Projeto

NUCCIBER

Combate aos Crimes Cibernéticos

Navegar é preciso. Arriscar-se não.

CUIDADO. VOCÊ PODE ESTAR AGINDO ASSIM NA INTERNET.

Privacidade é segurança. Proteja seus dados.

NÚCLEO DE COMBATE AOS CRIMES CIBERNÉTICOS

COORDENAÇÃO:

Fabrício Rabalo Patury

SERVIDORES:

Elizângela Nogueira Lopes

Fernanda Veloso Salgado

Bahia. Ministério Público. Núcleo de Combate aos Crimes Cibernéticos

Segurança na Internet / Ministério Público do Estado
da Bahia. Núcleo de Combate aos Crimes Cibernéticos. -
Salvador: Ministério Público do Estado da Bahia, 2013. 2 ed. rev. amp. 2015

20 p. il. color.

1. Internet. 2 Crimes cibernéticos. I. Ministério Público - Núcleo de Combate aos Crimes Cibernéticos. II. Título.

CDir: 341.559

SUMÁRIO

SEGURANÇA NA INTERNET

MEDIDAS PREVENTIVAS

Nas Redes Sociais

No Uso de Navegadores

Uso de Correio Eletrônico

Transações Bancárias

Comércio Eletrônico

Certificação Digital

Redes

Dispositivos Informáticos e Internet das Coisas

Programas de Distribuição de Arquivos

Deep Web

Marco Civil da Internet

CRIMES CIBERNÉTICOS

CRIMES DE AÇÃO PRIVADA

CRIMES DE AÇÃO PÚBLICA CONDICIONADA

CRIMES DE AÇÃO PÚBLICA INCONDICIONADA

DENÚNCIAS

REFERÊNCIAS

SEGURANÇA NA INTERNET

O que é internet?

A internet é um conglomerado de redes que permite a interconexão descentralizada de computadores por meio de um conjunto de protocolos (denominado **TCP/IP**) e que coloca à disposição do usuário uma enorme quantidade de informações e possibilidades de acesso a serviços diversificados através de páginas (sites). É uma rede de computadores interconectados.

A internet traz inúmeras possibilidades de uso, porém, para aproveitar cada uma delas de forma segura, é importante que alguns cuidados sejam tomados.

ALERTA: A internet é um espaço virtual coletivo. É um espaço público. Postar uma foto em uma rede social é o mesmo que fazer a exposição da foto em uma praça pública movimentada.

MEDIDAS PREVENTIVAS

Nas Redes Sociais

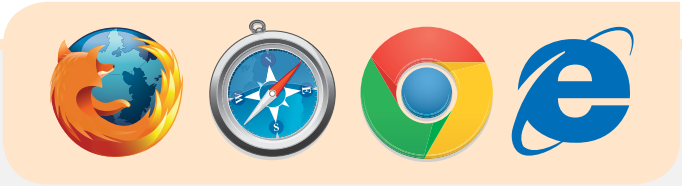
O que são redes sociais?

Uma rede social é uma estrutura composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

São exemplos de redes sociais sites como: Facebook, Twitter, Badoo, Linkedin e outros.

Ao utilizar tais espaços, é preciso ficar atento, porque:

- Pessoas estranhas podem acessar fotos e outras informações pessoais, podendo fazer uso indevido desses dados;
- É preciso educar crianças e jovens sobre o cuidado de publicar conteúdos ofensivos a outras pessoas;
- Hoje em dia, a reputação de uma pessoa também é determinada a partir do uso adequado desses sites de relacionamento.



No Uso de Navegadores

O que são navegadores?

Trata-se de programas de computador que habilitam seus usuários a interagirem com documentos virtuais da internet, também conhecidos como páginas da web.

