Estrutura de Segurança, Estabilidade e Resiliência

A ICANN é uma organização global que coordena os sistemas de identificadores exclusivos da Internet para proveito público no mundo todo, proporcionando uma só Internet interoperável.

Março de 2013

Índice

Lista de figuras

Resumo Executivo

A Internet prosperou enquanto ecossistema atraindo muitos participantes por meio da colaboração em um ambiente aberto e transparente. A Internet incentiva o compartilhamento de conhecimento, criatividade e comércio em um bem comum a todos. A interoperabilidade desse bem comum a todos depende da operação e da coordenação dos sistemas de identificadores exclusivos da Internet e de uma Internet saudável, estável e resiliente.[1]

A ICANN e os operadores reconhecem que manter e melhorar a segurança, a estabilidade e a resiliência desses sistemas é um elemento essencial de sua relação colaborativa.

Desde 2009, a ICANN publica anualmente uma Estrutura de Segurança, Estabilidade e Resiliência (SSR). A Estrutura é reconhecida na Afirmação de Compromissos[2] e foi analisada positivamente pela Equipe de Revisão (RT) de Segurança, Estabilidade e Resiliência[3] como parte do processo de revisão da Afirmação de Compromissos.

A Estrutura de SSR descreve a função e os limites da ICANN na manutenção de uma Internet global única e interoperável, além dos desafios enfrentados com os sistemas de identificadores exclusivos da Internet. O documento é dividido em duas partes. A Parte A explica a base para a função da ICANN em segurança, estabilidade e resiliência, o ecossistema da Internet e a comunidade da ICANN. A Parte B descreve os objetivos estratégicos da ICANN para SSR e as atividades planejadas para o ano operacional do AF (Ano Fiscal) de 2014 (de julho de 2013 a junho de 2014).

A principal mudança na Estrutura do AF de 2014, em comparação ao de 2013, é a adoção das recomendações da Equipe de Revisão de SSR em outubro de 2012[4] e as reações aos avanços do ecossistema da Internet desde que a versão anterior foi publicada, em junho de 2012 (consulte a Parte B). As atividades projetadas para o AF de 2014 serão focadas na manutenção de um ecossistema saudável, a fim de fornecer a base para uma Internet mais estável, confiável e resiliente para a comunidade global.

A Estrutura do AF de 2014 está sendo disponibilizada como um documento único para facilitar a tradução e o compartilhamento no próximo encontro da ICANN em Pequim, China, nos dias 7 a 11 de abril de 2013.

---

[1] De acordo com os estatutos da ICANN, a ICANN coordena a alocação e a atribuição dos três conjuntos de identificadores exclusivos da Internet: os nomes de domínio (formando um sistema conhecido como DNS); os endereços IP (Internet Protocol) e os números de AS (Sistema Autônomo); e os números de parâmetro e porta de protocolo.

[2] Afirmação de Compromissos entre o Departamento de Comércio dos Estados Unidos e a ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[3] Relatório Final da Equipe de Revisão de Segurança, Estabilidade e Resiliência, 20 de junho de 2012, http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

[4] Adoção das recomendações da Equipe de Revisão de SSR pela Diretoria da ICANN, 18 de outubro de 2012, http://www.icann.org/en/about/aoc-review/ssr/board-action.

Parte A — Seção sobre a base para a função da ICANN

Missão e valores centrais da ICANN

"A missão da ICANN é coordenar, de forma geral, os sistemas de identificadores exclusivos da Internet globais e, particularmente, garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet."

Estatutos da ICANN, incluindo alterações de 20 de dezembro de 2012 (http://www.icann.org/en/about/governance/bylaws#I)

Valor central 1: "Preservar e aprimorar a segurança, a credibilidade e a estabilidade operacional e a interoperabilidade global da Internet."

Esse valor central é reconhecido na Afirmação de Compromissos, em que "a coordenação técnica global da infraestrutura subjacente da Internet (o DNS) é necessária para garantir a interoperabilidade" e "preservar a segurança, a estabilidade e a resiliência do DNS" são compromissos essenciais para o proveito de todos os usuários da Internet.

Competência e função de SSR da ICANN

No processo de revisão da Afirmação de Compromissos, a Equipe de Revisão de SSR recomendou à ICANN "publicar uma declaração clara e consistente de sua competência e a missão técnica limitada de SSR". (Recomendação 1, 20 de junho de 2012).

Uma declaração preliminar da função e a competência da ICANN com relação à segurança, estabilidade e resiliência dos identificadores exclusivos da Internet foi publicada em maio de 2012 (http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm) e revisada após os comentários públicos e a discussão nos encontros da ICANN em Praga (junho de 2012) e Toronto (outubro de 2012), http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf).

A descrição abaixo da competência e da função da ICANN tem como objetivo atender à Recomendação 1:

Como uma organização global composta por múltiplas partes interessadas, a ICANN facilita a segurança, a estabilidade e a resiliência dos sistemas de identificadores exclusivos da Internet por meio da coordenação e colaboração.

A comunidade espera que a ICANN, enquanto organização global, desempenhe sua função de modo aberto, responsável e transparente e abrangendo a diversidade de partes interessadas em todo o ecossistema da Internet.

Dentro de sua missão técnica, a função de SSR da ICANN abrange três categorias de responsabilidade:

1. As responsabilidades operacionais da ICANN (gerenciamento de riscos organizacionais de operações internas, incluindo servidor de raiz "L", operações de DNS, operações de atribuição de chaves DNSSEC, funções de IANA, novas operações de TLD, gerenciamento do banco de dados de fusos horários);

2. A participação da ICANN enquanto coordenadora, colaboradora e facilitadora com a comunidade global em questões de políticas e técnicas relacionadas aos identificadores exclusivos da Internet;
3. A dedicação da ICANN com os demais integrantes do ecossistema global da Internet.

Figura 1 — Missão técnica da ICANN

Definições para esta Estrutura

Segurança: a capacidade de proteger e prevenir o uso impróprio dos identificadores exclusivos da Internet.

Estabilidade: a capacidade de garantir o funcionamento esperado do sistema e que os usuários dos identificadores exclusivos tenham certeza de que o sistema funcionará conforme o esperado.

Resiliência: a capacidade de resistência/tolerância/sobrevivência do sistema de identificadores exclusivos a ataques maliciosos e outros eventos que causam interrupções sem resultar na interrupção ou paralisação do serviço.

Observação: essas definições não foram alteradas desde a Estrutura de SSR do AF de 2012, publicada em 2011.

Com base no trabalho do 2º Simpósio de Segurança do DNS (realizado em Kyoto, Japão, em 2010) e do 3º Simpósio de Segurança do DNS (realizado em Roma, Itália, em 2011), uma definição inicial de **Integridade de Identificador Exclusivo** foi incluída na Estrutura de SSR do AF de 2014. Com base na definição incluída no relatório do Simpósio de Kyoto para Integridade do DNS, esse conceito foi adaptado da seguinte maneira:

> Um estado de funcionamento geral dos identificadores exclusivos da Internet que está dentro dos limites técnicos nominais nas dimensões de coerência, integridade, velocidade, disponibilidade, vulnerabilidade e resiliência.

Uma definição da disciplina de economia ecológica descreve integridade de ecossistema como "uma medida do desempenho geral de um sistema complexo obtida a partir do comportamento de suas partes".[5]

As responsabilidades fora do escopo da função de SSR da ICANN incluem:

- A ICANN não desempenha uma função de controle sobre a Internet nem de combater operacionalmente comportamentos criminosos;
- A ICANN não tem uma função relacionada ao uso da Internet para espionagem cibernética nem guerra cibernética;
- A ICANN não tem a função de determinar o que constitui uma conduta ilícita na Internet.

Enquanto organização, a ICANN não se trata de um organismo encarregado pelo cumprimento da lei, um tribunal de justiça nem um órgão governamental. Os governos e os organismos encarregados pelo cumprimento da lei participam como partes interessadas no desenvolvimento de políticas e nos processos da ICANN.

A ICANN não é responsável por dar suporte ao trabalho de organismos encarregados pelo cumprimento da lei nem de órgãos governamentais na execução de ações legítimas quando solicitada. A ICANN participa junto com a comunidade de segurança operacional no estudo, na análise e na identificação de uso malicioso ou abuso do DNS.

A ICANN não pode suspender nem cancelar nomes de domínio unilateralmente. A ICANN pode executar seus contratos por meio de terceiros, incluindo fornecedores de registro de nome de domínio.

---

[5] Esse conceito é adaptado de "What is a healthy ecosystem?" ("O que é um ecossistema saudável"), de Robert Costanza e Michael Mageau, University of Maryland Institute for Ecological Economics, 1999, publicado em Aquatic Ecology, http://geminis.dma.ulpgc.es/profesores/personal/jmpc/Master08%28PrimeraEdici%F3n%29/Homeostasis/Homeo03s.pdf, http://books.google.com/books?id=YTeCxF5gqMQC&dq=ecosystem+and+health. O conceito descrito também foi influenciado por "A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective" ("Uma Estrutura para Analisar a Robustez de Sistemas Sócio-ecológicos de uma Perspectiva Institucional") (2004), http://www.ecologyandsociety.org/vol9/iss1/art18/.

A ICANN desempenha a mesma função que qualquer outra parte interessada com relação aos protocolos de Internet; a evolução dos protocolos da Internet e as normas relacionadas não fazem parte da jurisdição da ICANN. A ICANN apoia o desenvolvimento aberto de normas por meio de processos colaborativos com várias partes interessadas.

O desafio

O uso impróprio do DNS e de redes globais, bem como ataques a eles, são um desafio para a segurança do identificador exclusivo. Os ataques ao DNS são direcionados a um grande número de usuários, pessoas, empresas, sociedade civil e governos.

À medida que aumentam a frequência e a sofisticação de eventos que causam interrupções e outros comportamentos maliciosos, a ICANN e a comunidade global devem dar continuidade a uma colaboração que vise um ecossistema saudável, melhorando a resiliência dos sistemas de identificadores exclusivos e fortalecendo seus recursos.

A atividade na Internet reflete todo o âmbito de motivações e condutas humanas. Em parte, essa atividade reflete a natureza aberta da Internet que a tornou tão bem-sucedida, possibilitou grandes inovações e permitiu o compartilhamento de conhecimento, criatividade e comércio em um bem comum a todos.

No atual ambiente de governança colaborativa da Internet com várias partes interessadas em um ecossistema maior de Internet, as visões tradicionais de segurança cibernética conforme ditadas por um setor, seja ele o governamental ou o privado, não funcionam. Os governos e os integrantes individuais do setor privado não têm a competência administrativa ou legal adequada sobre o conjunto diversificado de sistemas e redes interconectados, e a dimensão da tarefa de operar e proteger esses recursos vai além do alcance de qualquer um deles, a menos que haja um esforço colaborativo e com vários participantes.

Todas as partes interessadas na segurança cibernética devem adotar uma visão mais ampla. A segurança no contexto dos identificadores exclusivos da Internet deve ser abordada por meio de um ecossistema saudável da Internet. Essa abordagem se concentra em uma Internet sustentável ou saudável, estável e resiliente. Um sistema sustentável para o futuro. Precisamos nos concentrar coletivamente no ecossistema no que diz respeito a sua "capacidade de manter a estrutura e de funcionar com o passar do tempo diante da pressão externa".[6]

No ano passado houve um aumento de ameaças contra os sistemas de identificadores exclusivos da Internet. Os ataques contra os operadores de registro de domínio de primeiro nível (consulte a declaração da IEDR de novembro de 2012, https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf e um artigo de novembro de 2012 na *Techcrunch* sobre PKNIC, http://ta.gg/5uf), registradores, setor bancário, organismos encarregados pelo cumprimento da lei e as ameaças contra operadores de servidor raiz apareceram nos noticiários em 2012. Consulte o "Arbor Networks Worldwide Infrastructure Security Report" ("Relatório de Segurança da Estrutura das Redes Mundias da Arbor"), janeiro de 2013, http://www.arbornetworks.com/research/infrastructure-security-report.

