# CARTILHA DE SEGURANÇA EM DISPOSITIVOS MÓVEIS

CAIS

RNP

Tablets e smartphones estão cada vez mais presentes na vida das pessoas. Diferente dos computadores pessoais, esses dispositivos tem menor poder de processamento, menor capacidade de memória e interfaces de comunicação com o usuário diferenciadas. Dispositivos diferentes devem contar com estratégias de proteção contra ameaças de segurança diferentes.

O CAIS/RNP preparou este guia para auxiliá-lo no mundo relativamente novo dos dispositivos móveis, oferecendo dicas simples e eficazes para um uso mais seguro dos mesmos.

# DICAS GERAIS

As dicas a seguir podem ser aplicadas a smartphones e tablets que abriguem os sistemas operacionais iOS (Apple iPhone 3GS e superiores, iPad) ou Android.

# EM AMBIENTE CORPORATIVO

A plataforma considerada com os melhores recursos de segurança para empresas é BlackBerry.

- **Há muitos anos a RIM (fabricante destes dispositivos) oferece soluções para gerenciamento remoto dos dispositivos** por meio de BlackBerry Enterprise Server, mais conhecido como BES. Através deste serviço, o administrador de sistemas da empresa pode forçar o uso de senhas fortes, proibir o uso de Wi-Fi, proibir a instalação de Apps de redes sociais, entre outros.

- **Os mecanismos de criptografia dos BlackBerry são reconhecidos por serem superiores**, desde transferência de dados segura até armazenamento de dados seguro oferecidos pelo próprio dispositivo, sem a necessidade de instalação de Apps adicionais.

Google Android e Apple também possuem recursos voltados à administração remota de dispositivos que são parte de uma corporação.

- **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*

# DICAS DE COMPRA

**Prefira os principais e mais promissores sistemas operacionais para smartphone.** No momento, essas opções são Google Android, Apple iPhone e o mais recente Windows Phone.

Historicamente, ocorreu uma incidência muito maior de Apps maliciosos para Google Android do que para Apple iPhone / iPad – os dois sistemas dominantes no mercado. Embora esse histórico favoreça a escolha de dispositivos Apple, nenhum sistema está livre de ameaças.

**Se possível, contrate seguro ou a garantia extendida do fabricante ou estabelecimento comercial.** Estas são algumas das opções disponíveis no Brasil:

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

# CONEXÃO SEGURA

- **Evite fornecer dados pessoais / financeiros a sites sem SSL/ TLS (site seguro).** Esta dica é particularmente importante quando o usuário usar Wi-Fi (802.11a, 802.11b, 802.11g, 802.11n). Para verificar se um site oferece conexão segura procure pela imagefm de um cadeado no navegador. Outra maneira de verificar é conferir se o endereço começa com https:// . O "s" ao final de http significa que o servidor está utilizando SSL/TLS.

- **Se possível evite usar qualquer App que lide com dados pessoais em redes Wi-Fi abertas** – aquelas sem senha, normalmente disponíveis em aeroportos e cafés. Alguns exemplos são Apps de bancos e sites de compras.

- **VPN**: Smartphones tem a opção de usar 3G como link de Internet, que atualmente é muito mais seguro do que usar uma rede Wi-Fi aberta em termos de possibilidade de interceptação dos dados por terceiros. Entretanto, também recomendamos o uso de VPN, que cria um canal seguro de comunicação, mesmo que a rede usada para acesso a Internet não seja. Para mais informações, consulte a página 25.

# SEGURANÇA FÍSICA

- **Em caso de roubo de seu smartphone ou tablet:**

  - Em primeiro lugar, assuma que seu maior problema é garantir que suas informações estejam a salvo.

  - A viabilidade de recuperar seu smartphone roubado ou perdido no Brasil é mínima, por isso prepare-se para poder perdê-lo sem grandes impactos em sua vida pessoal / profissional.

  - Em dispositivos iPhone e iPad, há um recurso que localiza o dispositivo perdido / roubado. Há também a opção de bloquear, apagar todos os dados ou simplesmente enviar uma mensagem (com grande destaque) para o celular. Consulte a página 18 (Buscar iPhone) para mais informações.

  - Em dispositivos Android há diversas maneiras de localizar e realizar ações no dispositivo perdido ou roubado. Uma das opções é Android Lost (*http://www.androidlost.com*).

  - Proíba o acesso de seu smartphone perdido a suas redes sociais. É possível realizar esta ação remotamente. Alguns exemplos:

**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 móveis com segurança:**

Você usou seu smartphone por anos e agora é hora de se desfazer do modelo antigo. O que fazer antes de dar a ele um destino, seja vendê-lo ou doá-lo?