Ao usar navegadores web:

- Mantenha-os atualizados, com a versão mais recente e com todas as atualizações aplicadas;
- Configure-os para verificar automaticamente atualizações, tanto deles próprios como de complementos que estejam instalados;
- Permita que programas sejam executados apenas quando vierem de sites conhecidos e confiáveis;
- Seja cuidadoso ao usar cookies (arquivos que armazenam as preferências do usuário sobre um determinado site), caso deseje ter mais privacidade.

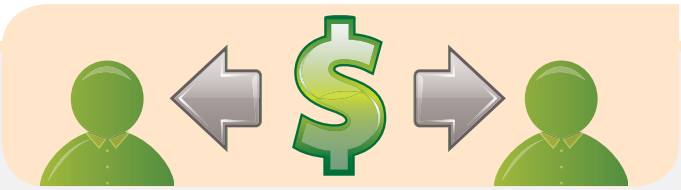
Uso de Correio Eletrônico

O que é correio eletrônico?

É um serviço básico de comunicação na rede que permite a troca de mensagens via e-mail.

Ao usar programas leitores de e-mails:

- Seja cuidadoso ao clicar em links presentes em e-mails;
- Desconfie de arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido falsificado e o arquivo anexado pode estar infectado;
- Antes de abrir qualquer arquivo anexado à mensagem, verifique-o com ferramentas antimalware;
- Verifique se seu sistema operacional está configurado para mostrar a extensão dos arquivos anexados;
- Desligue as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- Habilite, se possível, opções para marcar mensagens suspeitas de serem fraude;
- Use sempre criptografia para conexão entre seu leitor de e-mails e os servidores de e-mail do seu provedor.



Transações Bancárias

- Somente acesse sites de instituições bancárias digitando o endereço diretamente no navegador web, nunca clicando em um link existente em uma página ou em uma mensagem;
- Certifique-se da procedência do site e da utilização de conexões seguras ao realizar transações bancárias via web;
- Evite utilizar sites de buscas para acessar o seu banco. Os endereços (URLs) desse tipo de site são, geralmente, bastante conhecidos;
- Ao acessar o seu banco, forneça apenas uma posição do seu cartão de segurança. Desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição;
- Prefira o uso da extensão b.br (ex: www.nomedobanco.b.br)
- Não forneça senhas ou dados pessoais a terceiros, especialmente por telefone;
- Desconsidere mensagens de instituições bancárias com as quais você não tenha relação, principalmente aquelas que solicitem dados pessoais ou a instalação de módulos de segurança;
- Sempre que ficar em dúvida, entre em contato com a central de relacionamento do seu banco ou diretamente com o seu gerente;
- Não realize transações bancárias por meio de computadores de terceiros ou redes Wi-Fi públicas;
- Verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito e, caso detecte algum lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão;
- Antes de instalar um módulo de segurança, de qualquer internet banking, certifique-se de que o autor do módulo é realmente a instituição em questão;
- Mantenha seu computador seguro, atualizando sempre o programa antivírus.

Comércio Eletrônico

- Certifique-se da procedência do site e da utilização de conexões seguras ao realizar compras e pagamentos via web;
- Pesquise na Internet referências sobre o site antes de efetuar uma compra. Exemplo: Reclame Aqui (www.reclameaqui.com.br);

- Desconfie de preços muito abaixo dos praticados no mercado;
- Evite realizar compras ou pagamentos por meio de computadores de terceiros ou redes Wi-Fi públicas;
- Sempre que ficar em dúvida, entre em contato com a central de relacionamento da empresa com a qual está fazendo a compra;
- Ao efetuar o pagamento de uma compra, evite fornecer dados de cartão de crédito em sites sem conexão segura.

Certificação Digital

Para saber se um certificado é confiável, é necessário observar alguns requisitos. Dentre eles:

- Se o certificado foi emitido por uma Autoridade Certificadora (AC) confiável;
- Se o certificado está dentro do prazo de validade;
- Se o dono do certificado confere com a entidade com a qual está se comunicando.