[6] Costanza e Mageau, et al.

A intervenção governamental fez com usuários perdessem a conectividade com o mundo exterior, por exemplo, na Síria (acesse http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml). O furacão Sandy afetou a conectividade da Internet na região nordeste dos Estados Unidos, mostrando a força que desastres naturais têm sobre as redes globais (consulte o "Preliminary Analysis of Network Outages During Hurricane Sandy" ["Análise Preliminar de Interrupções de Redes Durante o Furacão Sandy"], relatório técnico ISI-TR-685b da USC/ISI, novembro de 2012, ftp://ftp.isi.edu/isi-pubs/tr-685.pdf).

Algumas tendências inibidoras do aprimoramento da integridade de identificadores exclusivos incluem a baixa taxa de adoção de DNSSEC por registradores, desenvolvedores de navegadores e aplicativos e registrantes. A maior conscientização do uso criminoso do DNS estimulou o interesse em desenvolver táticas e ferramentas para acompanhar essa evolução.

Outras tendências foram observadas:

- O crescimento contínuo da adoção de DNSSEC por operadores de TLD
- A expansão de instâncias de servidor raiz em todo o mundo
- Novos ccTLDs (IDN e não IDN) adicionais lançados em um número cada vez maior de idiomas e conjuntos de caracteres
- O progresso crescente da avaliação de aplicativos no programa de novos gTLDs e o esperado lançamento de novos gTLDs em 2013
- O aumento do interesse na capacitação para a segurança cibernética, estimulando a realização de treinamentos do DNS que incluem, além das comunidades operacionais, os organismos encarregados pelo cumprimento da lei e a comunidade jurídica.

O ecossistema da Internet e a comunidade da ICANN

A ICANN funciona para o proveito da comunidade da Internet como um todo. O público é um conjunto diversificado de comunidades unidas pela Internet e funcionando como um ecossistema complexo. A Internet hoje é essencial para possibilitar o conhecimento global e a troca de informações, comércio e governança. Declaração da UNESCO em Vancouver, setembro de 2012 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) e WSIS+10, "Toward Knowledge Societies for Peace and Development, Final Statement" ("Rumo a Sociedades de Conhecimento pela Paz e Desenvolvimento, Declaração Final"), 27 de fevereiro de 2013 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

A Internet é reconhecidamente fundamental para dar suporte à economia e ao desenvolvimento sustentável mundial (consulte o "OECD Internet Economy Outlook" ["Panorama da OECD sobre a Economia na Internet"], em 2012, http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

O termo "ecossistema" descreve o mundo natural a nosso redor. Ele pode ser definido como a rede de interações entre os organismos, bem como entre os organismos e seu ambiente. Os ecossistemas são entidades dinâmicas. A Internet é um ecossistema e é também uma rede de

organizações e comunidades. Essas organizações e comunidades funcionam juntas e cada uma desempenha sua função. A Internet é bem-sucedida e próspera porque seu ecossistema é aberto, transparente e colaborativo.

O Ecossistema da Internet é composto por uma série de organizações e processos que moldam a coordenação e o gerenciamento da Internet global e permitem seu funcionamento geral. Essas organizações incluem: organizações de tecnologia e engenharia, operadores de rede, organizações de gestão de recursos, usuários, sociedade civil, entidades comerciais e não comerciais, educadores, elaboradores de políticas, organismos encarregados pelo cumprimento da lei e governos.

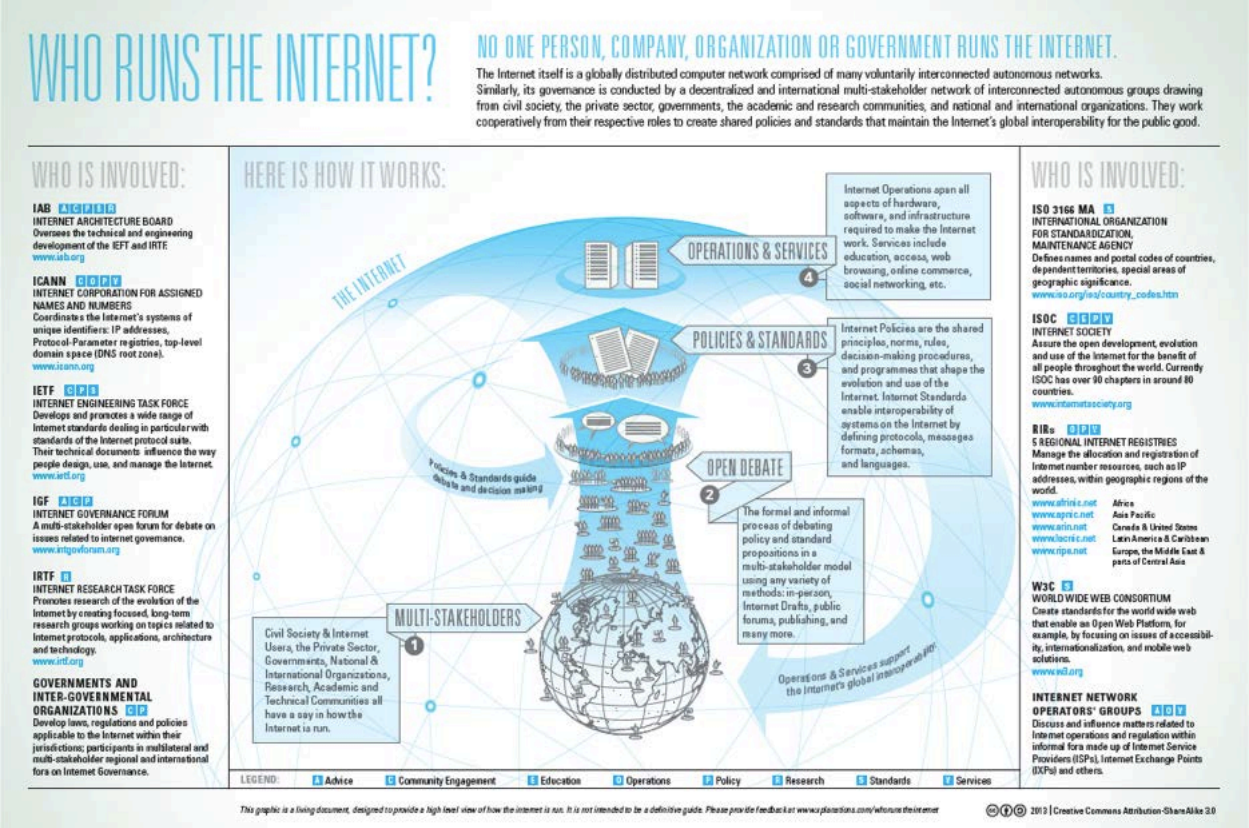


Figura 2 — Gráfico informativo do ecossistema da Internet

Do ponto de vista da ICANN, o ecossistema da Internet pode ser dividido em três camadas:

- a comunidade global,
- a comunidade da ICANN
- e a ICANN enquanto organização.

A comunidade global inclui pessoas que dependem de um sistema de identificadores exclusivos saudável, estável e confiável para o compartilhamento de conhecimento, comércio e inovação, mas que podem não estar cientes disso ou participam da ICANN.

A comunidade da ICANN contém o maior grupo de integrantes envolvidos nos programas, processos e atividades da ICANN, os quais impulsionam o modelo de desenvolvimento de políticas com várias partes interessadas para o proveito de todos os usuários da Internet.

A ICANN enquanto organização descreve as estruturas operacionais, as funções e dá apoio à equipe de suporte da comunidade da ICANN no geral e da coordenação com várias partes interessadas dos identificadores exclusivos da Internet.

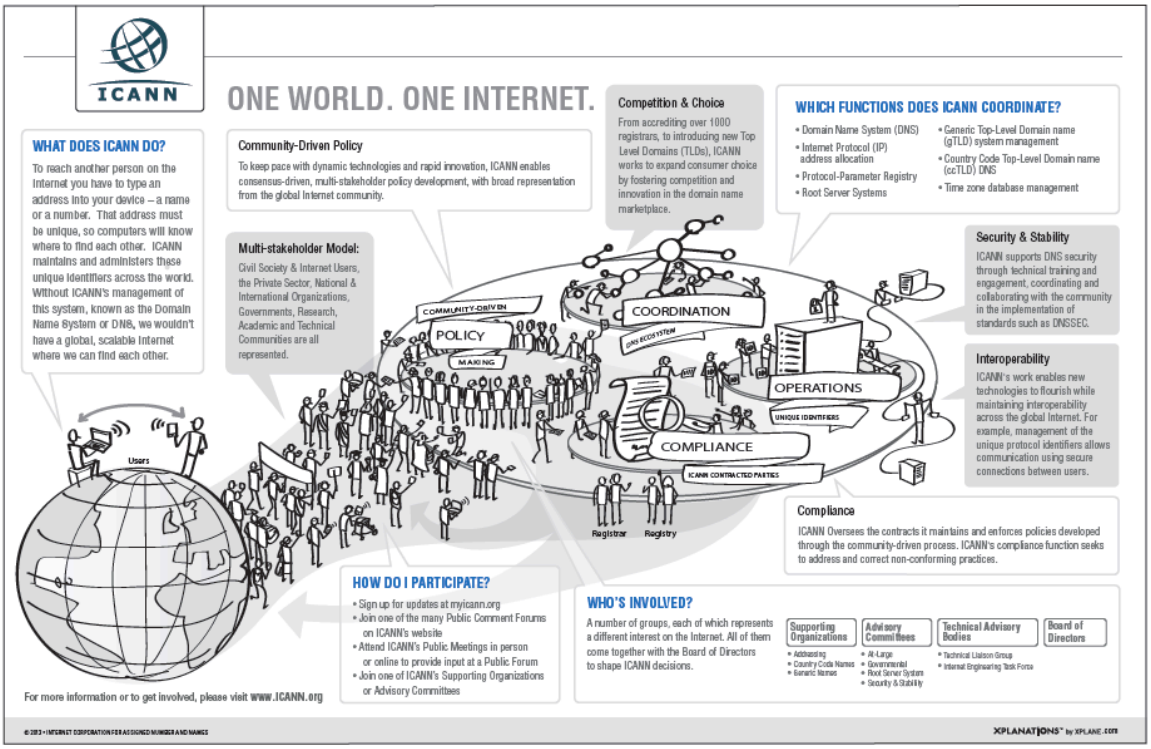


Figura 3 — Gráfico informativo da ICANN

Uma cópia completa 11x17 do gráfico informativo acima está disponível em seis idiomas em https://community.icann.org/display/ISBM/Handouts+for+Speakers+Bureau.
A comunidade participa na ICANN por meio de grupos de partes interessadas, grupos constituintes, organizações de apoio e comitês consultivos. Para obter mais informações sobre os comitês consultivos acesse as páginas abaixo:

1. Comitê Consultivo At-Large — http://www.atlarge.icann.org/alac
2. Comitê Consultivo para Assuntos Governamentais — https://gacweb.icann.org/
3. Comitê Consultivo do Sistema de Servidores Raiz — http://www.icann.org/en/groups/rssac
4. Comitê Consultivo de Segurança e Estabilidade — http://www.icann.org/en/groups/ssac

Esses comitês oferecem conselhos para a Diretoria da ICANN, fornecem informações sobre os processos de desenvolvimento de políticas e incentivam a participação da comunidade.

