tarjetas de memoria SD y dispositivos de almacenamiento USB (“pendrives” y discos rígidos externos) son muy comunes hoy en día. **La capacidad de almacenamiento de estos dispositivos es muy alta, lo que exige ciertos cuidados.**

- **Sabemos que es tentador usar “pendrives” como destino de sus copias de seguridad (backup), pero sugerimos que no haga eso.** La posibilidad de pérdida o robo de uno de esos dispositivos es muy grande. Además de eso, el hecho de no “eyectar” el “pendrive” o la caída de energía accidental durante la escritura de datos puede causar pérdida de datos. Use preferencialmente un disco rígido externo, un NAS (Network-attached Storage) o aún un servicio de backup “en la nube” seguro.
- **Incluya su “pendrive” o tarjeta de memoria en las barreduras de su anti-virus.**
- **Criptografe los datos de su tarjeta de memoria (si no fuera para uso en cámaras digitales) y “pendrives”.** De esta forma datos almacenados en ellos no serán accesibles por terceros en caso de pérdida o robo. Una vez más, recordamos que sus bienes más valiosos son sus datos. Sugerimos el uso de TrueCrypt (<http://www.truecrypt.org>), que es compatible con los principales sistemas operacionales del mercado.