# ANEXO


INTERPOL

"O desenvolvimento do ciberespaço:
uma ameaça à segurança internacional"

# GUIA DE POSICIONAMENTOS

**Caros delegados, buscando uma melhor compreensão do tema e das políticas adotadas pelos países que venham a representar, disponibilizamos para vocês este breve resumo de posicionamentos, juntamente com um guia de links, a fim de que sirvam como uma base de direcionamento em seus estudos.**

**Desejamos a todos uma boa leitura e proveitosas pesquisas!**

**Att,**

**Diretoria de Cibercrimes da Interpol.**

## ALEMANHA

A Alemanha, como o país que é, desde sempre procurou manter-se atualizada de todas a maneiras. E, tecnologicamente falando, apesar de sua derrota na Segunda Guerra Mundial - tendo que assinar diversos acordos de retaliação -, foi um país que conseguiu se reconstruir ainda mais desenvolvido.

Quando entramos no assunto de cibersegurança e cibercrimes, enxergamos que esse país está a frente de muitos programas, juntamente com o Brasil. Além de ter aprovado recentemente uma lei de cibersegurança para proteger suas infra-estruturas críticas, foi estabelecida uma aliança entre Alemanha e Brasil, na busca de combater os cibercrimes e procurar desenvolver novos projetos no mundo digital.

Seus projetos mais atuais são voltados principalmente para o setor digital, vindo a possuir até mesmo um Conselho Nacional de CiberSegurança, além de um sistema altamente desenvolvido chamado de Bundeskriminalamt (BKA), que opera em tempo integral para obter informações da polícia e da comunicação, alem de fornecer suporte

para todas as forças policiais federais e coordenar as atividades nacionais de supressão de crimes.

## ARÁBIA SAUDITA

A sede da Interpol na Arábia Saudita é localizada em sua capital, Riyadh e serve como principal meio de acesso para as investigações internacionais sobre o país e seus cidadãos, visando principalmente facilitar a luta contra o crime transnacional e a localização de fugitivos internacionais.

Como estratégia principal de segurança, a politica criminal saudita adota um aspecto mais liberal no que diz respeito ao acesso á informação, uma vez que a Interpol local concedeu aos oficiais comandantes das linhas policiais acesso direto ao banco de dados global da instituição, permitindo o fácil acesso a informações importantes sobre documentos de identificação e movimentação de pessoas.

Suas linhas principais de trabalho encontram-se focados no combate ao tráfico de pessoas, no combate ao cibercrime e ao bioterroristmo.

## AUSTRÁLIA

A Austrália, por ser um país desenvolvido, possui recursos aplicados em todos os setores de seu país. Sua economia é estável, sua infraestrutura é bem desenvolvida e sua sociedade bem cuidada.

Contudo, no tocante ao setor de cibersegurança o país está atrás da maioria. O próprio Centro Australiano para a Cibersegurança (ACSS, sigla em inglês) já emitiu aviso deixando clara a situação de incapacidade militar e de segurança na era digital.

Apesar disso, o país está desenvolvendo, aos poucos, algumas ferramentas que podem melhorar sua situação, como a Rede Australiana de Denúncia Online de

Cibercrimes (ACORN) - onde usuários poderão registrar suas denúncias e facilitar o trabalho da polícia - e leis para o combate a hackers.

Contudo, um ponto de grande relevância no país diz respeito à censura da internet, sendo constituída por um regime regulatório que funciona pela imposição de restrições sobre o conteúdo da Internet que é hospedado dentro da Austrália, criando uma memória de segurança contra sites no exterior que são pegos pelos mais variados nos softwares de filtragem.

## BRASIL

O Brasil é um dos países que, atualmente, está despertando cada vez mais para o mundo digital. Como o país ainda é muito novo nesse ramo, não pode-se dizer que está completamente imerso. Mas suas propostas inovadoras e projetos de lei estão cada vez mais próximos da realidade da Era da Informação.