O desenvolvimento de políticas é realizado por três Organizações de Apoio:

1. Organização de Apoio de Endereços (ASO) — http://aso.icann.org/ (endereços IP)
2. Organização de Apoio para Nomes de Domínio com Código de País (ccNSO) — http://ccnso.icann.org/ (ccTLDs)
3. Organização de Nomes Genéricos — http://gnso.icann.org (gTLDs)

Desde a formação da ICANN em 1998, há 15 anos, o DNS cresceu de algumas centenas de milhares de nomes de domínio, distribuídos entre sete domínios de primeiro nível e aproximadamente 250 TLDs com código de país, para um DNS com mais de 250 milhões de nomes de domínio, usados por 2,5 bilhões de usuários da Internet em 316 TLDs. Esse espaço deve aumentar drasticamente com o lançamento de novos TLDs genéricos em 2013.

Até março de 2013, havia 316 TLDs delegados na zona raiz. O gráfico a seguir explica como esses TLDs estão categorizados.

Figura 4 — TLDs de zona raiz (crédito de imagem: Kim Davies, IANA)

Relações de SSR

A ICANN mantém parcerias e relações com terceiros (registros de nome de domínio e registradores, prestadores de garantia, entre outros), memorandos de entendimento, estruturas de responsabilidade ou tratados. Há também relações menos formais ou sem uma estrutura definida entre a ICANN e outras organizações internacionais ou partes interessadas do ecossistema. https://www.icann.org/en/about/agreements.

Os participantes do processo de registro de nome de domínio devem trabalhar juntos para garantir que as decisões relacionadas à coordenação global técnica dos identificadores exclusivos da Internet sejam tomadas tendo em vista o interesse público e sejam justificáveis e transparentes.

A imagem abaixo representa a natureza das relações no processo de registro de domínios.

Como parte das Recomendações 4 e 5 da Equipe de Revisão de SSR, a ICANN está elaborando uma documentação e definição da natureza de suas relações de SSR dentro da comunidade da ICANN. Isso ajudará a fornecer um ponto de foco único para entender as interdependências entre as várias organizações e entidades, cada qual com suas respectivas funções, permitindo que a ICANN realize disposições eficientes de trabalho a fim de apoiar suas metas e objetivos estratégicos de SSR.

Parte B — Módulo de SSR para o AF de 2014

Esta seção da Estrutura de Segurança, Estabilidade e Resiliência se concentra nas atividades e iniciativas de SSR projetadas para o Ano Fiscal de 2014, abrangendo o período de 1 de julho de 2013 a 30 de junho de 2014.

Segurança no Plano Estratégico da ICANN

O Plano Estratégico da ICANN identifica a segurança e a estabilidade do DNS como uma das quatro áreas estratégicas de concentração para a organização. Isso condiz com a grande importância dada à SSR na Afirmação de Compromissos. O Plano Estratégico separa o amplo escopo de responsabilidades de segurança, estabilidade e resiliência da ICANN em objetivos estratégicos, trabalho da comunidade, projetos estratégicos e trabalho de equipe.

O Plano Estratégico de 2012 a 2015 da ICANN não será alterado em 2013 (acesse https://www.icann.org/en/news/announcements/announcement-28jan13-en.htm). Esse é o mesmo Plano Estratégico publicado antes da Estrutura de SSR do AF de 2013 (junho de 2012). Foi constatado por meio de comentários no ciclo de planejamento de 2013 que há uma demanda contínua da comunidade por treinamento e atividades de capacitação. Isso mostra o apoio à participação técnica fornecida pela Equipe de Segurança da ICANN.

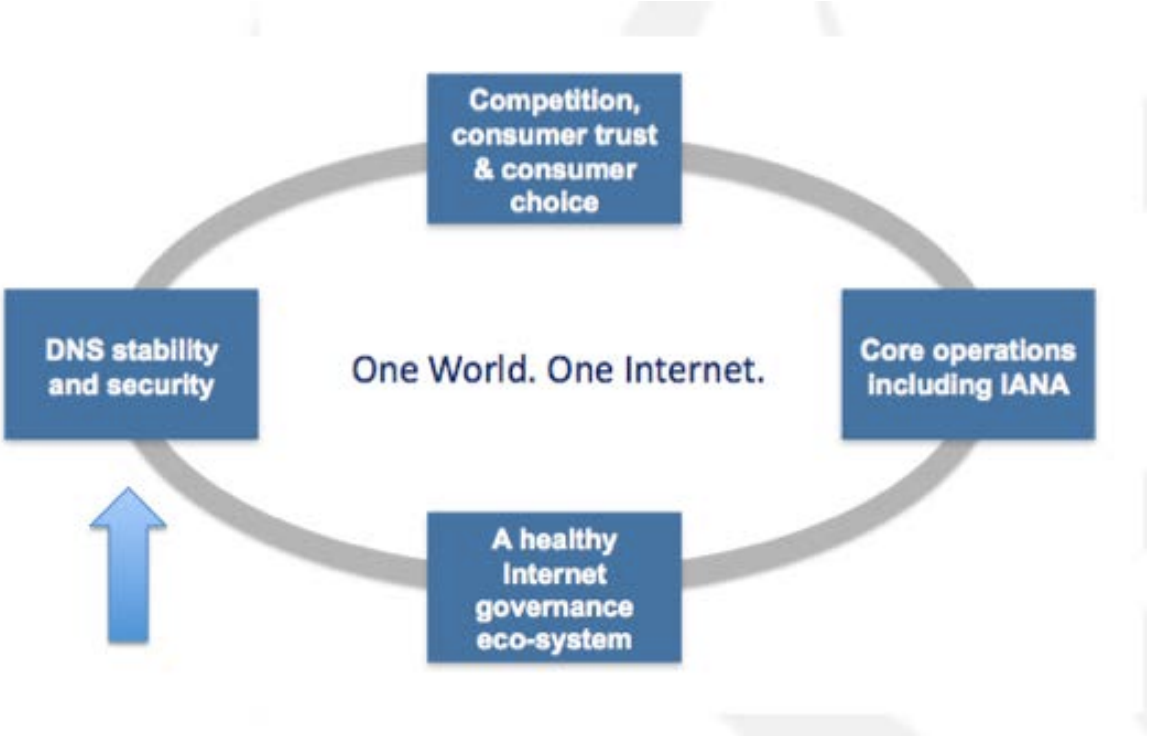


Figura 5 — Plano Estratégico da ICANN

O Plano Estratégico de 2012 a 2015 descreveu 5 Objetivos Estratégicos para a Segurança e a Estabilidade do DNS:

1. Manter e estimular a disponibilidade do DNS
2. Melhorar o gerenciamento de riscos e a resiliência do DNS, endereços IP e parâmetros
3. Promover a ampla adoção de DNSSEC
4. Aprimorar a cooperação internacional do DNS
5. Melhorar a resposta a incidentes de segurança do DNS

Em junho de 2013, a ICANN dará início a um processo de planejamento estratégico focado em um plano a longo prazo para os próximos cinco anos. Mais informações sobre essa nova abordagem serão disponibilizadas futuramente. Como a segurança é fundamental para a organização, a segurança, a estabilidade e a resiliência de identificadores exclusivos continuará sendo uma das principais áreas estratégicas para a ICANN.

Revisão da Afirmação de Compromissos

A Afirmação de Compromissos assinada pela ICANN e o Departamento de Comércio dos EUA em 30 de setembro de 2009 (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) estabeleceu que um compromisso fundamental inclui a preservação da segurança, a estabilidade e a resiliência do DNS (seção 3b). A Afirmação também "institucionalizou e registrou a coordenação técnica do sistema de endereçamento de nome de domínio (DNS) da Internet globalmente por uma organização liderada pelo setor privado".

A Afirmação reconhece na seção 9.2 que a ICANN adotou um Plano de Segurança, Estabilidade e Resiliência (SSR), que será atualizado regularmente a fim de refletir as ameaças emergentes ao DNS (incluindo os identificadores exclusivos). Esse Plano será revisado, no mínimo, a cada três anos.

A primeira revisão de SSR foi concluída em junho de 2012, e "foram encontradas áreas em que a ICANN está apresentando um bom desempenho, áreas que podem ser melhoradas e outras áreas em que é necessário definir e implementar elementos importantes de SSR" (Relatório Final da RT de SSR, junho de 2012).

A Diretoria da ICANN aprovou o relatório final e as recomendações em outubro de 2012.[7] Desde o encontro em Toronto, a ICANN tem dado continuidade à implementação das recomendações da Equipe de Revisão de SSR.

Uma atualização sobre o andamento da implementação da ICANN foi publicado em 19 de dezembro de 2012 (http://blog.icann.org/2012/12/tracking-the-ssr-review-implementation/). Duas recomendações já foram implementadas (as Recomendações 18 e 24). Durante o resto do período do AF de 2013 até o AF de 2015 e o início do próximo processo de revisão de SSR, a ICANN acompanhará a implementação junto com as demais revisões da Afirmação de Compromissos (http://www.icann.org/en/news/in-focus/accountability).

As 28 recomendações foram alinhadas com a estrutura de Distribuição de Gerenciamento da ICANN apresentada no encontro da ICANN em Toronto. As recomendações são:

- Afirmação de Finalidade [Recomendações 1, 2, 18 e 24]
- Excelência de Operações [Recomendações 7, 8, 17, 20, 21, 9, 10, 11, 22, 25, 26, 27, 15 e 28]
- Internacionalização [Recomendações 3, 4, 5, 14 e 16]
- Evolução do Modelo de Várias Partes Interessadas [Recomendações 6, 12, 13, 19 e 23]

Mais informações sobre a implementação de recomendações individuais podem ser encontradas no Anexo A. As Estruturas e Planos de SSR anteriores da ICANN, que abrangem os Anos Fiscais de 2010, 2011, 2012 e 2013, estão disponíveis em https://www.icann.org/en/about/staff/security/archive.

Uma nova temporada — mudando para uma organização matricial

Em outubro de 2012, no encontro da ICANN em Toronto, Fadi Chehade, CEO da ICANN, apresentou a nova Estrutura de Distribuição de Gerenciamento da ICANN. Isso aplica uma organização matricial às funções da ICANN. A segurança faz parte das funções técnicas dentro da ICANN, juntamente com as equipes de operações de DNS da IANA, TI e ICANN.