A seguir oferecemos algumas dicas básicas para o descarte seguro de dispositivos móveis:

- Smartphones e tablets armazenam muitos tipos diferentes de dados. É possível afirmar que esses dispositivos armazenam uma variedade maior de dados pessoais do que computadores pessoais, particularmente fotos pessoais. Você deve garantir que estes dados não cheguem a terceiros.

- A principal ação que deve ser feita é limpar todos os dados e configurações do dispositivo. Isto tem vários nomes, dependendo do fabricante: wipe, reset, reiniciar, redefinir.

- Como realizar "wipe" em cada dispositivo:

**iPhone / iPad:**
App "Ajustes", Opção "Geral", Opção "Redefinir" (a última da tela Geral). Escolha a opção "Apagar Todo o Conteúdo e Ajustes".

**Android:**
Botão "Menu", opção "Configurações do sistema", opção "Fazer backup e redefinir". Escolha a opção "Configuração original"

**BlackBerry:**
- Na tela inicial ou em uma pasta, clique no ícone Opções.
- Clique em Opções de segurança. Depois clique em Configurações gerais.
- Pressione a tecla Menu.
- Clique em Limpar dispositivo portátil.
- Para excluir todos os aplicativos de terceiros do dispositivo, marque a caixa de seleção Incluir aplicativos de terceiros.
- Clique em Continuar.
- Digite blackberry.

## DICA

Com exceção de iPhone e iPad, a maioria dos smartphones e tablets possui o recurso de expansão de memória de armazenamento por cartão MicroSD ou SD. Esse cartão pode estar localizado em uma porta externa ou atrás da bateria. Antes de doar ou vender este dispositivo certifique-se, se houver cartões de memória, que eles estejam sem dados de qualquer tipo (fotos, arquivos de sistema, documentos).

# PREVINA-SE CONTRA ACIDENTES

**SINCRONIZAÇÃO**. Sincronize os contatos e agenda de seu smartphone ou tablet. Desta forma, você não perderá contatos em caso de perda, roubo ou mesmo quebra do dispositivo. Os principais serviços de Webmail (ex: Gmail) permitem a sincronização com smartphone de maneira muito fácil.

**BACKUP!** Todos os sistemas de smartphone oferecem a opção de backup completo do dispositivo. Normalmente isso é feito automaticamente (iPhone, BlackBerry) ao se conectar o dispositivo ao computador pessoal para sincronização de multimídia, contatos e apps.

## VOCÊ SABIA?

- É possível exigir duas senhas para acesso a seu Gmail. Para isto configure a "Verificação em duas etapas" em:

  *https://accounts.google.com/b/0/SmsAuthConfig*

- Google também oferece uma App chamada "Google Authenticator". Entretanto, sugerimos a verificação por SMS porque ela funciona mesmo em caso de bateria descarregada.

- Caso seu celular primário não possa receber SMS por alguma razão é possível cadastrar um segundo número de celular. Para isso, configure a opção "backup phones".

- Caso você não tenha acesso a nenhum dos celulares que foram configurados para receber o SMS, é possível obter um conjunto de senhas de emergência. Para isso, basta acessar os códigos de backup (backup codes). Preventivamente, recomenda-se que uma cópia de tais códigos seja impressa e mantida em sigilo.

# CÓDIGOS MALICIOSOS

**Antivírus:** instalar ou não? A incidência de vírus para smartphones não é alarmante, mas significativa o suficiente (particularmente em Google Android) para que as pessoas possam começar a tratar smartphones como computadores pessoais.

- Soluções de segurança não tratam apenas de vírus.
- Algumas funcionalidades são redundantes (exemplo: localização e bloqueio / dados apagados remotamente).
- Algumas sugestões de produtos. Não indicaremos uma única solução para evitar parcialidade:
  - **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 SOMENTE A PARTIR DAS FONTES OFICIAIS

No caso de iPhone e iPad, só é possível instalar Apps de fontes alternativas se o dispositivo tiver passado pelo processo de "jailbreak". Caso contrario, seu dispositivo é impedido de acessar fontes não oficiais de Apps, garantindo a procedência das mesmas.

**Fontes oficiais de cada plataforma:**

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

# CARTÕES DE MEMÓRIA E DISPOSITIVOS DE ARMAZENAMENTO USB

Cartões de memória SD e dispositivos de armazenamento USB ("pendrives" e discos rígidos externos) são muito comuns hoje em dia. **A capacidade de armazenamento destes dispositivos é muito alta, o que exige certos cuidados**.