Em meados de 2012, já surgia a Lei Carolina Dieckmann, falando sobre o vazamento de dados; em 2014, veio o Marco Civil da Internet, um documento que cria principalmente a previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado..Além disso, o Brasil já exporta módulos de criptografia para a Arábia Saudita e possui diversos projetos em parceria com a Alemanha, no desenvolvimento da cibersegurança e crimes digitais.

A INTERPOL Brasília tem trabalhado duro para assegurar o controle de imigração no Brasil, possibilitando aos oficiais brasileiros o acesso direto às bases de dados da Interpol. Usando a tecnologia conhecido como MIND, a polícia de choque rapidamente pode verificar se um passaporte apresentado à imigração consta como roubado em bancos de dados da Interpol, assegurando um combate mais eficiente e ágil a este e a muitos outros crimes internacionais.

## CANADÁ

O Canadá se insere no contexto da Era da Informação na medida em que age, principalmente, se defendendo de ataques de hackers e ciberterroristas, além de possuir o maior número de compartilhadores de arquivos per capita no mundo. Por ser um país que possui muitas informações importantes de países aliados – como os EUA, principalmente –, diversos serviços de inteligência estrangeiros – não necessariamente estatais – tendem a quebrar os sistemas canadenses atrás dessas informações, roubando informações industriais e segredos nacionais.

Em vista disso, o Canadá estabeleceu um programa chamado de *Estratégia Canadense de CiberSegurança*, no qual seu governo iria investir em torno de 142 milhões de dólares para, no período de 2010 à 2015, desenvolver novas ferramentas defensivas e maneiras mais eficientes de lidar com tais ataques; garantindo ao país uma melhoria considerável, mas ainda incipiente.

Além disso, Usando a tecnologia da INTERPOL conhecida como FIND, o Canadá tornou-se pioneiro ao criar uma interface entre dois bancos de dados chaves da Interpol e o banco de dados da polícia nacional canadense, possibilitando a agentes policiais de todo o território o acesso facilitado a informações críticas sobre quaisquer indivíduos considerados como ameaça.

## CINGAPURA

Cingapura é um país extremamente incorporado no contexto internacional. Desde que uniu-se com ex-territórios britânicos em 1963 para formar a Malásia e tornou-se um Estado independente dois anos mais tarde, aumentou exorbitantemente suas riquezas e transformou-se num dos Tigres Asiáticos – fato esse que lhe garantiu uma economia forte e independente, o quarto principal centro financeiro do mundo, considerado pelo Banco Mundial como o melhor lugar para se fazer negócios.

Por esse motivo, não é estranho encontrá-lo como um dos principais países ativos no que concerne à cibersegurança. A própria Interpol criou em 2014 um complexo contra cibercrimes localizado lá em Cingapura, uma vez que a demanda lá é muito grande, envolvendo não somente os cidadãos nacionais, como também empresas e cidadãos internacionais envolvidos com o país de qualquer maneira.

Além disso, a NEC Corporation inaugurou sua primeira fábrica de Cibersegurança em Cingapura, trabalhando em conjunto com a *Singapore Economic Development Board* (EDB) para lançar o Programa *Strategic Attachment and Training* (STRAT), que irá preparar a próxima geração de especialistas de TI em segurança cibernética.

## CHINA

A China é um país milenar; sempre conhecida por suas tradições e governos autoritários. Mas apesar disso, quando passou pela revolta palaciana de Deng Xiaoping – a qual abriu a China ao mercado internacional –, não somente a economia chinesa se recuperou, mas também sua concentração de tecnologia.

A partir daí, sua capacidade de domínio das novas tecnologias lhe garantiu os primeiros lugares no topo dos países mais eficazes no mundo virtual. Possuindo uma divisão especialista em Ciberguerra, a China hoje possui diversos programas capazes de defendê-la contra muitos dos ataques que lhe são direcionados; fato esse que ao contrário também funciona muito bem: a China é um dos líderes – se não o líder – em ataques hackers.

Dessa maneira, com sua potência militar cibernética, os EUA acabaram entrando em contato, a fim de firmar parcerias não somente no âmbito econômico, mas também, de poderio digital; nisso, optando por firmar um acordo de cibersegurança entre ambos os países.