[7] http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e

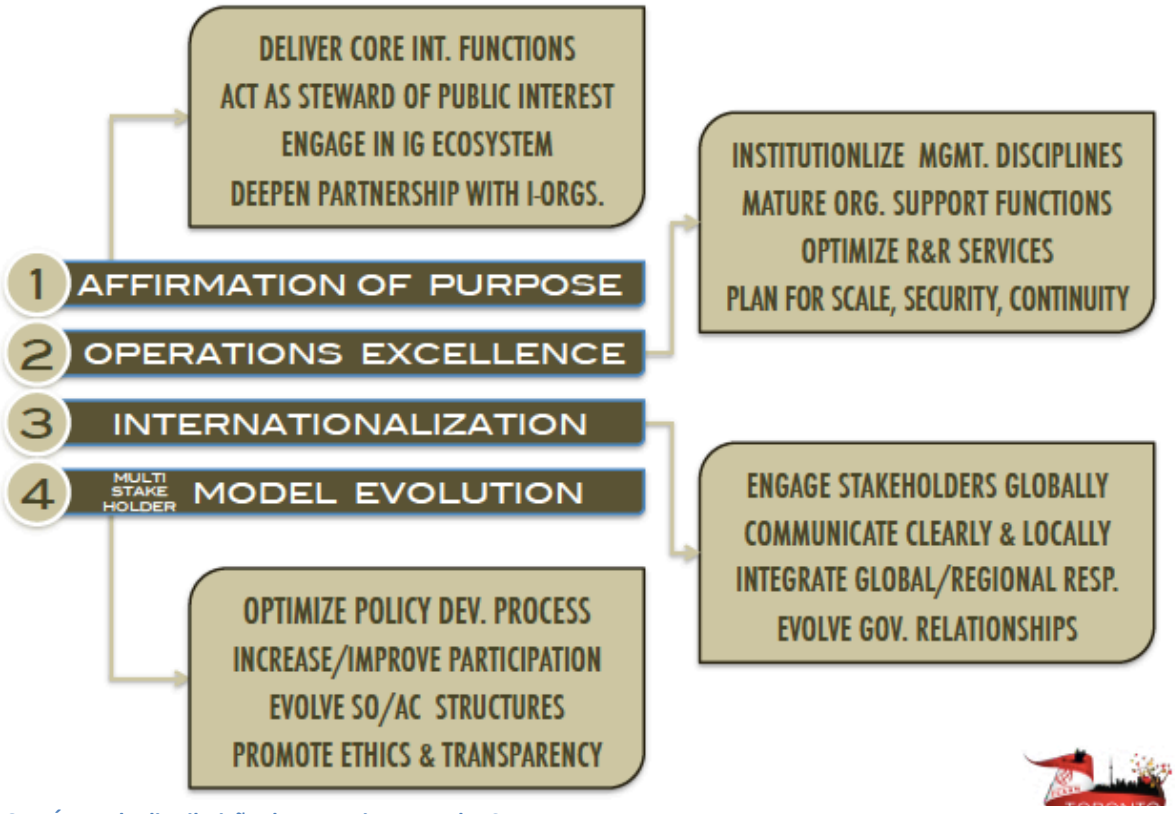


Figura 6 — Áreas de distribuição de gerenciamento da ICANN

A atividade da equipe de segurança abrange toda a organização, dando suporte a cada uma das quatro áreas de distribuição de gerenciamento. Isso inclui o suporte à Excelência de Operações e à equipe de Participação Global de Partes Interessadas (GSE) da ICANN na Internacionalização, evolução do Modelo de Várias Partes Interessadas e contribuições para a ampliação de discussões sobre governança da Internet com toda a comunidade.

O modelo matricial será implementado distribuindo o trabalho da ICANN entre os três principais núcleos: Los Angeles, Cingapura e Istambul. A ICANN também manterá escritórios de participação em Bruxelas, Washington, D.C., e outros locais, para se aproximar de suas partes interessadas.

Uma visualização da segurança da ICANN

Para ajudar a explicar a competência e a função da ICANN, o gráfico preliminar a seguir fornece uma visualização das funções da ICANN com relação à segurança, estabilidade e resiliência.

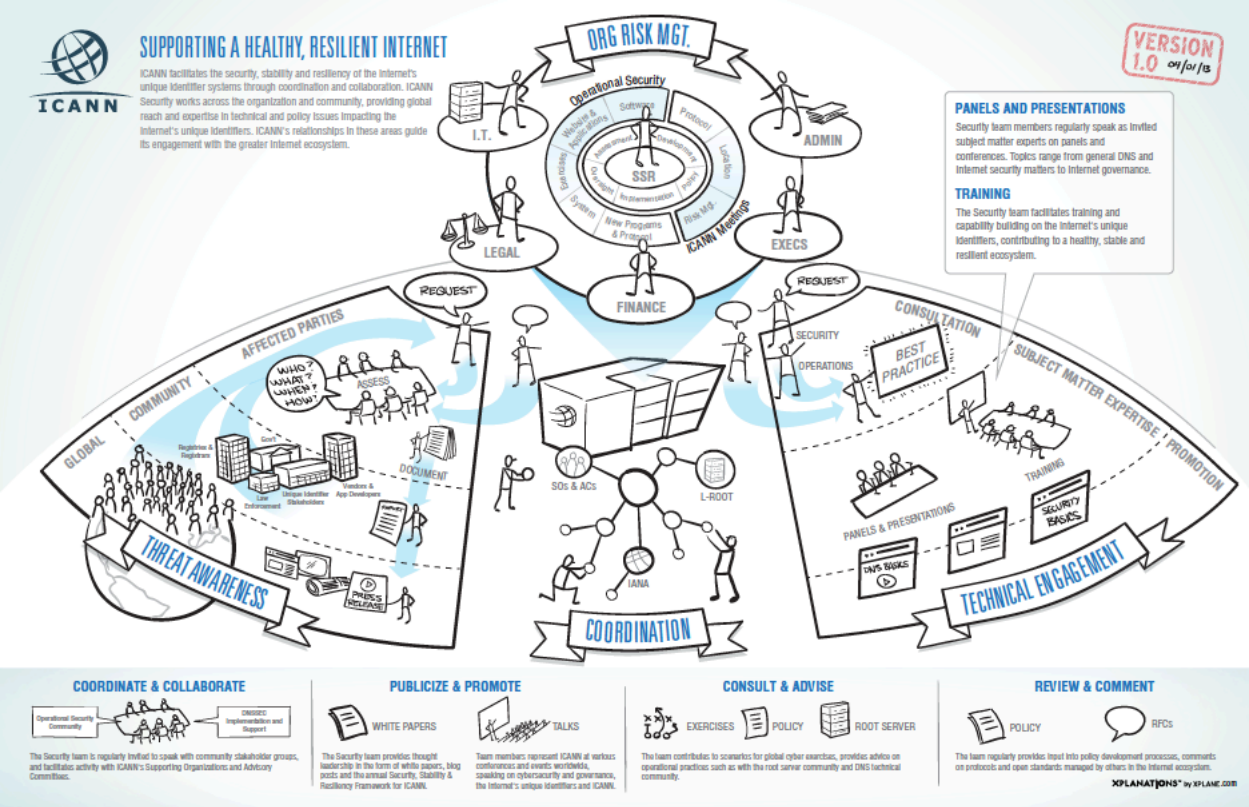


Figura 7 — Gráfico informativo sobre segurança da ICANN

Esse gráfico mostra as principais funções da segurança da ICANN, dando suporte ao gerenciamento de riscos organizacionais, facilitando o reconhecimento de ameaças aos identificadores exclusivos da Internet, colaborando e coordenando junto com parceiros da comunidade da Internet e fornecendo especialistas em participação técnica, abrangendo treinamento, liderança inovadora e consultas para assuntos técnicos e políticas. (Observação: esse trabalho está em andamento e será revisado antes do encontro da ICANN em Pequim).

Como segurança, estabilidade e resiliência se enquadram nas áreas funcionais da ICANN

A segurança na ICANN pode ser entendida como:

- Um valor central para a ICANN, na Afirmação de Compromissos
- Uma das quatro áreas de concentração do Plano Estratégico
- Uma área temática geral que abrange toda a organização
- Um departamento da ICANN
- Um elemento essencial em projetos e atividades

A segurança da ICANN é uma equipe distribuída, com abrangência global e experiência em assuntos técnicos e de políticas que afetam os identificadores exclusivos da Internet. A equipe de segurança tem uma função interna e externa, trabalhando em toda a organização e a comunidade para dar suporte à missão da ICANN de preservar e melhorar a estabilidade operacional, a confiabilidade e a interoperabilidade global da Internet. Esse trabalho pode não

ser sempre notado nem percebido pelo público, mas desempenha um papel muito importante para a ICANN e seus compromissos. A equipe serve como uma ponte entre os operadores do DNS, a comunidade técnica, os organismos encarregados pelo cumprimento da lei, a comunidade de segurança operacional e os grupos de partes interessadas.

Membros da equipe de segurança da ICANN

Até a publicação deste documento, a equipe de segurança era composta por:

- Jeff Moss: Vice-presidente e Diretor de Segurança (líder de equipe e membro da equipe executiva da ICANN; participação técnica e palestrante frequente sobre assuntos de Internet e segurança)
- Geoff Bickers: Diretor de Operações de Segurança (Programas de Segurança Corporativa, Segurança de Encontros, Segurança de Bens Físicos e Funcionários da ICANN, parceria com o departamento de TI da ICANN)
- John Crain: Diretor Sênior, Segurança, Estabilidade e Resiliência (participação técnica, liderança em reconhecimento e monitoramento de ameaças e representante de Servidor Raiz na Diretoria do DNS-OARC)
- Patrick Jones: Diretor Sênior, Segurança (coordenação de equipe, membro da equipe executiva da ICANN, implementação da RT de SSR, parceria com a GSE da ICANN e participação na governança da Internet)
- Richard Lamb: Gerente de Programa Sênior, DNSSEC (participação técnica na adoção e no treinamento de DNSSEC; colaboração com a comunidade sobre DNSSEC; gerenciamento de políticas e práticas para a implementação de DNSSEC)
- Dave Piscitello: Tecnólogo de Segurança Sênior (participação técnica, treinamento e liderança inovadora; líder da comunidade de organismos encarregados pelo cumprimento da lei e de segurança operacional; membro do Grupo de Gestão Executiva para a Commonwealth Cybercrime Initiative [Iniciativa da Commonwealth contra Crimes Cibernéticos])
- Sean Powell: Engenheiro de Segurança de Informações (segurança organizacional; segurança de rede e informações; colaboração com o departamento de TI da ICANN e suporte para o Diretor de Operações de Segurança)

Imagem 1 — Jeff Moss no IGF da Rússia

Imagem 2 — John Crain, Rick Lamb (ICANN) e Revil Wooding (PCH) no CaribNOG 3

Imagem 3 — Patrick Jones no Cyber Security Dialogue (Diálogo sobre Segurança Cibernética) da OEA, em dezembro de 2012

Imagem 4 — Dave Piscitello dando uma palestra na ICLN, Haia, em dezembro de 2012

Critérios de participação

Em fevereiro de 2012, a equipe de segurança formalizou seus critérios de difusão e participação. Os critérios influenciaram outros setores da ICANN e tem como finalidade fornecer uma orientação para a equipe de segurança e a Gestão Executiva da ICANN sobre os tipos de atividades colaborativas e da comunidade que têm o suporte da equipe de segurança.

Tabela 1 — Critérios de segurança para difusão e participação

Tipos de eventos	Exemplos
Encontros públicos da ICANN	ICANN Pequim, Durban, Buenos Aires
Encontros internos da ICANN	Encontro executivo, equipe de segurança, workshop da diretoria, treinamento de equipes, orçamento, entre outros
Encontros relevantes aos aspectos operacionais da ICANN/IANA/Servidor de raiz "L"/DNSSEC, etc.	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC, entre outros
Encontros em que a ICANN fornece colaboração sobre ameaças globais/mitigação	APWG (Grupo de Trabalho Anti-phishing), MAAWG (Grupo de Trabalho Anti-Abuso de Mensagens), Conferência sobre Underground Economy ("Mercado Negro") da Interpol, exercícios cibernéticos, OEA
Participação técnica — treinamentos e capacitação	Treinamento para ataques e resposta de contingência (ACRP), operações de segurança de registro, DNSSEC, organismos encarregados pelo cumprimento da lei e governos, Commonwealth Cybercrime Initiative
Simpósios, convites para conferências de SME, educação continuada	SATIN, Simpósio de SSR, Security Confab, RSA, BlackHat, FIRST, ICLN
Participação no ecossistema, modelo de várias partes interessadas	IGF e IGFs regionais, RANS, OECD, Fórum de WSIS, segurança cibernética pan-árabe, CTU

Critérios de participação	✓
O evento apoia um Objetivo Estratégico da ICANN?	1. Manter e estimular a disponibilidade do DNS 2. Melhorar o gerenciamento de riscos e a resiliência do DNS 3. Promover a ampla adoção de DNSSEC 4. Aprimorar a cooperação internacional do DNS 5. Melhorar a resposta a incidentes de segurança do DNS
O evento se enquadra em uma das seguintes áreas:	1. Operacional/organizacional 2. Colaboração 3. Participação técnica

Dá suporte a uma relação de parceria, MOU ou parte interessada?	
Isso apoia ou acrescenta algo à reputação organizacional da ICANN?	
Com que frequência o evento é realizado?	
É possível se encontrar com outras partes interessadas que estejam localizadas por perto?	Quem mais participará?
Como isso se encaixa no orçamento?	Isso serve para apoiar outra equipe?

