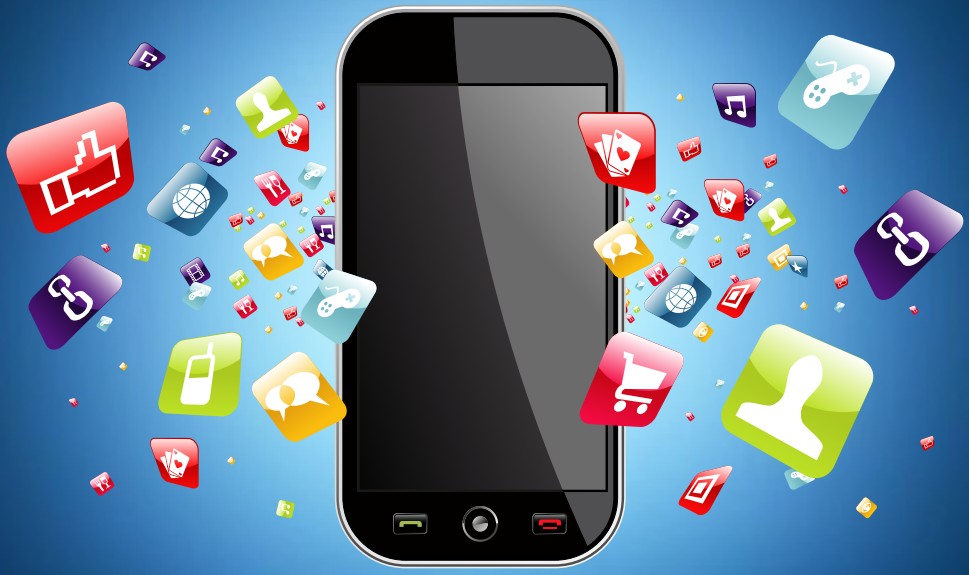
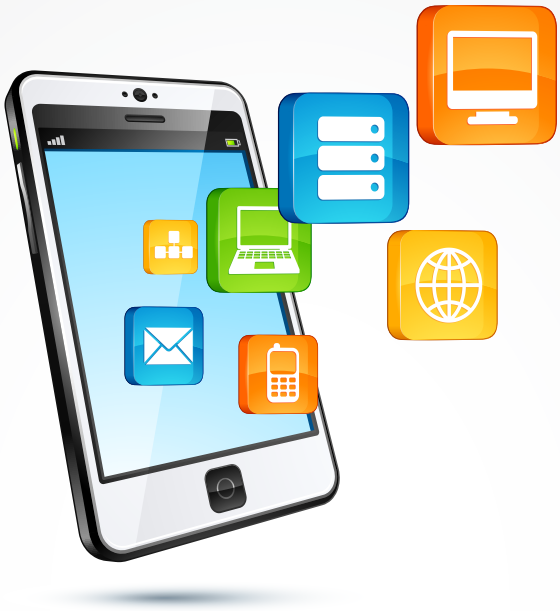
# CARTILLA DE SEGURIDAD EN DISPOSITIVOS MÓVILES



CAIS

RNP



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 auxiliarlo 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 promisores 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 se deshacer 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 accesar 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 accesar 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 escrita 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.

# CONSEJOS ESPECÍFICOS POR SISTEMA OPERACIONAL

Los consejos a seguir atienden las especificidades de cada sistema operacional. Para este guía, fueran considerados los sistemas operacionales más usados: iOS, Android e Blackberry.

# IOS (IPHONE/IPAD)

iOS es el sistema operacional de diversos dispositivos Apple: iPhone (3GS y más recientes), iPad (todos) y Apple TV. La versión considerada en los consejos a seguir es iOS 5.1.1, liberada en Mayo de 2012.

Todos los consejos a seguir se refieren al app Ajustes (Settings para aparatos configurados en inglés), presente en todos los dispositivos iOS.

Fueron considerados dispositivos que no sufrieron "Jailbreak", o sea, iPhone o iPad que esté con el sistema operacional iOS original de la Apple. Para saber si su dispositivo fue desbloqueado (si pasó por el proceso de "jailbreak"), haga una búsqueda por la app Cydia – solamente si estuviera presente entonces el dispositivo pasó por el proceso de "Jailbreak".