## CUBA

Cuba, como já é do saber geral, é um país conturbado, que enfrentou diversos problemas e teve grandes dificuldades em se desenvolver. Graças ao bloqueio econômico dos Estados Unidos, o país sofreu muito até conseguir estabilidade novamente e, em virtude disso, tecnologicamente falando, é muito fraco e subdesenvolvido.

Nesse sentido, uma pequena parcela da população possui acesso a internet e até mesmo o próprio governo cubano tem dificuldades para lidar com a tecnologia ainda incipiente em seu país.

Não obstante, o governo tem começado a desenvolver a informatização da sociedade e começou a colocar a internet a serviço de todos, chegando a promover, no ano de 2014, a Primeira Oficina de Informatização e Cibersegurança, reunindo peritos do país para debater sobre os rumos que o país irá tomar.

## ESTADOS UNIDOS DA AMÉRICA

Os Estados Unidos da América é um dos países mais fortes, tecnologicamente falando. Foi lá que se desenvolveu praticamente tudo o que se conhece da internet. Movidos cada vez mais pelo domínio digital, hoje, em termos de cibersegurança e potência militar cibernética, os EUA estão bastante desenvolvidos, "competindo" diretamente com outras potências como a China, a Rússia e outros.

O próprio governo possui um conhecimento vasto sobre a internet e o mundo virtual, capacitando todas as suas esferas. Seus órgãos de atuação secreta estão entre os mais reconhecidos do mundo e grande parte disso se deve à manipulação do mundo digital.

Além disso, seus cidadãos tem um conhecimento muito grande em tecnologia de informação, garantindo ao país uma posição ainda mais a frente nesse ramo.

## FINLÂNDIA

A Finlândia é um dos países do continente europeu com grande domínio tecnológico e suas políticas de segurança de fronteiras chamam muito a atenção pelo fato de assegurarem vigilância total e especializada através de redes.

Por ser um país pequeno, seu governo conseguiu implantar internet – mais especificamente o acesso a banda larga – um direito fundamental. Ou seja, o conhecimento técnico da população ajuda a própria Finlândia a se desenvolver.

## FRANÇA

O diferencial da força policial francesa encontra-se na possibilidade de cada prefeito poder formar uma divisão municipal responsável pela aplicação das leis e regulamentos próprios para pequenos delitos da comunidade, contando ainda com a *Gendermerie Nationale*, uma força de aproximadamente 100.000 policiais.

Neste país, a atuação de Interpol toma forma através da ligação entre o órgão e os mecanismos policiais e judiciários franceses, estreitamente relacionados com os serviços de monitoramento territorial, possibilitando uma reação mais eficiente e direta nos problemas que venham a ocorrer.

Entre suas principais conquista no meio internacional, possuem a promulgação da “Lei de Criação e Internet”, sendo uma das mais severas nesse sentido em relação ao controle de informações, possuindo como principal órgão de monitoramento o “Hadopi”, uma autoridade pública e independente que verifica o fluxo informacional do país.

Possuem como principais frentes de atuação a luta contra o crime organizado, contra o tráfico de pessoas, os cibercrimes, tráficos de obras de arte, redes de imigração clandestina e principalmente os crimes relacionados a fortunas.

## IRÃ

A força policial iraniana forma uma organização independente liderada pelo chefe das forças armadas, característica que lhe atribui métodos de aspecto militar.

Apresentam ainda uma política inovadora no que diz respeito a uma força nacional de cyber polícia, formada com o intuito de proteger a informação e comunicação através do ciberespaço.

O sistema de censura na internet no Irã é um dos mais completos e sofisticados do mundo, sem contar que os avanços na capacidade técnica interna têm contribuído para a implementação de uma estratégia de filtragem centralizada e uma dependência reduzida em tecnologias ocidentais.

Denominada de Divisão Naja, esta célula visando garantir principalmente a proteção das identidades nacionais e religiosas de seus cidadãos, a autoridade do pais em meio cibernético, a proteção da infraestrutura crítica contra ataques eletrônicos ao governo, o impedimento das invasões a sistemas e redes, tudo através de uma forca policial voltada para a área das tecnologias da informação e conhecimentos digitais.