- **Sabemos que é tentador usar "pendrives" como destino de suas cópias de segurança (backup), mas sugerimos que você não faça isso**. A chance de perda ou roubo de um desses dispositivos é muito grande. Além disso, o fato de não "ejetar" o "pendrive" ou a queda de energia acidental durante a escrita de dados pode causar perda de dados. Use preferencialmente um disco rígido externo, um NAS (Network-attached Storage) ou mesmo um serviço de backup na nuvem seguro.

- **Inclua seu "pendrive" ou cartão de memória nas varreduras de seu antivírus.**

- **Criptografe os dados de seu cartão de memória (se não for para uso em câmeras digitais) e "pendrives"**. Desta forma dados armazenados neles não serão acessíveis por terceiros em caso de perda ou roubo. Mais uma vez lembramos que seus bens mais valiosos são seus dados. Sugerimos o uso de TrueCrypt (*http://www.truecrypt.org*), que é compatível com os principais sistemas operacionais do mercado.

# DICAS ESPECÍFICAS POR SISTEMA OPERACIONAL

As dicas a seguir atendem as especificidades de cada sistema operacional. Para este guia, foram considerados os sistemas operacionais mais usados: iOS, Android e Blackberry.

# IOS (IPHONE/IPAD)

iOS é o sistema operacional de diversos disposivos Apple: iPhone (3GS e mais recentes), iPad (todos) e Apple TV. A versão considerada nas dicas a seguir é iOS 5.1.1, liberada em maio de 2012.

Todas as dicas a seguir se referem à app Ajustes (Settings para aparelhos configurados em Inglês), presente em todos os dispositivos iOS.

Consideramos dispositivos que não sofreram "Jailbreak", ou seja, iPhone ou iPad que esteja com o sistema operacional iOS original da Apple. Para saber se seu dispositivo foi desbloqueado (se passou pelo processo de "jailbreak") procure pela app Cydia – somente se ela estiver presente então o dispositivo passou pelo processo de "Jailbreak".

- **GERAL**

  - **Atualização de software**
    Escolha a opção "Atualização de Software" e busque por novas atualizações do iOS (sistema operacional de dispositivo). AVISO: Caso seu dispositivo tenha passado por Jailbreak este processo removerá os desbloqueios.

- **Bloqueio Automático**
  Recomenda-se a configuração de bloqueio automático. "2 minutos" é uma boa escolha, equilibrando facilidade de uso e segurança.

- **Bloqueio por Código**
  Nesta opção são definidos vários aspectos do bloqueio.

  - Código Simples: marque esta opção para senhas mais simples e mais adequadas para iPhone.

  - Com esta opção marcada as senhas são números com 4 algarismos. Para senhas com maior complexidade, desmarque a opção "Código Simples". Recomendamos esta opção para iPad e iPhone para uso corporativo.

  - Escolha a opção "Eliminar Dados" para proteger mais seu dispositivo. Esta opção é útil no caso de seu dispositivo cair em mãos de terceiros. Se uma pessoa digitar o código errado 10 vezes todo o conteúdo de seu dispositivo será apagado automaticamente.

## ICLOUD

iCloud é um serviço de armazenamento e computação "na nuvem" que iniciou suas operações em outubro de 2011. Em linhas gerais, é um recurso que a Apple oferece para integrar todos os dispositivos iOS (Apple TV, iPhone 3GS e mais recente, iPad) e computadores (Mac OS X a partir da versão Lion) dos usuários, de forma que arquivos e configurações sejam iguais em todos os dispositivos.

Alguns exemplos de recursos oferecidos por iCloud são agenda, contatos, backup completo do dispositivo, marcadores do navegador, entre outros. Mais informações sobre iCloud em *http://www.apple.com/br/icloud/* .

- **Documentos e dados**
  Opção é útil como backup de Apps e documentos armazenados no dispositivo.

- **Buscar iPhone**
  - Permite a busca de um iPhone, iPad ou Macbook (com Mac OS X Lion ou superior).

  - Assuma que recuperar o dispositivo em caso de roubo nem sempre é viável. Entretanto, perder dados e permitir que um desconhecido tenha acesso a eles, incluindo fotos.

  - Este recurso permite que você apague remotamente todos os dados do dispositivo. Isto é feito a partir do seguinte website: *https://www.icloud.com/*

  - **ATENÇÃO**: Se as credenciais (Apple ID) caírem em mãos erradas é possível não apenas localizar o dispositivo, como apagar completamente os dados a partir do website icloud.com. Escolha senhas complexas para seu Apple ID, bem como "perguntas de segurança" que não possam ser respondidas facilmente.