Com a criação da nova estrutura matricial, a equipe de segurança dá apoio à equipe de Participação Global de Partes Interessadas (GSE) da ICANN e outras equipes em toda a organização. Seguem abaixo exemplos dos tipos de eventos e atividades com suporte da equipe de segurança da ICANN:

- Encontros de IETF em Vancouver e Atlanta
- Encontros X-Con, CNNIC e CONAC na China
- BlackHat e DefCon em Las Vegas, Abu Dhabi e Amsterdã
- Grupo de Peritos das Nações Unidas em Nomes Geográficos/Conferência das Nações Unidas sobre Padronização de Nomes Geográficos, em Nova York.
- Interpol Underground Economy em Lyon, França
- Encontro de Registros de CIS em Budva, Montenegro
- Treinamento de DNS com a SOCA (Serious Organized Crime Agency) e o OFT (Office of Fair Trading) em Londres, Reino Unido
- Treinamento de DNSSEC na Colômbia com .CO; no Peru com .PE e o Network Startup Resource Center, em Hong Kong
- Treinamento de capacitação de DNS com LACTLD em São Martinho e Paraguai
- Asia-Pacific Telecommunity em Macau
- MENOG em Jordão
- LACNIC/LACNOG no Uruguai
- Treinamento de DNS com a Europol
- MAAWG, APWG, RIPE NCC e DNS-OARC
- Lançamento do CyberLab da OEA CICTE para exercícios
- APNIC 34
- ION Mumbai e Interop
- Fornecendo palestras por meio de apresentação remota, como o IGF caribenho em Santa Lúcia, em agosto de 2012, e a Conferência de ICT, no Nepal, em fevereiro de 2013.

Uma parte importante da participação técnica fornecida pela equipe de segurança é o treinamento de DNS, em resposta às solicitações da comunidade. A equipe desenvolveu um currículo, que inclui módulos sobre:

- Fundamentos do DNS (incluindo uma visão geral sobre a participação na ICANN)
- Programa de Ataque e Resposta de Contingência para operadores de TLD
- Treinamento de DNS para organismos encarregados pelo cumprimento da lei e a comunidade de segurança operacional
- Treinamento de DNSSEC
- Curso de Operações Seguras de Registro

A ICANN faz parcerias regularmente com o Network Startup Resource Center (http://nsrc.org/), com base na Universidade do Oregon, para fornecer participação técnica com organizações regionais de TLD, universidades e operadores no mundo todo. A ICANN também estabelece parcerias com a AfTLD, APTLD e LACTLD nesse treinamento.

Desenvolvimentos internacionais

No âmbito global, ocorreram atividades significativas no AF de 2013. A ICANN assinou os Principles for Cyber Resilience ("Princípios para Resiliência Cibernética") do Fórum Econômico Mundial, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf e participou de eventos do Fórum Econômico Mundial em Davos, Suíça, e em Washington, D.C., em 2012 e 2013.

A ICANN organizou a Commonwealth Cybercrime Initiative (CCI) no encontro de Praga, República Tcheca, em junho de 2012. Dave Piscitello, da equipe de segurança da ICANN, foi indicado para o Grupo de Gestão Executiva da CCI em novembro de 2012 (http://blog.icann.org/2012/11/icann-security-team-members-appointed-to-lead-roles-in-global-community-initiatives/).

A ICANN deu suporte ao treinamento de DNSSEC na América Latina e no Caribe (Trinidad, Colômbia, Chile, Peru e Paraguai).

Em julho, o Departamento de Comércio do EUA anunciou que a ICANN recebeu o contrato de funções de IANA, http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann. A ICANN publicou uma versão revisada de sua proposta para o contrato de funções de IANA em 9 de julho de 2012: https://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm. O período de exercício tem início em 1 de outubro de 2012 e se estende a 30 de setembro de 2015, com dois períodos opcionais de dois anos, resultando em um período contratual de sete anos.

Em julho de 2012, a ICANN participou do encontro Hemispheric Cybersecurity (Segurança Cibernética Hemiférica) da OEA, no Uruguai, e o Cybersecurity Dialogue (Diálogo sobre Segurança Cibernética) da OEA, em Washington, D.C., em 13 de dezembro de 2012, http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-465/12.

Em agosto de 2012, a IAB, IEEE-SA, IETF, Sociedade da Internet e W3C lançaram o Open Stand (http://open-stand.org/) como um modelo aberto para o desenvolvimento colaborativo e ascendente de normas para a inovação e a interoperabilidade. Essa iniciativa está alinhada aos princípios da ICANN para a colaboração ascendente e voltada ao consenso com várias partes interessadas.

A ICANN contribuiu para o Communications Security, Reliability and Interoperability Council III ("3º Conselho sobre Segurança das Comunicações, Confiabilidade e Interoperabilidade") (CSRIC III) da Comissão Federal de Comunicação (FCC) dos EUA. O Grupo de Trabalho 4 publicou seu relatório sobre Práticas Recomendadas para a Segurança da Rede em setembro de 2012 (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf). Também foram feitas contribuições para o Grupo de Trabalho 3, DNSSEC, e para o Grupo de Trabalho 7, Código de Conduta Anti-bot para ISPs.

A ICANN participou da Conferência de Budapeste sobre o Espaço Cibernético, em outubro de 2012, (http://www.cyberbudapest2012.hu/), o evento posterior à Conferência de Londres, em 2011, (https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement).

A ICANN organizou, junto com o Grupo de Trabalho Anti-phishing (APWG), seu 4º Simpósio Global de SSR para o DNS em seu evento eCOS em Las Croabas, Porto Rico, em outubro de 2012 (http://docs.apwg.org/events/2012_ecrime.html).

A Organização para Coordenação e Desenvolvimento Econômico (OECD) publicou uma análise das estratégias nacionais de segurança cibernética em outubro de 2012, descrevendo o apoio a um diálogo com várias partes interessadas sobre a segurança cibernética em vários documentos de estratégia nacional. A referência para esse documento é OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy" ("Elaboração de Políticas de Segurança Cibernética em um Momento Decisivo: Analisando uma Nova Geração de Estratégias Nacionais de Segurança Cibernética para a Economia na Internet"), OECD Digital Economy Papers, nº 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

A ICANN foi bem representada no 7º Fórum de Governança da Internet em Baku, Azerbaijão, em novembro de 2012 (http://blog.icann.org/2012/10/icann-at-internet-governance-forum-2012-2/), em que a segurança na Internet foi um dos principais tópicos da discussão (http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/927-igf-2012). A ICANN também participou de eventos regionais da IGF na América Latina e no Caribe, na Rússia, nos Emirados Árabes Unidos e nos Estados Unidos.

Em dezembro de 2012, Fadi Chehade, CEO da ICANN, falou na abertura da Conferência Mundial de Telecomunicações Internacionais, em Dubai (http://www.itu.int/en/wcit-12/Pages/speech-chehade.aspx). Em fevereiro de 2013, a ICANN colaborou na preparação do Informal Experts Group (Grupo Informal de Especialistas) para o Fórum Mundial de Políticas de Telecomunicações em Genebra, em maio de 2013.

A ICANN participou do Pan Arab Cybersecurity Observatory (Observatório Pan-árabe de Segurança Cibernética) em Túnis, na Tunísia, em dezembro de 2012, compartilhando

informações com os participantes sobre a função e a competência da ICANN em atividades de segurança, estabilidade e resiliência. A ICANN também participou da Conferência da International Criminal Law Network em Haia, Países Baixos, e se uniu à Europol para ajudar no treinamento de DNS com o lançamento do novo Centro Europeu de Combate a Crimes Cibernéticos (EC3).

Em janeiro de 2013, a equipe de segurança da ICANN publicou um artigo de reflexão intitulado "Value of Assessing Collateral Damage Before Requesting a Domain Seizure" ("A Importância de Fazer uma Avaliação de Danos Colaterais Antes de Solicitar um Confisco de Domínio"), http://blog.icann.org/2013/01/the-value-of-assessing-collateral-damage-before-requesting-a-domain-seizure/. Esse artigo é uma continuidade do artigo de reflexão de março de 2012 sobre Confiscos e Remoções de Domínios, http://blog.icann.org/2012/03/thought-paper-on-domain-seizures-and-takedowns/. Isso está relacionado à SAC 056, "SSAC Advisory on Impacts of Content Blocking via the Domain Name System" ("Conselho do SSAC sobre os Impactos do Bloqueio de Conteúdo por meio do Sistema de Nomes de Domínio"), http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf, publicado em outubro de 2012.

A ICANN acompanhou o desenvolvimento da Estratégia de Segurança Cibernética da UE (janeiro de 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security e o Decreto Presidencial sobre Segurança Cibernética dos EUA (fevereiro de 2013),http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. Esses dois documentos representam o interesse cada vez maior de estabelecer mecanismos para o compartilhamento de informações e a colaboração em resposta às ameaças contra a segurança cibernética.

Os eventos globais importantes da Internet anteriores à publicação desse documento que também foram incluídos são:

- APRICOT 2013 (Conferência Regional da Internet Ásia/Pacífico sobre Tecnologias Operacionais) em Cingapura, de 19 de fevereiro a 1 de março de 2013, http://www.apricot2013.net/.
- WSIS+10, "Toward Knowledge Societies for Peace and Sustainable Development" (organizado pela UNESCO), em Paris, de 25 a 27 de fevereiro de 2013, http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/.
- Evento árabe sobre governança da Internet com várias partes interessadas em Dubai, EAU, e evento africano sobre governança da Internet com várias partes interessadas em Adis Abeba, Etiópia, http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm.
- IETF 86, Orlando, Flórida, de 10 a 15 de março de 2013, http://www.ietf.org/meeting/86/index.html.

Atividades para o AF de 2014

No AF de 2014, as atividades da ICANN para apoiar um ecossistema saudável, estável e resiliente serão focadas no seguinte:

- Dar suporte à excelência operacional em atividades lideradas pela IANA, TI e operações do DNS
- Fornecer participação técnica (por meio de especialistas e liderança inovadora, participação da comunidade, realização de atividades de treinamento de DNS e capacitação quando solicitadas por parceiros)
- Incentivar junto a empresas, usuários e operadores a adoção e a conscientização de DNSSEC
- Implementar as recomendações da Equipe de Revisão de SSR
- Dar suporte a mais capacidade de servidor de raiz "L", publicação de dados e avaliação da equipe de operações do DNS da ICANN
- Fornecer uma Estrutura de Gerenciamento de Riscos do DNS e concluir um ciclo de avaliação
- Aumentar o conhecimento da ICANN sobre o gerenciamento de riscos corporativos a fim de fornecer maior suporte ao Comitê de Riscos da Diretoria e às exigências crescentes da ICANN com relação ao gerenciamento de riscos organizacionais
- Dar suporte ao estabelecimento de novos escritórios da ICANN em Cingapura e Istambul e expandir os recursos da equipe de segurança nesses locais a fim de melhor atender a comunidade
- Servir de apoio para a equipe de Participação Global de Partes Interessadas em discussões sobre governança e segurança cibernética, representando a ICANN em conferências e encontros
- Facilitar e incentivar a maior participação dos organismos encarregados pelo cumprimento da lei e da comunidade de segurança operacional na ICANN
- Dialogar com a sociedade civil sobre questões de liberdade de expressão e privacidade relacionadas à segurança dos identificadores exclusivos e a um ecossistema saudável da Internet (expandir a difusão e o envolvimento de participantes do ecossistema nas questões de SSR)
- Fortalecer as redes internas da ICANN, os processos de TI e a segurança das informações
- Colaborar com a comunidade técnica, os operadores de servidor raiz e os desenvolvedores de aplicativos e navegadores com relação às questões do DNS
- Dar suporte às equipes de Políticas e Relações com Partes Interessadas da ICANN quando necessário (SSAC, RSSAC e questões de SSR quando discutidas em SOs e ACs)
- Dar suporte a encontros bem-sucedidos da ICANN em Durban, Buenos Aires, Cingapura e Londres

Para realizar essas iniciativas, a ICANN precisa fortalecer sua equipe de segurança no AF de 2014 com mais conhecimento e habilidades. Isso é necessário para atender às exigências da comunidade e à estrutura matricial sendo implementada neste Ano Fiscal. Uma explicação para apoiar as atividades de SSR projetadas para o AF de 2014 será fornecida no futuro orçamento e plano operacional do AF de 2014, que será publicado após o encontro da ICANN em Pequim. Isso seguirá como diretriz as Recomendações de SSR 20 e 21, de que a ICANN aumente a transparência das informações sobre a organização e o orçamento referente à Estrutura de SSR e forneça um processo mais estruturado para mostrar como a organização e as decisões de orçamento se relacionam com a Estrutura de SSR.