## JAPÃO

A Agencia Nacional de Polícia Japonesa supervisiona e controla as atividades de mais de 47 departamentos policiais distritais. Localizada em Tóquio, a agência da Interpol japonesa aposta em uma funcionalidade comunicativa bastante desenvolvida para o intercambio e cruzamento de informações, permitindo uma maior precisão na investigação dos fatos que lhe competem.

Além disso, as forças policiais da instituição colaboram diretamente com os mecanismos de fortalecimento da lei, na tentativa de derrubar a globalização criminal.

Em outro sentido, destaca-se ainda por ser uma das sedes da Interpol que mais sedia a maior parte das conferências relacionadas ao aperfeiçoamento das unidades policiais, principalmente através de seus parceiros na Ásia e no Pacifico, possuindo atuação principal nas áreas de crimes cibernéticos, segurança nuclear, e combate ao contrabando de veículos.

## NOVA ZELÂNDIA

Os objetivos principais da polícia neozelandesa são a redução da criminalidade e a seguridade social, através de um sistema de segurança operacional 24h por dia, além de possuir divisões terrestres, aéreas e marítimas.

Grande parte da população da Nova Zelândia possui acesso à internet doméstica, o que leva o país a ter grande cautela quanto ao material relacionado à pornografia infantil, de modo a evitar sua difusão e armazenamento, por meio de uma unidade que monitora diversos sites em busca de atividade ilegal.

Sua forma de atuação se baseia na promoção da troca de informações e pelo fornecimento de assistência investigativa entre a polícia neozelandesa e as agências da INTERPOL de outros países membros, buscando sempre a intensificação da cooperação em função do enfrentamento de práticas criminosas.

## REINO UNIDO

A força policial do pais caracteriza-se por não funcionar por meio de uma unidade central, mas sim pela integração de 44 unidades setoriais que atuam em um sistema interligado e bem organizado.

Com a sede em Manchester, a Interpol do Reino Unido partilha da mesma bandeira do órgão internacional, providenciando um sistema completamente integrado e

eficiente na troca de informações entre as agencias policiais e os oficiais operadores da justiça.

Possuem divisões especializadas na quebra de criptografia e tradução, além de possuir uma divisão em sub agencias que cuidam da cobertura territorial integrada, em razão de tratar-se de um território separado por fronteiras marítimas.

Buscando garantir altos níveis de segurança em seus territórios, o sistema policial busca amparo em leis de extremo rigor e solidez.

Possui como marca as iniciativas voltadas ao território caribenho, em assistência que busca acabar com o terrorismo internacional e o crime organizado.

## RÚSSIA

A Rússia já passou por períodos muito turbulentos. À época da Guerra Fria, o país competia constantemente com os EUA, principalmente em desenvolvimento militar, mas também em todas as esferas. E isso se perpetua até os dias atuais, levando essa richa para o âmbito virtual.

Sendo considerada uma das maiores potências cibernéticas do mundo, juntamente dos EUA e China, principalmente, a Rússia foi classificada como o país com maior quantidade de hackers perigosos, os quais conseguem invadir diversos dispositivos em qualquer parte do mundo sem muitas dificuldades.

Não obstante, apesar de toda a richa com os EUA, em 2013 ambos os países se reuniram em conjunto com a China para discutir métodos de combate ao Cibercrime e procurar regulamentar o ciberespaço.

Além disso, a INTERPOL Russa localiza-se na cidade de Moscou, procurando combater, principalmente, o tráfico de drogas e armas via ciberespaço e o crime organizado.

## SUÍÇA

Os bancos suíços são mundialmente famosos por sua política de proteção máxima de suas contas bancárias, raramente abrindo exceções. E essa conduta de proteção deles não fica somente somente nessa etapa: a Suíça agora se propõe a proteger os dados de empresas que a solicitem.

Logo depois do pronunciamento de Edward Snowden, uma quantidade massiva de empresas descobriu-se desprotegida e, procurando amparo para proteger-se, empresas suíças especializaram-se na proteção de dados.

Nesse diapasão, somente no país, 64 centros de proteção encontram-se instalados, colocando-a na posição de quinto país europeu mais bem seguro.

