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