Quando se tenta acessar um site utilizando conexão segura, normalmente o navegador já realiza todas essas verificações. Caso alguma delas falhe, o navegador emitirá alertas. Esses alertas são emitidos em situações como:

- Se o certificado estiver fora do prazo de validade;
- Se o navegador não identificou a cadeia de certificação;
- Se o endereço do site não confere com o descrito no certificado;
- Se o certificado foi revogado.

Em suma, caso receba um certificado desconhecido ao acessar um site e tenha alguma dúvida ou desconfiança, evite o envio de qualquer informação para o site antes de entrar em contato com a instituição que o mantém para esclarecer o ocorrido.

Redes (Wi-Fi e Bluetooth):

Wi-Fi (Wireless Fidelity) é um tipo de rede local que utiliza sinais de rádio para comunicação.

Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Embora sejam bastante convenientes, há alguns riscos que você deve considerar ao usá-las, como:

- Por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Devido a isso, os dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (por exemplo, um notebook, smartphone ou tablet);
- Por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por atacantes, por meio de uso não autorizado ou de "sequestro"(1);
- Em uma rede Wi-Fi pública - como as disponibilizadas em aeroportos, hotéis e conferências - os dados que não estiverem criptografados podem ser indevidamente coletados por atacantes;
- Uma rede Wi-Fi aberta pode ser propositadamente disponibilizada por atacantes para atrair usuários, a fim de interceptar o tráfego e coletar dados pessoais ou desviar a navegação para sites falsos.

Para resolver alguns destes riscos foram desenvolvidos mecanismos de segurança, como:

WEP (Wired Equivalent Privacy): primeiro mecanismo de segurança a ser lançado. É considerado frágil e, por isto, o uso deve ser evitado.

WPA (Wi-Fi Protected Access): mecanismo desenvolvido para resolver algumas das fragilidades do WEP. É o nível mínimo de segurança que é recomendado.

WPA-2: similar ao WPA, mas com criptografia considerada mais forte. É o mecanismo mais recomendado.

Cuidados a serem tomados:

- Habilite a interface de rede Wi-Fi do seu computador ou dispositivo móvel somente quando usá-la e desabilite-a após o uso;
- Use, quando possível, redes que oferecem autenticação e criptografia entre o cliente e o ponto de acesso. Evite conectar-se a redes abertas ou públicas, sem criptografia, especialmente as que você não conhece a origem;
- Evite o acesso a serviços que não utilizem conexão segura (https);
- Evite usar WEP, pois ele apresenta vulnerabilidades que, quando exploradas, permitem que o mecanismo seja facilmente quebrado;

• Use WPA-2 sempre que disponível. Caso seu dispositivo não tenha este recurso, utilize no mínimo WPA.

(1): Por sequestro de rede Wi-Fi, entende-se uma situação em que um terceiro ganha acesso à rede e altera configurações no ponto de acesso para que somente ele consiga acessá-la.

Bluetooth

Bluetooth é um padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência, permitindo a formação de redes pessoais sem fio. Está disponível em uma extensa variedade de equipamentos, como dispositivos móveis, videogames, mouses, teclados, impressoras, sistemas de áudio, aparelhos de GPS e monitores de frequência cardíaca. A quantidade de aplicações também é vasta, incluindo sincronismo de dados entre dispositivos, comunicação entre computadores e periféricos e transferência de arquivos.

Embora traga muitos benefícios, o uso desta tecnologia traz também riscos, visto que está sujeita às várias ameaças que acompanham as redes em geral, como varredura, furto de dados, uso indevido de recursos, ataque de negação de serviço, interceptação de tráfego e ataque de força bruta.

Um agravante que facilita a ação dos atacantes é que muitos dispositivos vêm, por padrão, com o bluetooth ativo. Desta forma, muitos usuários não percebem que possuem este tipo de conexão ativa e não se preocupam em adotar uma postura preventiva.