- Para trocar a senha de seu Apple ID, efetue login no website abaixo e escolha a opção "Senha e segurança":

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

- Altere a senha escolhendo "Alterar a senha" (seção "Escolha uma nova senha"). Recomendamos que você escolha sua própria pergunta de segurança

- **Armazenamento e Backup**

Use este recurso para realizar backups de seu dispositivo na "nuvem", ou seja, na Internet. Este recurso substitui o backup que acontece quando o Apple iTunes é aberto, depois de conectado por meio de USB.

## TELEFONE

- Defina uma senha para o chip do celular.
- A cada vez que o telefone for ligado, ou que o chip for inserido novamente no compartimento, uma senha será solicitada.
- Escolha a opção "PIN SIM". Depois marque a opção "PIN do SIM". Consulte o cartão no qual seu chip foi vendido para saber o PIN padrão. Ex: 8486 para VIVO, 1010 para TIM.

# ANDROID (CELULARES E TABLETS)

As principais configurações de segurança de sistemas Android estão na seção "Segurança" de "Configurações do sistema" (acesso pelo botão Menu).

- **Bloqueio de Tela**
  - Escolha a opção uma das opções de bloqueio de tela. Sugerimos a opção "Senha", que permite a configuração de senhas mais complexas.
  - As opções "PIN" (um número) e "Padrão" (unir pontos formando um certo padrão) são menos recomendadas por serem menos complexas.
- **Bloqueio do SIM**
  - Marcar a opção "Bloquear cartão SIM"
  - Alterar o PIN (normalmente o padrão definido pela operadora) escolhendo a opção "Alterar PIN do SIM"

- **Fontes Desconhecidas (em Administração do Dispositivo)**

  - Um dos maiores problemas de Android é o crescente número de Apps maliciosas já encontradas. Infelizmente uma App maliciosa não é facilmente identificada por usuário. Apps maliciosas normalmente são identificadas por especialistas em segurança, que reportam as mesmas ao Google, que posteriormente as removem do serviço. Nossa recomendação simples: sempre use o serviço oficial de Apps, Google Play (*http://play.google.com/*).

  - Desmarque a opção "Permitir a instalação de aplicativos de fontes desconhecidas". Desta forma, somente aplicações autorizadas pelo Google Play podem ser instaladas.

# BLACKBERRY (RIM)

Assim como Android, são várias as versões de sistema operacional dos smartphones RIM. Atualmente as versões presentes em aparelhos novos são BlackBerry OS 6 e BlackBerry OS 7, mas ainda há muitos aparelhos com BlackBerry OS 5 no mercado.

**A seguir apresentamos as configurações essenciais de segurança em smartphones Blackberry**, independente da versão de Sistema Operacional. Procure pela opção "Configurações" (Settings).