## GUIA DE LINKS

### Alemanha:

1. http://www.interpol.int/Member-countries/Europe/Germany
   http://www.germany.info/
2. http://interpol.einnews.com/country/germany
3. http://www.interpol.int/News-and-media/News/2015/N2015-099
   http://www.interpol.int/News-and-media/News/2009/PR111
4. https://www.europol.europa.eu/category/press-release-category/cybercrime

### Arábia Saudita:

1. http://interpol.einnews.com/country/saudiarabia
2. http://www.interpol.int/Member-countries/Asia-South-Pacific/Saudi-Arabia
3. http://www.saudi.gov.sa/wps/portal/
4. http://www.interpol.int/News-and-media/News/2011/N20110323

### Austrália:

1. http://www.australia.gov.au
2. http://www.dfat.gov.au
3. http://g1.globo.com/tecnologia/blog/seguranca-digital/post/saiba-se-seus-dados-foram-vazados-com-o-have-i-been-pwned.html

4. http://www.lifehacker.com.au/2016/03/warning-new-cyber-threat-hits-australias-major-banking-apps/
5. http://www.bbc.com/portuguese/noticias/2015/12/151214_virus_chantagem_rb
6. http://www.afr.com/brand/chanticleer/israels-cyber-security-expert-details-his-protection-network-20160309-gnetvr

**Brasil:**

1. http://www.brasil.gov.br/
2. http://www.cebri.org/
3. http://computerworld.com.br/por-que-o-brasil-se-tornou-o-segundo-maior-gerador-de-cibercrime-do-mundo
4. http://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html
5. http://187.45.221.194/cgi/cgilua.exe/sys/start.htm?infoid=41500&sid=18
6. http://www.tecmundo.com.br/seguranca-de-dados/92800-relatorio-kaspersky-revela-submundo-cibercrimes-brasil.htm

**Canadá:**

1. www.international.gc.ca/international/index.aspx
2. https://www.canada.ca/en/index.html?_ga=1.48169572.2108973576.1410829970
3. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx
4. http://www.cbc.ca/news/technology/canada-cybercrime-hacking-seglins-1.3312153
5. http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html

**Cingapura:**

1. http://www.gov.sg
2. http://www.siiaonline.org/page/Home
3. http://pt.euronews.com/2014/09/30/interpol-cria-complexo-contra-o-cibercrime-em-singapura/
4. http://www.bit.pt/singapura-em-alerta-elevado-ciber-ataques/

**China:**

1. http://www.gov.cn/english/
2. http://www.interpol.int/Member-countries/Asia-South-Pacific/China
3. http://www.chinadaily.com.cn/china/2015-04/23/content_20521796.htm
4. http://br.china-embassy.org/por/szxw/t1324954.htm
5. http://www.interpol.int/News-and-media/News/2015/N2015-157
6. http://interpol.einnews.com/country/china

**Cuba:**

1. http://www.cubagob.cu/
2. http://observador.pt/2014/07/17/russia-vai-investir-em-infra-estruturas-em-cuba-e-podera-mesmo-reabrir-centro-de-espionagem/
3. http://navalbrasil.com/cuba-defende-em-genebra-direito-humano-a-privacidade/
4. http://www.diariodocentrodomundo.com.br/a-confissao-do-espiao-cubano-rene-gonzalez/

**Estados Unidos da América:**

1. http://www.usa.gov/
2. http://www.state.gov/index.htm
3. https://www.nsa.gov/
4. http://www.redebrasilatual.com.br/mundo/2016/02/otan-anuncia-acordo-com-uniao-europeia-para-combater-cibercrime-1771.html5
5. http://www.theguardian.com/world/pris
6. http://observador.pt/2016/03/07/entrevista-paul-mockapetris/
7. http://blogs.estadao.com.br/link/obama-quer-us-19-bilhoes-para-combater-cibercrime/
8. http://www.segs.com.br/info-ti/4369-ransomware-o-malware-sequestrador-ameaca-a-seguranca-de-dados-nas-pequenas-e-medias-empresas.html