Anexos

Anexo A — Acompanhamento das recomendações da RT de SSR

Esta seção fornece detalhes sobre as abordagens de implementação das 28 recomendações da Equipe de Revisão de SSR, alinhadas às quatro áreas de distribuição de gerenciamento.

Afirmação de Finalidade — Missão e competência da ICANN

Recomendação da RT de SSR	Implementação e status
Nº 1 — A ICANN deve publicar uma declaração clara e consistente de sua competência e a missão técnica limitada de SSR.	Comentário público retirado de uma declaração preliminar entre maio e setembro de 2012 [link: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm]. A declaração preliminar foi revisada em 4 de outubro de 2012 [http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct2012-en.pdf]. Uma versão atualizada é apresentada na Estrutura de SSR do AF de 2014.
Nº 2 — A definição e a implementação da competência e da missão técnica limitada de SSR da ICANN devem ser revisadas a fim de manter um consenso e extrair comentários da comunidade.	A declaração atualizada de função e competência será revisada pela próxima RT de SSR em 2015.
Nº 24 — A ICANN deve definir claramente o regulamento, as funções e as responsabilidades da Equipe do Departamento de Segurança.	**Implementada** com a página atualizada da equipe de segurança [link: https://www.icann.org/security] em 4 de outubro de 2012 e a publicação da Estrutura de SSR do AF de 2013. As funções e as responsabilidades serão aprimoradas ainda mais com a implementação da nova estrutura de Distribuição de Gerenciamento em 2013.
Nº 18 — A ICANN deve realizar uma revisão operacional anualmente do progresso da implementação da Estrutura de SSR e incluir essa avaliação como um componente da Estrutura de SSR do ano seguinte.	**Implementada** como parte da Estrutura de SSR do AF de 2013 e será repetida anualmente. O acompanhamento do progresso será adicionado à nova página Dashboard da página da equipe de segurança no site da ICANN.

Excelência de Operações — Objetivos

Recomendação da RT de SSR	Implementação e status
Nº 7 — A ICANN deve aprender com sua atual Estrutura de SSR estabelecendo um conjunto claro de objetivos e priorizando suas iniciativas e atividades de acordo com esses objetivos.	A nova estrutura de Distribuição de Gerenciamento será usada para alinhar os objetivos e as iniciativas da ICANN com a Estrutura de SSR anual e para dar apoio ao desenvolvimento do orçamento para o AF de 2014, o plano operacional e o próximo Plano Estratégico da ICANN. A ICANN está trabalhando para alinhar seus objetivos e atividades a essa estrutura.
Nº 8 — A ICANN deve dar	Isso está vinculado ao próximo Plano Estratégico. É necessário

continuidade ao aprimoramento dos objetivos de seu Plano Estratégico, em particular a meta de manutenção e promoção da disponibilidade do DNS. Alinhamento claro da Estrutura e do Plano Estratégico.	haver um alinhamento de objetivos e atividades do Plano Estratégico com as recomendações da Equipe de Revisão de SSR e a Estrutura de SSR anual.

Excelência de Operações — Transparência

Recomendação da RT de SSR	Implementação e status
Nº 17 — A ICANN deve estabelecer um processo interno mais estruturado para mostrar como as atividades e as iniciativas se relacionam especificamente com as metas estratégicas, os objetivos e as prioridades incluídos na Estrutura de SSR.	A estrutura de Distribuição de Gerenciamento tem sido útil para cumprir com essa recomendação, criando um mecanismo para o processo interno que mostrará como as atividades de SSR da ICANN se relacionam com as metas, os objetivos e as prioridades. Mais informações sobre esse processo serão disponibilizadas à comunidade pelo MyICANN e no site da ICANN entre os encontros da ICANN em Pequim e Durban, em 2013.
Nº 20 — A ICANN deve melhorar a transparência de informações sobre a organização e o orçamento com relação à implementação da Estrutura de SSR e à execução de funções relacionadas a SSR.	Isso será implementado com a Estrutura de SSR do AF de 2014 e o processo de Orçamento e Plano Operacional do AF de 2014. A nova página Dashboard da equipe de segurança também será usada para abordar essa recomendação.

Excelência de Operações — Estrutura

Recomendação da RT de SSR	Implementação e status
Nº 21 — A ICANN deve estabelecer um processo interna mais estruturado para mostrar como a organização e as decisões de orçamento se relacionam com a Estrutura de SSR, abrangendo a análise subjacente de custo e benefício.	A ICANN usará o trabalho da Distribuição de Gerenciamento como o processo estruturado a fim de identificar a organização e as decisões de orçamento e alinhá-las às atividades de SSR na Estrutura anual. Isso será implementado no Orçamento e Plano Operacional do AF de 2014.

Excelência de Operações — Normas e conformidade

Recomendação da RT de SSR	Implementação e status
Nº 9 — A ICANN deve avaliar as opções de certificação com relação às normas internacionais aceitas (por exemplo, ITIL, ISO e SAS-70) quanto a suas responsabilidades operacionais. A	A implementação de DNSSEC da ICANN na raiz obteve a certificação SysTrust [link: https://www.iana.org/dnssec/systrust e https://cert.webtrust.org/icann.html]. Outros processos de certificação estão sendo liderados pela equipe de funções de IANA e as equipes de TI e Operações do DNS da ICANN, com o suporte da segurança.

ICANN deve publicar um guia claro sobre certificações.	
Nº 10 — A ICANN deve dar continuidade a seu trabalho de definir a aplicação de conformidade de contratos e fornecer os recursos adequados para essa função. A ICANN também deve desenvolver e implementar um processo mais estruturado para monitorar as questões de conformidade e investigações.	Essa recomendação está sendo liderada pela equipe de conformidade da ICANN e por meio da implementação das recomendações da Equipe de Revisão de WHOIS.

Excelência de Operações — nTLDs

Recomendação da RT de SSR	Implementação e status
Nº 11 — A ICANN deve finalizar e implementar as medidas de sucesso para novos gTLDs e tramitação rápida de IDN que se relaciona expressamente com seus objetivos de programa referentes a SSR, abrangendo medidas para a eficiência de mecanismos a fim de reduzir o abuso de nomes de domínios.	A equipe está investigando todas as implicações desta Recomendação. A equipe de segurança acredita que isso envolverá a colaboração de uma equipe da comunidade para sua total implementação. Como isso está relacionado à Revisão de Concorrência, Confiança do Consumidor e Escolha do Consumidor e às medidas para novos gTLDs e IDN ccTLDs delegados pela Tramitação Rápida de IDN ccTLD, haverá o envolvimento de partes interessadas de toda a comunidade. O foco dessa recomendação são os mecanismos relacionados à redução do abuso de nomes de domínio. A equipe está dando apoio ao trabalho dos Comitês Consultivos e da comunidade com relação a medidas contra o abuso.
Nº 22 — A ICANN deve publicar, monitorar e atualizar a documentação sobre a organização e os recursos de orçamento necessários para gerenciar as questões de SSR juntamente com a introdução de novos gTLDs.	Isso está relacionado à Recomendação 21 (decisões de orçamento e organização), bem como ao desenvolvimento do monitoramento com a introdução de novos gTLDs.

Excelência de Operações — Gerenciamento de riscos e redução de ameaças

Recomendação da RT de SSR	Implementação e status
Nº 25 — A ICANN deve colocar em vigor mecanismos para identificar riscos a médio e longo prazos e fatores estratégicos de sua Estrutura de Gerenciamento de Riscos.	Isso está em andamento e vinculado à entrega da Estrutura de Gerenciamento de Riscos de acordo com a Recomendação 26.

Nº 26 — A ICANN deve priorizar a conclusão de uma Estrutura de Gerenciamento de Riscos no prazo estipulado.	Isso está em andamento. A ICANN contratou a Westlake Governance para ajudar com o projeto da Estrutura de Gerenciamento de Riscos de DNS. A Westlake realizou uma sessão aberta em Toronto, fornecerá uma estrutura preliminar em breve e fará um resumo sobre o conceito da estrutura no encontro da ICANN em Pequim.
Nº 27 — A Estrutura de Gerenciamento de Riscos da ICANN deve ser abrangente dentro do escopo de sua competência e missões limitadas de SSR.	A Estrutura de Gerenciamento de Riscos estará alinhada com as atividades da ICANN apoiando sua missão técnica e a comunidade. Isso será abrangente no escopo e será realizado com a entrega da Estrutura de acordo com a Recomendação 26.
Nº 15 — A ICANN deve atuar como facilitadora na divulgação responsável e na disseminação de técnicas de mitigação e ameaças à segurança do DNS.	Um documento preliminar de Divulgação Coordenada está sendo elaborado pela equipe de segurança da ICANN. A equipe colabora com operadores e entidades confiáveis da comunidade de segurança na elaboração de técnicas de mitigação e ameaças à segurança do DNS. Isso está relacionado à Recomendação 28.
Nº 28 — A ICANN deve dar continuidade ao trabalho ativo na detecção e mitigação de ameaças, e participar na divulgação de informações sobre ameaças e incidentes.	Essa recomendação apoia a continuação do trabalho da ICANN, inclusive o monitoramento de zona raiz, a detecção e a mitigação de ameaças referentes às Operações de DNS da ICANN e aos incidentes e ameaças do DNS em geral.

Internacionalização — Terminologia e relacionamentos

Recomendação da RT de SSR	Implementação e status
Nº 3 — Depois de publicar uma declaração consensual de sua competência e missão técnica limitada de SSR, a ICANN deve usar uma terminologia e descrições consistentes dessa declaração em todos os materiais.	A equipe de segurança trabalhará em toda a organização de modo que uma terminologia e descrições consistentes referentes à função e à competência de SSR da ICANN sejam usadas em todos os materiais. A primeira etapa é realizar um treinamento da equipe da ICANN e, em seguida, oferecer seminários na Web para a participação da comunidade. Nós também usaremos essa terminologia e descrições em apresentações e projetos da ICANN.
Nº 4 — A ICANN deve documentar e definir claramente a natureza das relações de SSR presentes na comunidade da ICANN a fim de fornecer um ponto central único para o entendimento das interdependências entre as organizações.	Já foi dado início ao trabalho de documentar e definir essas relações. A visualização das funções de segurança da ICANN será usada para mapear as relações com as funções das áreas de coordenação e colaboração, reconhecimento de ameaças e participação técnica.
Nº 5 — A ICANN deve usar a definição de suas relações de SSR para manter disposições eficientes de trabalho e para demonstrar como essas relações são utilizadas	A equipe de segurança trabalhará com a equipe de Participação Global de Partes Interessadas da ICANN para manter e aprimorar as disposições eficientes de trabalho e relações. A equipe de segurança firmou relações com organismos encarregados pelo cumprimento da lei e a comunidade de segurança operacional no

a fim de alcançar a meta de SSR.	mundo todo e já realizou treinamentos na República Tcheca, França, Países Baixos, Reino Unido, Estados Unidos, entre outros.