Cuidados a serem tomados:

• Mantenha as interfaces bluetooth inativas e somente as habilite quando fizer o uso;

• Configure as interfaces bluetooth para que a opção de visibilidade seja "Oculto" ou "Invisível", evitando que o nome do dispositivo seja anunciado publicamente. O dispositivo só deve ficar rastreável quando for necessário autenticar-se a um novo dispositivo ("pareamento");

• Altere o nome padrão do dispositivo e evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo;

• Sempre que possível, altere a senha (PIN) padrão do dispositivo e seja cuidadoso ao elaborar a nova;

• Evite realizar o pareamento em locais públicos, reduzindo as chances de ser rastreado ou interceptado por um atacante;

• Fique atento ao receber mensagens em seu dispositivo solicitando autorização ou PIN. Não responda à solicitação se não tiver certeza que está se comunicando com o dispositivo correto;

• No caso de perda ou furto de um dispositivo bluetooth, remova todas as relações de confiança já estabelecidas com os demais dispositivos que possui, evitando que alguém, de posse do dispositivo roubado/perdido, possa conectar-se aos demais.

Dispositivos Informáticos e Internet das coisas:

Dispositivos informáticos (tablets, smartphones, celulares, smartwatch, etc.) e demais equipamentos com acesso à Internet, conhecidos como Internet das coisas (geladeira, televisores, óculos, elevadores, automóveis, etc.) têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação web, internet banking e acesso a e-mails e redes sociais. Infelizmente, as semelhanças não se restringem apenas às funcionalidades apresentadas. Elas também incluem os riscos de uso que podem representar. Assim como seu computador, o seu dispositivo informático também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de spam e a propagação de códigos maliciosos, além de poder fazer parte de botnets (softwares que automaticamente se instalam no sistema do dispositivo, controlados remotamente, e exploram os arquivos, programas e informações) e ser usados para disparar ataques na internet.

Somadas a esses riscos, há características próprias que os dispositivos móveis possuem que, quando abusadas, os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas, como:

Grande quantidade de informações pessoais armazenadas: informações como conteúdo de mensagens SMS, MMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, números de cartão de crédito e senhas costumam ficar armazenadas nos dispositivos informáticos.

Maior possibilidade de perda e furto: em virtude do tamanho reduzido, do alto valor que podem possuir, pelo status que podem representar e por estarem em uso constante, os dispositivos informáticos podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes.

Grande quantidade de aplicações desenvolvidas por terceiros: há uma infinidade de aplicações sendo desenvolvidas, para diferentes finalidades, por diversos autores e que podem facilmente ser obtidas e instaladas. Entre elas podem existir aplicações com erros de implementação, não confiáveis ou especificamente desenvolvidas para execução de atividades maliciosas.

Rapidez de substituição dos modelos: em virtude da grande quantidade de lançamentos, do desejo dos usuários de ter o modelo mais recente e de pacotes promocionais oferecidos pelas operadoras de telefonia, os dispositivos informáticos costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados neles gravados.

De forma geral, os cuidados que você deve tomar para proteger seus dispositivos informáticos são os mesmos a serem tomados com seu computador pessoal, como mantê-lo sempre atualizado e utilizar mecanismos de segurança. Outros

cuidados complementares a serem tomados são:

Antes de adquirir seu dispositivo informáticos:

• Considere os mecanismos de segurança que são disponibilizados pelos diferentes modelos e fabricantes e escolha aquele que considerar mais seguro;

• Caso opte por adquirir um modelo já usado, procure restaurar as configurações originais, ou "de fábrica", antes de começar a usá-lo;

• Evite adquirir um dispositivo informáticos que tenha sido ilegalmente desbloqueado (jailbreak) ou cujas permissões de acesso tenham sido alteradas. Essa prática, além de ser ilegal, pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho.

Ao usar seu dispositivo informáticos:

• Se disponível, instale um programa antimalware antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;

• Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;

• Fique atento às notícias veiculadas no site do fabricante, principalmente as relacionadas à segurança;

• Seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e plug-ins. Procure usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação;

• Seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isso pode comprometer a sua privacidade.