## GENERAL

### Actualización de software

Escoja la opción "Actualización de Software" y busque por nuevas actualizaciones del iOS (sistema operacional de dispositivo). AVISO: Caso su dispositivo haya pasado por jailbreak, este proceso retirará los desbloqueos.

- **Bloqueo Automático**
  Se recomienda la configuración de bloqueo automático. "2 minutos" es una buena opción, equilibrando facilidad de uso y seguridad.

- **Bloqueo por Código**
  En esta opción son definidos varios aspectos del bloqueo.

  - Código Simple: marque esta opción para contraseñas más simples y más adecuadas para iPhone.

  - Con esta opción marcada, las contraseñas son números con 4 dígitos. Para contraseñas con mayor complejidad, desmarque la opción "Código Simple". Se recomienda esta opción para iPad y iPhone para uso corporativo.

  - Escoja la opción "Eliminar Datos" para proteger aún más su dispositivo. Esta opción es útil en el caso de su dispositivo caer en manos de terceros. Si una persona digitar el código equivocado 10 veces, todo el contenido de su dispositivo será borrado automáticamente.

## ICLOUD

iCloud es un servicio de almacenamiento y computación "en la nube" que inició sus operaciones en octubre de 2011. En líneas generales, es un recurso que la Apple ofrece para integrar todos los dispositivos iOS (Apple TV, iPhone 3GS y más recientemente, iPad) y computadoras (Mac OS X a partir de la versión Lion) de los usuarios, de forma que archivos y configuraciones sean iguales en todos los dispositivos.

Algunos ejemplos de recursos ofrecidos por iCloud son programados, contactos, backup completo del dispositivo, marcadores del navegador, entre otros. Más informaciones sobre iCloud en *http://www.apple.com/br/icloud/ .*

- **Documentos y datos**
  Opción es útil como backup de Apps y documentos almacenados en el dispositivo.

- **Buscar iPhone**
  - Permite la busca de un iPhone, iPad o Macbook (con Mac OS X Lion o superior).

  - Debe reconocer querecuperar el dispositivo en caso de robo no es viable siempre. Sin embargo, perder datos es permitir que un desconocido tenga acceso a ellos, incluyendo fotos.

  - Este recurso permite que usted borre remotamente todos los datos del dispositivo. Esto es hecho a partir del siguiente website: *https://www.icloud.com/*

  - **ATENCIÓN**: Si las credenciales (Apple ID) cayeran en manos equivocadas es posible no apenas localizar el dispositivo, como también borrar completamente los datos a partir del website icloud.com. Escoja contraseñas complejas para su Apple ID, bien como "preguntas de seguridad" que no puedan ser respondidas fácilmente.

- Para cambiar la contraseña de su Apple ID, efectúe login en el website a seguir y escoja la opción "Contraseña y seguridad":

*https://appleid.apple.com/*

- Altere la contraseña escogiendo "Alterar la contraseña" (sección "Escoja una nueva contraseña"). Se recomienda que escoja su propia pregunta de seguridad.

- **Almacenamiento y Backup**
  Use este recurso para realizar backups de su dispositivo en la "nube", o sea, en la Internet. Este recurso substituye el backup que ocurre cuando el Apple iTunes es abierto, después de conectado por medio de USB.

## TELÉFONO

- Defina una contraseña para el chip del celular.

- Cada vez que el teléfono es conectado, o que el chip venga a ser inserido nuevamente en el compartimiento, una contraseña será solicitada.

- Escoja la opción "PIN SIM". Después marque la opción "PIN del SIM". Consulte la tarjeta en la cual su chip fue vendido para saber el PIN padrón. Ej: 8486 para VIVO, 1010 para TIM.

# ANDROID (CELULARES Y TABLETS)

Las principales configuraciones de seguridad de sistemas Android están en la sección "Seguridad" de "Configuraciones del sistema" (acceso por el botón Menú).