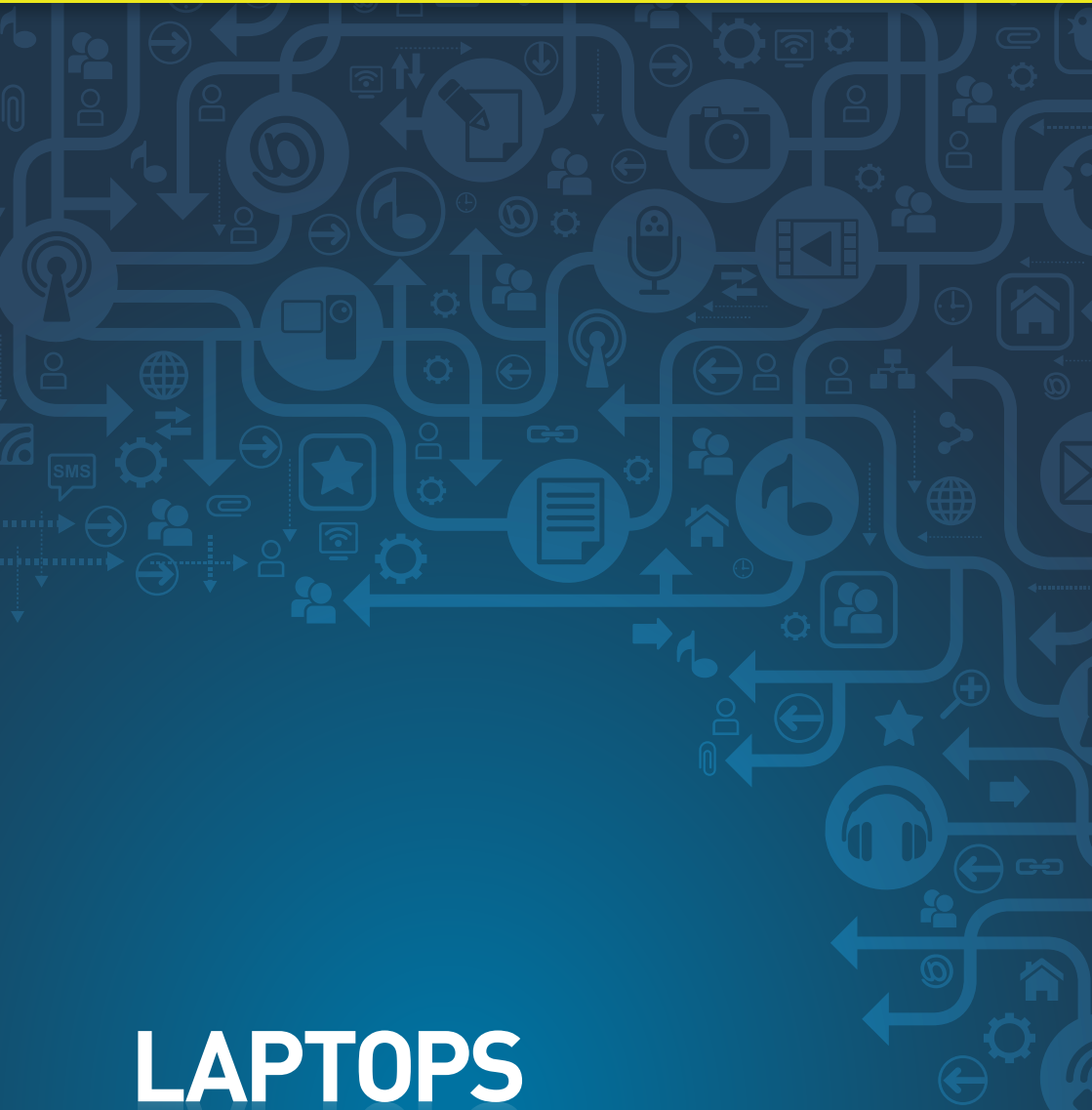
- **SENHA:** Defina uma senha para seu BlackBerry.

- **OPÇÕES DE SEGURANÇA:** Neste item estão os elementos mais essenciais da segurança em um BlackBerry. A mais importante é:

  **CRIPTOGRAFIA.** Habilite criptografia tanto na memória principal quanto no cartão de memória (SD / MicroSD). Escolha no mínimo a opção "Forte" para a força da senha.

- **Mais informações em:**

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




# LAPTOPS

# LAPTOPS

Você já viu muitas palestras sobre segurança em PC e leu muitas orientações em edições passadas do DISI (Dia Internacional de Segurança em Informática). De qualquer forma, não custa lembrar alguns pontos essenciais considerando a mobilidade dos laptops, netbooks e ultrabooks e os riscos que redes Wi-Fi oferecem.

- **Instale e mantenha um software antivírus.** Alguns sistemas operacionais são mais explorados do que outros por questão de popularidade, mas tenha em mente que nenhum deles está livre de ser infectado.

- **Instale e mantenha um firewall pessoal.** Mais importante do que instalar, entenda como este elemento de segurança funciona. Possuir um firewall e clicar desatentamente em "OK", para todos os alertas que aparecem na sua tela, não é um comportamento seguro.

- **Mantenha todos os softwares atualizados, mas dê atenção especial ao navegador web.** O navegador é a principal porta de entrada de ameaças. É importantíssimo que você mantenha Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera, ou qualquer outro navegador, sempre atualizado.

- **Possua sempre software registrado, legítimo, em seu computador.** De maneira geral, os fabricantes dificultam as atualizações de segurança em computadores com licenças de software irregular.

- **Softwares e Sistema Operacional (Microsoft Windows, Apple Mac OS X, GNU/Linux de qualquer distribuição) sempre atualizados** é muito importante na proteção contra a exploração de vulnerabilidades de segurança já conhecidas e corrigidas.

- **Evite usar redes Wi-Fi abertas.** Você já sabe que deve usar sem SSL / TLS em websites para conexões seguras. O problema é que normalmente há incontáveis aplicações que utilizam Internet e nem sempre elas aplicam SSL/TLS. Se possível use um link 3G ou use uma VPN.

- **VPN é muito útil para, de certa forma, tornar segura uma rede Wi-Fi aberta ou rede cabeada de hotel.** Existem muitas opções de VPN que você pode contratar, algumas boas opções estão no seguinte artigo:

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

- **Comportamento.** Evite abrir links de email, particularmente aqueles recebidos de pessoas e organizações que você não conhece.

- **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