**Finlândia:**

1. http://valtioneuvosto.fi/en/frontpage

2. http://formin.finland.fi/public/default.aspx?culture=en-US&contentlan=2
3. http://agenciabrasil.ebc.com.br/internacional/noticia/2016-02/otan-anuncia-acordo-com-uniao-europeia-para-combater-cibercrime
4. https://www.intermin.fi/en/security/combating_crime/cyber_crime
5. http://jakartaglobe.beritasatu.com/news/finland-offers-help-tackling-indonesias-cyber-crimes/

**França:**

1. http://www.gouvernement.fr/en/news
2. http://www.diplomatie.gouv.fr/en/
3. http://www.interpol.int/Member-countries/Europe/France
4. http://interpol.einnews.com/country/france
5. https://www.publico.pt/destaque/jornal/interpol-inglesa-pediu-colaboracao-da-justica-francesa-mas-nao-prendeu-pierre-falcone-187895
6. http://www.france24.com/en/20121109-france-french-woman-elected-interpol-first-female-president-ballestrazzi-crime-police
7. http://www.france24.com/en/tag/interpol/

**Irã:**

1. http://www.president.ir/en/
2. http://cyber.police.ir/
3. http://www.ibtimes.com/iran-saudi-arabia-heading-toward-cyber-war-1989789
4. http://www.thedailybeast.com/articles/2015/04/06/is-the-u-s-iran-cyber-war-over.html
5. http://www.defesanet.com.br/cyberwar/noticia/13301/Ira-denuncia-plano-internacional-de-ciberataque-contra-programa-nuclear/

**Japão:**

1. http://interpol.einnews.com/country/japan
2. http://www.interpol.int/Member-countries/Asia-South-Pacific/Japan
3. http://www.br.emb-japan.go.jp/itprtop_pt/index.html
4. http://www.japan.go.jp/

5. http://asia.nikkei.com/Politics-Economy/International-Relations/Japan-plays-key-role-in-Interpol-s-new-cybercrime-center
6. http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/Events2/INTERPOL-National-Cybercrime-Training-Seminar

**Nova Zelândia:**

1. https://www.govt.nz
2. https://www.mfat.govt.nz
3. http://www.newshub.co.nz/nznews/spying-legislation-needs-major-upheaval-2016031112#axzz42Y6YURiH
4. http://asiapacificreport.nz/2016/03/10/selwyn-manning-more-intrusive-spy-laws-loom-for-nz/
5. http://www.nzherald.co.nz/kpmg/news/article.cfm?c_id=1503886&objectid=11588563

**Reino Unido:**

1. https://www.gov.uk/
2. https://www.gov.uk/government/organisations/department-for-international-development
3. http://expresso.sapo.pt/economia/2015-11-08-Sonae-desmantelou-rede-de-cibercrime
4. http://agenciabrasil.ebc.com.br/internacional/noticia/2016-02/otan-anuncia-acordo-com-uniao-europeia-para-combater-cibercrime
5. http://idgnow.com.br/seguranca/2011/02/21/cibercrimes-custam-us-43-5-bilhoes-por-ano-a-economia-do-reino-unido/
6. http://24.sapo.pt/article/sapo24-blogs-sapo-pt_2016_02_08_1401895288_interpol-junta-se-ao-barclays-para-combater-o-cibercrime

**Rússia:**

1. http://government.ru/en/

2. http://www.gov.ru/main/ministry/isp-vlast44_en.html
3. http://www.interpol.int/Member-countries/Europe/Russia
4. http://interpol.einnews.com/country/russia
5. http://gazetarussa.com.br/tag/interpol
6. http://www.euronews.com/newswires/3148898-interpol-refuses-russian-request-for-khodorkovsky-search-notice-tass/

**Suíça:**

1. https://www.admin.ch/gov/en/start.html
2. http://swiss-government-politics.all-about-switzerland.info/
3. http://www.interpol.int/Member-countries/Europe/Switzerland
4. http://interpol.einnews.com/country/switzerland
5. http://espn.go.com/sports/soccer/news/_/id/6641147/switzerland-quiz-interpol-fifa-donation