Internacionalização — Difusão e participação

Recomendação da RT de SSR	Implementação e status
Nº 14 — A ICANN deve garantir que suas atividades de difusão relacionadas a SSR sejam desenvolvidas continuamente a fim de permanecerem relevantes, oportunas e apropriadas.	As atividades de difusão foram ampliadas e serão revisadas anualmente. A equipe de segurança executa uma função de prestação de serviços para a equipe de Participação Global de Partes Interessadas enquanto especialistas no assunto, e uma função para a comunidade na difusão e na participação de assuntos de SSR.
Nº 16 — A ICANN deve dar continuidade ao seu trabalho de difusão a fim de ampliar a participação e a colaboração da comunidade com o processo de desenvolvimento da Estrutura de SSR. A ICANN também deve estabelecer um processo para obter a colaboração de maneira mais sistemática de outros participantes do ecossistema.	As atividades e os processos de difusão foram ampliados e serão revisados anualmente. O trabalho contínuo da equipe de segurança com as comunidades de segurança, como o APWG e o MAAWG, resultou na participação de membros dessas comunidades no SSAC. Através do envolvimento com a ICLN (Rede de Direito Penal Internacional) e a CCI (Commonwealth Cybercrime Initiative), a equipe de segurança enfatiza o valor das abordagens com várias partes interessadas nas questões referentes a crimes cibernéticos. Isso está relacionado às Recomendações 4, 5 e 14. A equipe de segurança apoia uma série de iniciativas de capacitação mediante a solicitação das partes interessadas, como o treinamento de DNSSEC, treinamento de ataque e resposta de contingência de ccTLD, treinamento para o cumprimento da lei, difusão em encontros de Grupos de Operadores de Rede, como o CaribNOG, MENOG, entre outros.

Evolução do Modelo de Múltiplas Partes Interessadas

Recomendação da RT de SSR	Implementação e status
Nº 6 — A ICANN deve publicar um documento descrevendo claramente as funções e as responsabilidades do SSAC e do RSSAC a fim de delinear com clareza as atividades dos dois grupos.	Essa recomendação exigirá a colaboração da equipe da comunidade. Para facilitar o acompanhamento, essa área foi dividida em 6A [SSAC] e 6B [RSSAC]. 6A — As funções e as responsabilidades do SSAC são definidas nos Procedimentos Operacionais do SSAC. O SSAC está avaliando seus procedimentos operacionais para 2013 e está interessado em alinhá-los às funções e às responsabilidades do RSSAC. 6B — As funções e as responsabilidades para o RSSAC estão em desenvolvimento, após o encerramento dos comentários públicos para as correções propostas nos Estatutos da ICANN sobre a finalidade do RSSAC. Acesse http://www.icann.org/en/news/public-comment/bylaws-

	03jan13-en.htm.
Nº 12 — A ICANN deve trabalhar com a comunidade a fim de identificar as práticas recomendadas para SSR e dar suporte à implementação de tais práticas por meio de contratos, acordos e MOUs, entre outros mecanismos.	A implementação da Recomendação 12 envolverá a colaboração de uma equipe da comunidade. Haverá mais discussões sobre essa questão no encontro da ICANN em Pequim em um Painel de Peritos sobre a segurança de DNS e com o Grupo de Trabalho Técnico da ccNSO sobre práticas recomendadas não contratuais. A equipe de segurança trabalhou com o Comitê de Políticas da Internet do APWG a fim de publicar recomendações para a proteção de aplicativos da Web, participou no desenvolvimento de recursos para o conhecimento sobre segurança (com atividades no Securethehuman.org do SANS e com o Stop.Think.Connect da NCA). O período atual para comentários públicos sobre o acordo de registro de novos gTLDs (acesse http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm) contém mais informações sobre as práticas recomendadas.
Nº 13 — A ICANN deve incentivar que todas as Organizações de Apoio desenvolvam e publiquem práticas recomendadas de SSR para seus membros.	Esse recomendação envolverá a colaboração da equipe da comunidade pela ASO, ccNSO e GNSO sobre as práticas recomendadas adequadas referentes aos identificadores exclusivos em suas respectivas funções.
Nº 19 — A ICANN deve estabelecer um processo que permita à comunidade acompanhar a implementação da Estrutura de SSR. As informações devem ser fornecidas com clareza suficiente de modo que a comunidade possa acompanhar a execução das responsabilidades de SSR da ICANN.	A equipe de segurança lançará em breve um Dashboard na página da equipe para mostrar o acompanhamento de status da Estrutura de SSR e as iniciativas de SSR da ICANN.
Nº 23 — A ICANN deve fornecer os recursos apropriados para os Grupos de Trabalho e Comitês Consultivos de SSR, consistentes com as demandas impostas sobre eles. A ICANN também deve garantir que as decisões alcançadas pelos Grupos de Trabalho e os Comitês Consultivos sejam obtidas de modo objetivo, sem a interferência de coações externas ou internas.	A equipe está elaborando um inventário [23A] de atividades nos atuais grupos de trabalho e Comitês Consultivos de SSR (SSAC e RSSAC). Uma descrição ou documentação do processo de orçamento será apresentada posteriormente para informações de SO/AC [23B]. 23C descreverá uma etapa padrão de processo operacional para mostrar que as decisões do(a) SO/AC/Grupo de Trabalho são obtidas de modo objetivo.

SSR RT Recommendations Tracking – February 2013

Recommendation	FY 13 T1	T2	T3	FY 14 T1	T2	T3	FY 15 T1	T2	T3
Rec 1 – Clear statement of ICANN's SSR role and remit	Published	Revise	Update						
Rec 2 – Role & remit review in 2015								Review	Publish
Rec 3 – Use consistent terminology	Develop	Ongoing							
Rec 4 – Document & define SSR relationships		Develop	Publish						
Rec 5 – Use SSR relationships for effective working	Ongoing	Ongoing	Ongoing						
Rec 6 – Roles for SSAC (6A) & RSSAC (6B)		Publish							
Rec 7 – Build from SSR Framework, clear objectives & priorities	Develop	Publish	Expected Complete	Reporting					
Rec 8 - Strategic Plan & SSR Framework alignment		Publish	Refine						
Rec 9 – Assess certification options, publish roadmap		Develop	Publish						
Rec 10 – Process for monitoring compliance & investigations (see Whois RT Implementation)		Whois RT Recs							
Rec 11 – Measures for success in nTLD & IDN FT re SSR			Develop	Publish			AoC CCR		
Rec 12 – w/Community, SSR-related best practices	Engage	Discuss							
Rec 13 – Encourage SOs/SGs to develop & publish SSR-related best practices			Expected Complete						
Rec 14 – Evolving SSR outreach		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 15 – Facilitate responsible disclosure of threats		Draft	Ongoing	X					
Rec 16 – Outreach w community; process for input		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 17 – Mapping activities to SSR Framework		Publish	X	Reporting					
Rec 18 (Implemented w FY 13 SSR Framework) – Annual review of SSR Framework	Complete								
Rec 19 – Dashboard for SSR Framework			Publish	Reporting					
Rec 20 – Transparency on SSR budget			Publish	ongoing					
Rec 21 – Show how budget & op decisions relate to SSR			Publish						
Rec 22 – Documenting mgmt. of SSR issues with operational readiness from introduction of nTLDs		Develop	Publish						
Rec 23 – Appropriate resources for SSR-related WGs & ACs		FY 14 Budget	Budget approx						
Rec 24 (Implemented w FY 13 SSR Framework) – Define Security team roles	Complete								
Rec 25 – DNS Risk Management Framework	Consultant	Draft	Publish	Assess	work	work	Review		
Rec 26 – Prioritizing completion of DNS RMF		Publish	Approx						
Rec 27 – DNS RMF covers IANA, L-root, other functions				Assess	work	work	Review		
Rec 28 – Active engagement in threat detection & mitigation	Underway	X							

Figura 8 — Acompanhamento de recomendações da RT de SSR

Anexo B — Relatório de status do AF de 2013

Área geral	Programa/iniciativa	Status
Envolvimento da Segurança Global	Envolvimento com toda a comunidade, empresas, comunidade acadêmica, comunidade técnica e organismos encarregados pelo cumprimento da lei sobre questões de segurança de DNS.	Organizou o 4º Simpósio Global de SSR para DNS, em parceria com o APWG na eCOS, Porto Rico, em outubro de 2012.
		Workshops da Commonwealth Cybercrime Initiative nos encontros do CCI Steering Group (Grupo de Orientação da CCI), EMG e ICANN na Costa Rica e em Praga.
		BlackHat/Defcon em julho de 2012.
		Fórum de Governança da Internet e eventos regionais da IGF.
		Palestra para o Constituency Business (Grupo Constituinte de Negócios) em Washington, D.C., e contribuição para o boletim informativo do BC para a ICANN Toronto.
Colaboração	Maior suporte para ferramentas de métrica e medição do DNS, como o ATLAS do RIPE NCC (Centro de Coordenação de Redes IP Europeias).	Colaboração com o RIPE NCC para maior implementação de nós e análises de dados do ATLAS. https://atlas.ripe.net/
	Automação de zona raiz	O sistema de RZM (Gerenciamento de Zona Raiz) usado pela IANA com a NTIA (Administração Nacional de Telecomunicações de Informação) e Verisign comemorou um ano em agosto de 2012 (acesse http://blog.icann.org/2012/08/rzm-is-one-year-old/). A equipe da IANA está trabalhando em outros processos de segurança, como o sistema de Notificação Segura. Acesse http://www.icann.org/en/news/public-comment/iana-secure-notification-12dec12-en.htm.
	Treinamento técnico com organismos encarregados pelo cumprimento da lei e a comunidade de segurança operacional.	A equipe de segurança patrocinou os organismos encarregados pelo cumprimento da lei nos encontros da ICANN Praga e Toronto, e deu treinamento de DNS na Europol nos Países Baixos e SOCA, OFT e a Polícia Metropolitana do Reino Unido.
	Segurança e estabilidade Comitê Consultivo	Colaboração com o SSAC em workshops de DNSSEC em encontros da ICANN; equipes de trabalho e Relatórios e Consultorias do SSAC. O trabalho do SSAC foi significativo no AF de 2013.
	Apoio ao WG de Análise de Segurança	O DSSA concluiu o Relatório da Fase 1 em agosto de 2012. http://www.icann.org/en/news/public-comment/dssa-phase-1-