- **Bloqueo de Pantalla**
  - Escoja la opción una de las opciones de bloqueo de pantalla. Sugerimos la opción "Contraseña", que permite la configuración de contraseñas más complejas.
  - Las opciones "PIN" (un número) y "Padrón" (unir puntos formando un cierto padrón) son menos recomendadas por ser menos complejas.
- **Bloqueo del SIM**
  - Marcar la opción "Bloquear tarjeta SIM"
  - Alterar el PIN (normalmente el padrón definido por la operadora) escogiendo la opción "Alterar PIN del SIM"

- **Fuentes Desconocidas (en Administración del Dispositivo)**

  - Uno de los mayores problemas de Android es el creciente número de Apps maliciosas encontradas. Lamentablemente, una App maliciosa no es fácilmente identificada por usuario. Apps maliciosas normalmente son identificadas por especialistas en seguridad, quienes las reportan al Google, que posteriormente las remueve del servicio. Nuestra recomendación simple: siempre use el servicio oficial de Apps, Google Play (*http://play.google.com/*).

  - Desmarque la opción "Permitir la instalación de aplicativos de fuentes desconocidas". De esta forma, solamente aplicaciones autorizadas por el Google Play pueden ser instaladas.

# BLACKBERRY (RIM)

Así como Android, son varias las versiones de sistema operacional de los smartphones RIM. Actualmente las versiones presentes en aparatos nuevos son BlackBerry OS 6 y BlackBerry OS 7, mas todavía hay muchos aparatos con BlackBerry OS 5 en el mercado.

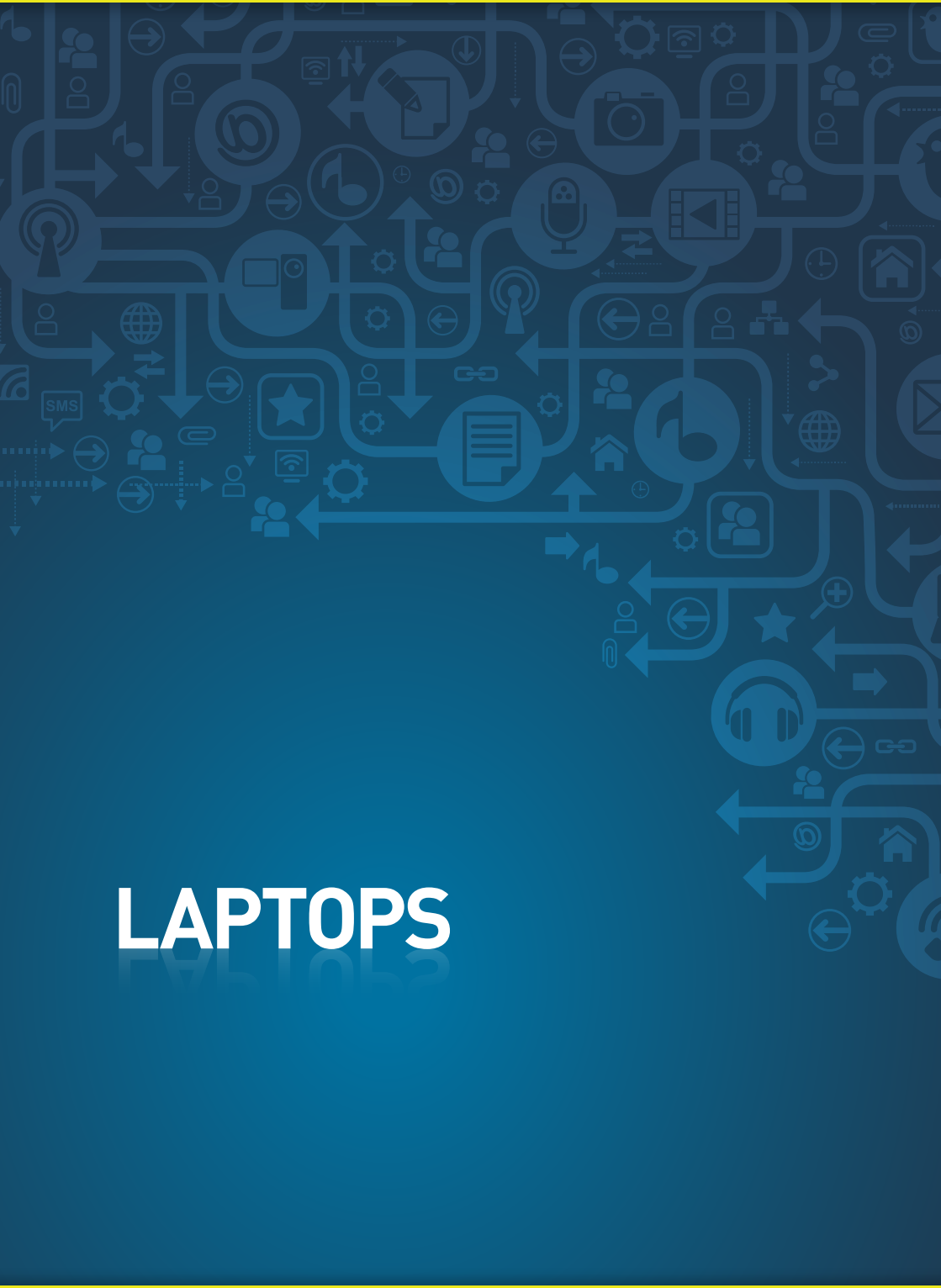
**A seguir, presentamos las configuraciones esenciales de seguridad en smartphones Blackberry**, independiente de la versión de Sistema Operacional. Haga una búsqueda por la opción "Configuraciones" (Settings).