Ao acessar redes:

• Seja cuidadoso ao usar redes Wi-Fi públicas;

• Mantenha interfaces de comunicação, como bluetooth, infravermelho e Wi-Fi desabilitadas e somente as habilite quando for necessário;

• Configure a conexão bluetooth para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos. Em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível".

Proteja seu dispositivo informáticos e os dados nele armazenados:

• Mantenha as informações sensíveis sempre em formato criptografado;

• Faça backups periódicos dos dados nele gravados;

• Mantenha controle físico sobre ele, principalmente em locais de risco. Procure não deixá-lo sobre a mesa, e tenha cuidado

com bolsos e bolsas quando estiver em ambientes públicos;

• Use conexão segura sempre que a comunicação envolver dados confidenciais;

• Não siga links recebidos por meio de mensagens eletrônicas;

• Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas);

• Configure-o para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização. Isso pode ser bastante útil em casos de perda ou furto;

• Configure-o, quando possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso. Use essa opção com bastante cautela, principalmente se você tiver filhos e eles gostarem de "brincar" com o seu dispositivo.

Ao se desfazer do seu dispositivo informáticos:

• Apague todas as informações nele contidas;

• Restaure a opções de fábrica.

O que fazer em caso de perda ou furto:

• Informe a sua operadora e solicite o bloqueio do seu número (chip), bem como seu "IMEI";

• Altere as senhas que possam estar nele armazenadas. Por exemplo, as de acesso ao seu e-mail ou rede social;

• Bloqueie cartões de crédito cujo número esteja armazenado em seu dispositivo móvel;

• Se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados.

Programas de Distribuição de Arquivos – Torrents (P2P)

Programas de distribuição de arquivos, ou P2P, são aqueles que permitem que os usuários compartilhem arquivos entre si. Alguns exemplos são: Kazaa, Emule, Dreamule, Gnutella e BitTorrent. Alguns riscos relacionados ao uso destes programas são:

Acesso indevido: caso esteja mal configurado ou possua vulnerabilidades, o programa de distribuição de arquivos pode permitir o acesso indevido a diretórios e arquivos além dos compartilhados.

Obtenção de arquivos maliciosos: os arquivos distribuídos podem conter códigos maliciosos e, assim, infectar seu computador ou permitir que ele seja invadido.

Violação de direitos autorais: a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação dessa lei.

Prevenção:

- Mantenha seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- Certifique-se de ter um antimalware instalado e atualizado e o utilize para verificar qualquer arquivo obtido;
- Mantenha o seu computador protegido, com as versões mais recentes e com todas as atualizações aplicadas;
- Certifique-se que os arquivos obtidos ou distribuídos são livres, ou seja, não violam as leis de direitos autorais.

Deep web

- Conhecida também como Deepnet, Web Invisível, Undernet ou Web oculta.
- A Deep Web se refere a tudo que está disponível em máquinas, porém não pode se reconhecida através do DNS (ex: www.enderecoeletronico.com.br), nem pelos sites de busca (ex: Google, Yahoo, Bing, etc). Dessa forma, seu conteúdo só poderá ser acessado se o usuário souber o endereço da máquina.
- A proposta inicial de sua criação é válida, se não fossem as atividades ilegais disponibilizadas nela. Tudo está na Deep Web.
- Aventureiros e curiosos devem fica fora dela, apesar da disponibilidade de um vasto, interessante e raro conteúdo vinculado aos mais diversos ramos do conhecimento. Mas, na sua grande parte, tem conteúdo assustador e criminoso.
- Os principais hackers e crackers da internet estão lá.
- É lá também que os vírus surgem e são testados com maior frequência. inúmeras armadilhas estão na Deep Web para tentar controlar e invadir seu computador, mesmo com máquinas virtuais.
- O acesso a Deep Web é realizado por diversos navegadores (I2P, Freenet, Netsukuku, Freifunk, Funkfeuer, OneSwarm, etc.), porém o mais popular é o TOR. O objetivo destes navegadores é dificultar a identificação do IP.
- Se ainda assim você quiser acessar a Deep Web, fica a dica! Pesquise mais sobre o assunto e se previna ao máximo.