	e Estabilidade do DNS.	report-14aug12-en.htm. O DSSA se reunirá novamente no encontro da ICANN em Pequim. A ICANN também se uniu à Westlake Governance para a atividade da Estrutura de Gerenciamento de Riscos de DNS.
	Evolução técnica de WHOIS	Em fevereiro de 2013, a ICANN anunciou um grupo de especialistas em Serviços de Diretórios de gTLD (https://www.icann.org/en/news/announcements/announcement-14feb13-en.htm). Em outubro de 2012, a ICANN anunciou que se uniu ao CNNIC para implementar um servidor WHOIS de código aberto com Transferência de Estado Representativo (RESTful), http://blog.icann.org/2012/10/cnnic-selected-to-implement-an-open-source-restful-whois-server/.
	Desenvolvimento de políticas — abuso de registros; Contrato de Credenciamento de Registradores	A ICANN tem um período para comentários abertos sobre um relatório preliminar que trata da Uniformidade da Geração de Relatórios, https://www.icann.org/en/news/public-comment/uofr-20feb13-en.htm. Esse relatório resultou de uma ação do Conselho da GNSO em resposta ao Grupo de Trabalho das Políticas de Abuso de Registros. Com relação ao Contrato de Credenciamento de Registradores, as negociações continuam em andamento. Fadi Chehade, CEO, forneceu uma atualização em 7 de fevereiro de 2013, http://blog.icann.org/2013/02/registrar-accreditation-agreement-negotiation-session/.
	DNSSEC — grupo de trabalho de transferência de chaves no SSAC	O grupo de trabalho de transferência de chaves raiz está dando continuidade a suas atividades em 2013. Mais informações serão disponibilizadas no encontro da ICANN em Pequim. Foram realizadas cerimônias de chave bem-sucedidas em Culpeper, no estado da Virgínia, nos EUA, e em El Segundo, na Califórnia.
	DNSSEC – Auditoria da SysTrust	A certificação da SysTrust de DNSSEC está disponível em https://www.iana.org/dnssec/systrust.
	Treinamento de DNSSEC com a comunidade	A ICANN deu suporte ao treinamento de DNSSEC na Colômbia, Peru, Paraguai, Hong Kong, Chile e futuramente no Líbano (março de 2013) e na Tunísia (abril de 2013).
	Resiliência de raiz "L"	A ICANN apoiou o crescimento e a distribuição de instâncias de raiz "L" em todo o mundo. Em particular, foram anunciadas parcerias para fornecer instâncias de raiz "L" na África, com a AfriNIC, na América Latina e no Caribe, com o LACNIC, no Brasil, com o CGI.Br, na Coreia, com o KISA, e em outros locais.
Programas de segurança corporativa	Melhorar os processos e a segurança de rede interna da ICANN	A equipe de segurança tem trabalhado com o departamento de TI da ICANN a fim de fortalecer as redes internas. A equipe tem dado suporte ao treinamento de SANS para a equipe de TI e fornecido treinamento básico de segurança para a equipe da ICANN em Los Angeles e Bruxelas.
	Melhorar a continuidade de negócios e realizar exercícios internos	A segurança tem dado suporte a exercícios de resiliência raiz e processos internos de comunicação.
	Segurança de encontros —	Realizou avaliações nos locais de encontros da ICANN; forneceu serviços de emergência e atendimento médico no local nos encontros

	avaliações de riscos, segurança de participantes estrangeiros	da ICANN (ISOS).
Interorganizacional	Suporte a operações de novos gTLDs	Ofereceu apoio à equipe de novos gTLDs com o Sorteio de Priorização; processos de revisão
		Ajuda com a revisão do sistema de verificação de pré-delegação com .SE, http://www.icann.org/en/news/announcements/announcement-21dec12-en.htm.
	Conformidade contratual	A equipe de conformidade deu continuidade a seu crescimento no AF de 2013, publicando seu plano de auditoria (acesse http://www.icann.org/en/resources/compliance/audits)
	Programa de IDN	Compareceu aos encontros de UNGEGN/UNCSGN em Nova York, em julho e agosto de 2012, na sede da ONU, e deu apoio ao trabalho continuado do Programa de Variante de IDN.
	Gerenciamento de Riscos Corporativos	A ICANN contratou a Westlake Governance para uma iniciativa de Estrutura de Gerenciamento de Riscos do DNS. Mais informações sobre o progresso da Westlake serão fornecidas no encontro da ICANN em Pequim.

O trabalho de participação técnica realizado pela equipe de segurança da ICANN é colaborativo. Ele é realizado para o proveito de toda a comunidade. É muito bom receber cartas de apoio a nosso trabalho, mas não é algo que buscamos para simplesmente obter elogios. As cartas a seguir são um exemplo do apoio que a ICANN recebeu no AF de 2013 por sua participação na segurança da comunidade.

COMNET
Foundation for ICT Development

www.comnet.org.mt

ICANN Security Team

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

2nd July 2012

Re: Commonwealth Cybercrime Initiative

Dear ICANN Security Team,

We would like to express our gratitude and thanks for providing the Commonwealth Cybercrime Initiative the opportunity to host another workshop at the ICANN Meeting in Prague. The Event in Costa Rica was a big success and to follow with another space in Prague was excellent as it provided continuity. We sincerely appreciate the time and resources that ICANN has invested to provide a platform for the Initiative to raise its profile amongst the ICANN community.

Our Prague workshop resulted in two expressions of interest in the CCI from two governments in Africa and we also had excellent additions to our expert resource repository. We are already working on translating these expressions of interest into meaningful activity on the ground.

We are especially grateful of Mr Dave Piscitello's contributions in his capacity as ICANN representative on the CCI Steering Group. Mr Piscitello's involvement, in a very short time resulted in very tangible achievements for the Initiative.

ICANN's support of the Commonwealth Cybercrime Initiative has proven invaluable and we look forward to the opportunity to present the CCI at the next ICANN meeting in Canada if scheduling allows.

Thank you once again, and we look forward to our continued collaboration.

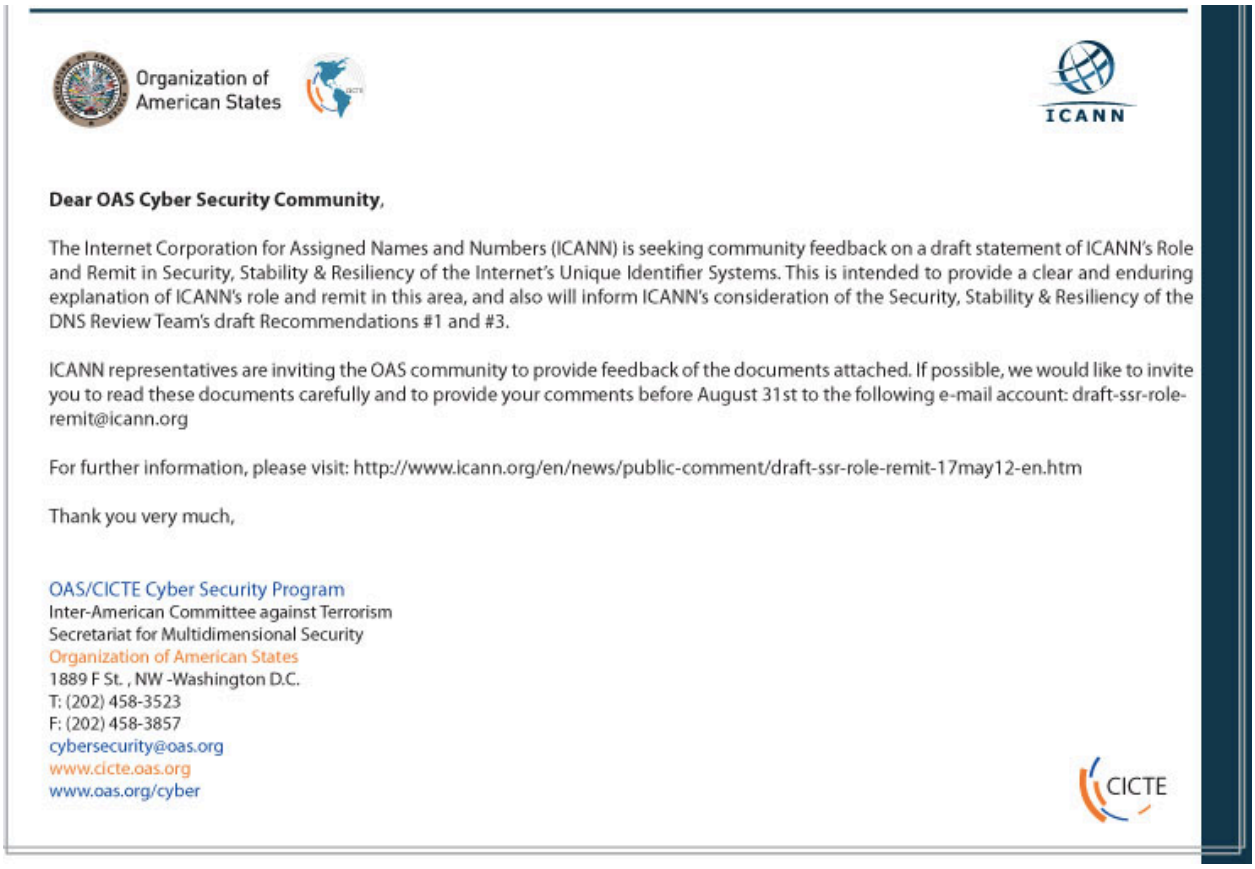
Yours,

Joseph V. Tabone

Chairman CCI Secretariat

Alfir, Reggie Miller Street, Gzira, GZR 1541, Malta | t: (356) 2132 3393 | f: (356) 2132 3390 | e: info@comnet.org.mt

Anexo C — Carta para a ICANN da COMNET



Organization of American States

ICANN

Dear OAS Cyber Security Community,

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. This is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also will inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

ICANN representatives are inviting the OAS community to provide feedback of the documents attached. If possible, we would like to invite you to read these documents carefully and to provide your comments before August 31st to the following e-mail account: draft-ssr-role-remit@icann.org

For further information, please visit: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm

Thank you very much,

OAS/CICTE Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States
1889 F St. , NW -Washington D.C.
T: (202) 458-3523
F: (202) 458-3857
cybersecurity@oas.org
www.cicte.oas.org
www.oas.org/cyber

CICTE

Anexo D — Solicitação de Comentário Público para a comunidade da OEA

CARIBBEAN TELECOMMUNICATIONS UNION
3rd Floor, Victoria Park Suites, 14-17 Victoria Square, Port of Spain, Trinidad & Tobago, W.I.
Tel: (868)627 0281/0347 Fax: (868) 623 1623 E-Mail: ctunion@ctu.int Website: www.ctu.int

7th September, 2012

Mr. Patrick Jones
Senior Manager, Security
Internet Corporation for Assigned Names and Numbers (ICANN)
1101 New York Ave
New York Avenue
Washington DC 20005
USA

Dear Mr. Jones,

Expression of Appreciation

On behalf of the Caribbean Telecommunications Union (CTU), I would like to express our sincere appreciation to you for participating in the CTU's 8th Caribbean Internet Governance Forum, which took place from the 29th to 30th August, 2012 at the Bay Gardens Hotel, Castries, St. Lucia.

Thank you for your presentation on "DNSSEC, Collaboration and Training" which was well received by the audience.

I take this opportunity to re-affirm the CTU's commitment to Caribbean ICT development and look forward to an ongoing partnership with ICANN in supporting Caribbean countries as they seek to leverage the power of ICT for social and economic development.

Sincerely,

Bernadette Lewis
SECRETARY GENERAL

Anexo E — Carta para a ICANN da União de Telecomunicações do Caribe (CTU)

Europol Unclassified – Basic Protection Level

The Hague, 3 January 2013

Ref: 647233

Dr Stephen D. Crocker
Internet Corporation for Assigned Names and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Dear Dr Crocker, Dear Steve!

Dave Piscitello of ICANN visited us in The Hague on 12 December. The purpose of this meeting was for Dave to be informed on the development of the new European Cybercrime Centre (EC3), ourselves to be aware of ICANN cooperation with law enforcement and all of us to see how this could specifically work between ICANN and the EC3.

We were all pleased by the constructive dialogue and positive outcomes of the meeting. There appear clear opportunities for the EC3 to play the role of facilitator with ICANN for MS law enforcement, both with respect to their views on internet governance and in training to improve investigative capabilities. We will be in contact with Dave over the specifics concerning this in the coming weeks.

The EC3 is very appreciative of this initiative between our two organisations and hope that you can lend your full support to it. Thank you very much.

Yours sincerely,

Troels Oerting
Assistant Director
Head of European Cybercrime Centre (EC3)

EDOC#647233

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

Anexo F — Carta para a ICANN da EC3