- **CONTRASEÑA:** Defina una contraseña para su BlackBerry.

- **OPCIONES DE SEGURIDAD:** En este ítem están los elementos más esenciales de la seguridad en un BlackBerry. Las más importantes son:

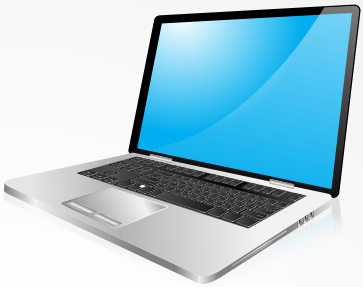
  **CRIPTOGRAFÍA.** Habilite criptografía tanto en la memoria principal cuanto en la tarjeta de memoria (SD / MicroSD). Escoja lo mínimo la opción "Fuerte" para que su contraseña sea más difícil de ser violada.

- **Más informaciones en:**
  *http://docs.blackberry.com/pt-br/smartphone_users/?userType=1*




# LAPTOPS

# LAPTOPS



Ya vió muchas presentaciones sobre seguridad en PC y leyó muchas orientaciones en ediciones pasadas del DISI. De cualquier forma, no cuesta recordar algunos puntos esenciales considerando la movilidad de los laptops, netbooks y ultrabooks, y los riesgos que redes Wi-Fi ofrecen.

- **Instale y mantenga un software anti-virus.** Algunos sistemas operacionales son más explorados que otros por cuestión de popularidad, pero tenga en mente que ninguno de ellos está libre de ser infectado.

- **Instale y mantenga un firewall personal.** Más importante que instalar, entienda como este elemento de seguridad funciona. Poseer un firewall y hacer clic desatentamente en "OK" para todos los alertas no es un comportamiento seguro.

- **Mantenga todos los softwares actualizados, mas dé atención especial al navegador web.** El navegador es la principal puerta de entrada de amenazas. Es importantísimo que usted mantenga Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera, o cualquier otro navegador, siempre actualizado.

- **Tenga siempre software registrado, legítimo, en su computador.** De manera general, los fabricantes dificultan las actualizaciones de seguridad en computadoras con licencias de software irregular.

- **Softwares y Sistema Operacional (Microsoft Windows, Apple Mac OS X, GNU/Linux de cualquier distribución) siempre actualizados** es muy importante en la protección contra la exploración de vulnerabilidades de seguridad conocidas y corregidas.

- **Evite usar redes Wi-Fi abiertas.** Usted sabe que debe usar sin SSL / TLS en websites para conexiones seguras. El problema es que normalmente hay incontables aplicaciones que utilizan Internet y ni siempre ellas se aplican SSL/TLS. Si fuera posible use un link 3G o use una VPN.

- **VPN es muy útil para, de cierta forma, tornar segura una rede Wi-Fi abierta o red cabeada de hotel.** Existen muchas opciones de VPN que puede contratar, algunas buenas opciones están en el siguiente artículo:

  **Five Best VPN Service Providers**
  *http://lifehacker.com/5759186/five-best-vpn-service-providers*

- **Comportamiento.** Evite abrir links de email, particularmente aquellos recibidos de personas y organizaciones que usted no conoce.

- **Cartões de memória e dispositivos de armazenamento USB:** Aos laptops, aplicam-se os mesmos cuidados da subseção homônima em "Dicas gerais".



Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL

BRASIL

PAÍS RICO É PAÍS SEM POBREZA