Marco Civil da Internet

• O crescimento do mundo virtual acarretou o aumento de crimes cometidos na Internet. Dessa forma, com a intensificação dos problemas ocasionados pela digitalização das relações pessoais, comerciais e governamentais, surgiu a necessidade de se regulamentar o uso da internet.

• A Lei nº 2.126/11, conhecido como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

• O Marco Civil regula a privacidade da rede, proibindo o acesso de terceiros a dados e correspondências ou comunicação, garantindo a liberdade de expressão e a proteção aos dados pessoais.

• O Marco Civil também regula a responsabilidade sobre os conteúdos que são publicados, estabelecendo responsabilidades, não só aos usuários, mas ainda aos provedores de conteúdo, caso não acatem a decisão judicial.

• A neutralidade da rede é o principal tema abordado pelo Marco Civil. Segundo este princípio, o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. As exceções previstas na Lei 12.935/2014, que demandam regulamentação, são: requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e priorização de serviços de emergência.

CRIMES CIBERNÉTICOS

Crimes cibernéticos, digitais ou virtuais, assim chamados, são atos lesivos cometidos por meio de computadores ou de periféricos com a intenção de se obter uma vantagem indevida.

Existem, no nosso ordenamento jurídico, diversos crimes tipificados que, muito comumente são cometidos na rede mundial de computadores.

Tal é a importância do tema que o Congresso Nacional aprovou a Lei 12.737/2012, que já se encontra em vigor e dispõe sobre a tipificação criminal de delitos cibernéticos, introduzindo no Código Penal os artigos 154-A e 154-B.

CRIMES DE AÇÃO PRIVADA

Em algumas situações, o Ministério Público não possui legitimidade para atuar como autor da ação penal, de forma que cabe ao ofendido o oferecimento da queixa ao Judiciário, para que, querendo, processe a respectiva ação penal privada.

CRIMES CONTRA A HONRA, que correspondem aos crimes de calúnia, difamação e injúria. Os criminosos são incentivados pelo anonimato e os crimes podem ocorrer em chats, blogs, pelo envio de spams, por meio de publicações em homepages, dentre outras formas de postagem eletrônica. Estes crimes contam com a facilidade de divulgação proporcionada pela rede.

CRIMES CONTRA O PATRIMÔNIO, que compreendem crime de dano, quando há prejuízo considerável à vítima.

CRIMES DE AÇÃO PÚBLICA CONDICIONADA

VIOLAÇÃO DE DIREITO AUTORAL; AMEAÇA; CRIME CONTRA A HONRA, cometido contra funcionário público ou quando se tratar de injúria preconceituosa (§ 3º do art. 140 do Código Penal).

CRIMES DE AÇÃO PÚBLICA INCONDICIONADA

DEMAIS CRIMES, nos quais não se opõe qualquer condição para que o Ministério Público atue. Considerando a importância do combate a esses crimes, o Ministério Público do Estado da Bahia, através do Núcleo de Combate aos Crimes Cibernéticos - NUCCIBER, visa articular medidas judiciais e extrajudiciais necessárias à efetivação do combate aos crimes cibernéticos.

DENÚNCIAS

www.mpba.mp.br/nucciber

REFERÊNCIAS

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS;

disponível em: http://www.mp.mg.gov.br/portal/public/interno/index/id/10

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS, Cartilha: Navegar com Segurança;

disponível em: http://cartilha.cert.br/redes - Cartilha de Segurança para Internet - CERT.br

ANOTAÇÕES

MPDABAHIA MPDABAHIA @MPDABAHIA

WWW.MPBA.MP.BR
WWW.NUCCIBER.MPBA.MP.BR
NUCCIBER@MPBA.MP.BR
(71) 3103-6636/6639

Combate ao Crime

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA