Panorama Setorial da Internet

Número 2
Julho, 2026
Ano 18

Internet no Brasil: robustez, confiança e mais segurança

Construindo confiança no ambiente digital: o papel do NIC.br na promoção de uma Internet mais segura no Brasil[1]

A disseminação da Internet e das tecnologias digitais tem impulsionado uma transformação digital cada vez mais acelerada em diversas dimensões da sociedade, nos âmbitos da vida social e econômica, ampliando sua centralidade nas atividades cotidianas de indivíduos, organizações e governos. Se, por um lado, a crescente incorporação dessas tecnologias está associada a importantes benefícios para o desenvolvimento econômico e o bem-estar social, a ampliação de sua presença nas atividades cotidianas também introduz novos desafios. Entre eles, destacam-se a crescente exposição a riscos digitais e possíveis incidentes de segurança associados ao uso de dispositivos conectados à Internet, o que, em alguma medida, torna seus usuários mais vulneráveis no ambiente digital.

Desde sua concepção, a Internet foi desenvolvida em um contexto caracterizado por relações de confiança entre os participantes que se interligam na rede de computadores, composta inicialmente por um número limitado de instituições acadêmicas, governamentais e de pesquisa, com vínculos ou propósitos em comum. Nesse contexto, os protocolos fundamentais da rede foram projetados com foco na interoperabilidade e na troca de informações, sem incorporar mecanismos robustos de segurança como requisitos centrais de seu desenho. Com a expansão da rede e sua crescente utilização por diferentes segmentos da sociedade, essa premissa original de confiança mostrou-se insuficiente diante dos desafios contemporâneos de segurança digital.

[1] Este artigo foi redigido por Javiera F. Medina Macaya, pesquisadora no Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), a partir dos materiais institucionais de cada uma das iniciativas do NIC.br. Javiera é doutora em Administração de Empresas e mestre em Administração Pública e Governo pela Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas (FGV EAESP), com graduação em Gestão de Políticas Públicas pela Universidade de São Paulo (USP). O artigo contou com a revisão de gestores envolvidos nessas iniciativas.

Não há uma solução única para a segurança e o tratamento de incidentes; por isso, a operacionalização dessas atividades passa por diversas frentes de atuação do NIC.br, de modo que seus vários departamentos atuam para fomentar uma rede baseada nos princípios de governança aprovados pelo CGI.br.

Embora os protocolos fundamentais da Internet tenham evoluído ao longo do tempo, incorporando novos mecanismos e extensões, muitos deles continuam baseados em uma arquitetura concebida em um contexto no qual a segurança não constituía um requisito central. Com a crescente expansão da conectividade e a intensificação da digitalização das atividades econômicas e sociais, ataques à segurança ganham outras proporções, e seus riscos e incidentes assumem maior escala e complexidade. Se, no passado, a realização de ataques exigia elevado conhecimento técnico e tendia a produzir impactos relativamente limitados, atualmente a ampla disponibilidade de ferramentas automatizadas reduziu as barreiras de entrada para agentes maliciosos, ao mesmo tempo em que ampliou significativamente o potencial de impacto sobre indivíduos, organizações e infraestruturas críticas.

Um dos princípios[2] que rege a governança da Internet no Brasil trata da preservação da funcionalidade, da segurança e da estabilidade da rede. Para assegurar esses três atributos, é fundamental a adoção de medidas técnicas alinhadas a padrões internacionais e o estímulo à implementação de boas práticas por parte dos diferentes atores do ecossistema digital. Nesse contexto, o NIC.br, entidade ligada ao CGI.br, é responsável por realizar o registro de nomes de domínio e a alocação de endereços de protocolo de Internet (*Internet Protocol* [IP]) no Brasil, bem como apoiar o desenvolvimento da Internet no país, promovendo sua segurança, estabilidade e resiliência. Essas atividades fomentam a estabilidade e robustez da rede no Brasil, incluindo a produção de estudos, recomendação de normas e padrões técnicos para redes e serviços de Internet, e o tratamento e a resposta a incidentes de segurança.

Não há uma solução única para a segurança e o tratamento de incidentes; por isso, a operacionalização dessas atividades passa por diversas frentes de atuação do NIC.br, de modo que seus vários departamentos atuam para fomentar uma rede baseada nos princípios de governança aprovados pelo CGI.br. A seguir, são apresentadas ações relacionadas à promoção de uma Internet mais segura no Brasil.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), departamento do NIC.br, atua como um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso. Com a missão de aumentar os níveis de segurança e capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil, o CERT.br atua na área de Gestão de Incidentes de Segurança da Informação, prestando serviços para qualquer rede que utilize recursos administrados pelo NIC.br; tais serviços se estruturam em: gestão de incidentes, consciência situacional e transferência de conhecimento. No artigo I ("Segurança e tratamento de incidentes de segurança no Brasil: história e papel do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil"), Cristine Hoepers, gerente do CERT.br, apresenta a história, as áreas de atuação e o papel do departamento no processo de tratamento a incidentes. Uma iniciativa importante é a Cartilha de Segurança para Internet, que reúne uma série de publicações com recomendações e dicas para uma navegação mais segura e proteção de possíveis ameaças, com usuários de Internet como público-alvo.

[2] Os Princípios para a Governança e Uso da Internet no Brasil, elaborados e adotados pelo Comitê Gestor da Internet no Brasil (CGI.br) em 2009 (Resolução CGI.br/RES/2009/003/P), embasam e orientam as ações e as decisões do comitê. Mais informações sobre a resolução e os princípios em: https://www.cgi.br/resolucoes/documento/2009/003/ e https://principios.cgi.br/

Outra parte importante diz respeito à robustez e à qualidade da infraestrutura no país. O Registro.br é o departamento do NIC.br responsável pelas atividades de registro e manutenção dos nomes de domínio sob o .br, e por sua publicação via Sistema de Nome de Domínio (*Domain Name System* [DNS]). Além da segurança e da robustez que caracterizam os serviços de DNS, desde 2007 é possível utilizar um *Domain Name System Security Extensions* (DNSSEC), um padrão internacional que confirma o conteúdo do DNS e ajuda a impedir ataques ao validar os dados e garantir a origem das informações. Outro aspecto ligado à infraestrutura é a manutenção no país de espelhos dos servidores-raiz da Internet; um de seus resultados é a melhora da qualidade do acesso por redes brasileiras, já que as informações sobre a raiz da Internet estão duplicadas e fisicamente mais próximas.

A robustez e a qualidade da infraestrutura da rede no Brasil também são fomentadas pelo IX.br (Internet Exchange Points), do Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (Ceptro.br), departamento do NIC.br responsável pelos Pontos de Troca de Tráfego (PTT), os quais promovem a interconexão direta e local entre sistemas autônomos (*Autonomous Systems* [AS]) que compõem a Internet no Brasil. Com 39 PTT distribuídos em áreas metropolitanas das cinco regiões do país, o IX.br é o maior conjunto de PTT do mundo: são cerca de 3,8 mil AS participantes, os quais geram mais de 7 mil conexões em todas as localidades. Essa infraestrutura compartilhada possibilita que o tráfego de dados se mantenha regionalizado, racionalizando o trajeto percorrido pelos dados e viabilizando uma Internet mais veloz, eficiente, resiliente e com custo mais baixo para o usuário final. Em países de grandes dimensões territoriais como o Brasil, os PTT cumprem um papel importante na disseminação da Internet por todo o território, uma vez que facilitam a provedores locais levarem banda larga até localidades menos atrativas comercialmente para as grandes operadoras.

Além da infraestrutura, a sensibilização sobre a importância, a formação e a articulação de atores em torno dos PTT é fundamental: quanto maior o número de participantes, mais denso será o ecossistema de redes interconectadas entre si. Por isso, além dos PTT, o NIC.br criou o projeto OpenCDN[3], o qual busca diminuir a distância entre as redes de distribuição de conteúdo (*Content Delivery Network* [CDN]) e os usuários de Internet por meio do compartilhamento de infraestrutura. Com o OpenCDN, essas redes de distribuição de conteúdo podem instalar seus servidores de cachê nos *data centers* da iniciativa, localizados em diferentes regiões do Brasil e ligados aos PTT locais do IX.br. A crescente concentração de tráfego em infraestruturas locais ilustra essa dinâmica: em 2026, o IX.br alcançou 50 Tbit/s de tráfego agregado, enquanto o OpenCDN ultrapassou 1 Tbit/s de distribuição de conteúdo no país[4].

Em países de grandes dimensões territoriais como o Brasil, os PTT cumprem um papel importante na disseminação da Internet por todo o território, uma vez que facilitam a provedores locais levarem banda larga até localidades menos atrativas comercialmente para as grandes operadoras.

[3] Saiba mais: https://opencdn.nic.br/

[4] Disponível em: https://ix.br/noticia/releases/ix-br-bate-recorde-de-50-tbit-s-de-trafego-internet-agregado-impulsionado-por-conteudo-e-servicos-digitais/

Figura 1 - ALGUMAS INICIATIVAS DO NIC.br EM PROL DA SEGURANÇA, ESTABILIDADE E ROBUSTEZ DA INTERNET NO BRASIL

Internet Segura

https://internetsegura.br/

INTERNET SEGURA BR

Portal que reúne iniciativas de conscientização sobre segurança e uso responsável da Internet no Brasil, com materiais com foco em diferentes públicos.

Programa por uma Internet mais segura

https://bcp.nic.br/i+seg/

PROGRAMA INTERNET +SEGURA

Iniciativa que promove a divulgação e uso de padrões utilizados na Internet e fomenta iniciativas educacionais e políticas públicas ligadas à Internet.

Desafio BCOP

https://bcp.nic.br/desafiobcop/

BCOP

Prêmio destinado a instituições que adotam boas práticas operacionais e de segurança, dando visibilidade e reconhecimento aos esforços das instituições participantes.

Pesquisas sobre o uso das TIC no Brasil

https://cetic.br/pt/pesquisas/

cetic.br

Dados robustos para monitorar aspectos relacionados às políticas de segurança digital e segurança da informação por indivíduos e estabelecimentos.

Cartilha de Segurança para Internet

https://cartilha.cert.br/

Portal composto por um conjunto de documentos com recomendações e dicas para usuários sobre um uso mais seguro da Internet e como se proteger de possíveis ameaças.

BCP

https://bcp.nic.br/

BCP

Portal que reúne um conjunto de boas práticas operacionais para Sistemas Autônomos conectados à Internet.

SIMET

https://simet.nic.br/

SIMET

Sistema disponibilizado para o público testar e encontrar informações sobre as métricas de qualidade da Internet, permitindo entender melhor a capacidade da rede.

Fonte: elaboração própria.

Outra iniciativa relevante é o Portal de boas práticas para a Internet no Brasil (BCP), mantido por profissionais de diversas áreas do NIC.br, como CERT.br, Ceptro.br e Registro.br, em colaboração com especialistas externos ao NIC.br. O portal está voltado à conscientização e à disseminação de boas práticas operacionais (*Best Current Practice* [BCP]) para AS conectados à Internet, oferecendo recomendações técnicas. Embora não exclusivamente, o portal se baseia nas BCP publicadas pela *Internet Engineering Task Force* (IETF) direcionadas a AS; por meio dele, é também possível se atualizar quanto à evolução dos padrões para a Internet. Nessa iniciativa, também há o Desafio BCOP, que premia instituições pela adoção de BCP e de segurança.

O Programa por uma Internet mais segura[5] é outra das iniciativas conduzidas pelo NIC.br no âmbito da segurança, que engloba algumas das iniciativas mencionadas. Por meio de diversas atividades, busca apoiar a comunidade técnica da Internet para reduzir ataques distribuídos de negação de serviços (*Distributed Denial of Service* [DDoS]) em redes brasileiras, sequestro de prefixos, vazamento de rotas, falsificação de endereços IP de origem, vulnerabilidades e falhas de configuração presentes nos elementos da rede. Além disso, também pretende aproximar as diferentes equipes responsáveis por segurança e estabilidade da rede para criar uma cultura de segurança entre seus operadores. Considerando que as questões de segurança são complexas e demandam uma ação conjunta, o programa envolve diretamente quatro departamentos técnicos do NIC.br: CERT.br, Registro.br, Ceptro.br e IX.br. Nesta edição do PSI, a entrevista I ("Segurança da Internet no Brasil: uma trajetória de cooperação") publicada com Gilberto Zorello, coordenador de Projetos do NIC.br, apresenta essas iniciativas, destacando a importância da colaboração e de sua disseminação entre os diferentes públicos-alvo.

A produção de métricas relevantes e confiáveis é também uma atividade desenvolvida pelo NIC.br que contribui para orientar processos de tomada de decisão e a formulação de políticas públicas. Além das métricas relativas a aspectos de segurança da rede, o NIC.br cuida de medições e estatísticas via área de Medições[6] do Ceptro.br|NIC.br e do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br|NIC.br).

O Ceptro.br|NIC.br, responsável por iniciativas e projetos que apoiam ou aperfeiçoam a infraestrutura da Internet no Brasil, contribuindo para seu desenvolvimento; na área de medições, especificamente, foi desenvolvido o Sistema de Medição de Tráfego Internet (SIMET), por meio do qual são organizadas iniciativas com o objetivo de melhorar a qualidade da Internet e ações que apoiam e aperfeiçoam a infraestrutura da Internet no Brasil. O SIMET é uma tecnologia que permite aos usuários realizar medições de qualidade da Internet precisas e confiáveis, avaliando a qualidade de conexão e explicando o que cada valor significa e como ele impacta sua experiência na Internet; dessa forma, provê informações relevantes que ajudam os usuários a identificar e resolver problemas na conexão. Os aspectos que devem ser destacados são a confiabilidade e a independência, baseadas na possibilidade de fazer medições para servidores SIMET dentro e fora das redes dos provedores, nos servidores neutros do NIC.br localizados nos PTT. Além disso, o SIMET tem soluções pensadas para consumidores, provedores, o setor público (nas áreas de educação e saúde, por exemplo) e integradores de soluções, a fim de promover uma melhoria contínua das redes.

A produção de métricas relevantes e confiáveis é também uma atividade desenvolvida pelo NIC.br que contribui para orientar processos de tomada de decisão e a formulação de políticas públicas. Além das métricas relativas a aspectos de segurança da rede, o NIC.br cuida de medições e estatísticas via área de Medições do Ceptro.br|NIC.br e do Cetic.br|NIC.br.

[5] Saiba mais: https://bcp.nic.br/i+seg/
[6] Saiba mais: https://medicoes.nic.br/

A estabilidade dos projetos desenvolvidos pelos diferentes departamentos do NIC.br permite a continuidade e a perenidade dos diversos serviços. (...) as ações viabilizam a criação de relações de confiança e reconhecimento nacional e internacional (...).

O Cetic.br | NIC.br, por sua vez, é o departamento responsável pela produção de dados estatísticos e análises sobre o acesso e o uso das tecnologias de informação e comunicação (TIC) no Brasil. Para isso, são utilizadas abordagens metodológicas definidas internacionalmente, a fim de garantir a comparabilidade internacional dos dados produzidos, conduzindo pesquisas de abrangência nacional em diversos setores da sociedade, seja em relação aos indivíduos ou a estabelecimentos. Especificamente, o centro coleta dados sobre políticas e práticas de segurança digital existentes nas empresas brasileiras por meio da pesquisa TIC Empresas; incidentes de segurança e ataques pela pesquisa TIC Provedores; políticas de segurança da informação pelas pesquisas TIC Saúde, TIC Educação e TIC Organizações sem Fins Lucrativos. Por sua vez, a pesquisa Privacidade e Proteção de Dados Pessoais, que conta com apoio institucional da Autoridade Nacional de Proteção de Dados (ANPD), busca compreender os desafios para a construção de um ecossistema digital que garanta a privacidade e a proteção de dados pessoais no Brasil, reunindo indicadores coletados com indivíduos, empresas e organizações públicas (governo, saúde e educação), com a finalidade de identificar suas práticas e suas percepções sobre o tema. Por fim, as pesquisas TIC Domicílios e TIC Kids Online abordam, a partir da perspectiva de indivíduos, questões relacionadas à segurança digital.

Além de todas essas iniciativas voltadas para especialistas e técnicos, o NIC.br também promove a conscientização sobre segurança e uso responsável da Internet no Brasil, com materiais de auxílio voltados para internautas. O portal Internet Segura[7] funciona como um espaço que reúne informações de interesse e materiais com foco em diferentes públicos: crianças, adolescentes, pais, responsáveis e educadores, pessoas idosas, técnicos e o público em geral.

A estabilidade dos projetos desenvolvidos pelos diferentes departamentos do NIC.br permite a continuidade e a perenidade dos diversos serviços. Buscando sempre uma Internet melhor no Brasil, as ações viabilizam a criação de relações de confiança e reconhecimento nacional e internacional, reputação essencial nas relações dentro do ecossistema de segurança digital, por viabilizar parcerias internacionais valiosas com instituições correlatas.

Em conjunto, essas iniciativas evidenciam a atuação abrangente do NIC.br para a promoção de uma Internet mais segura, estável e resiliente no Brasil. Por meio do fortalecimento da infraestrutura crítica da rede, da coordenação de ações de prevenção e resposta a incidentes, da disseminação de boas práticas técnicas, da capacitação da comunidade de operadores, e da produção de dados e indicadores sobre segurança digital, o NIC.br contribui para a construção de um ambiente digital mais confiável para usuários, organizações e instituições públicas.

Por articular diferentes atores do ecossistema da Internet, promover soluções alinhadas aos padrões internacionais e fortalecer a segurança, a estabilidade e a resiliência da rede, o NIC.br promove a ampliação da capacidade nacional de enfrentar riscos digitais, elevar a qualidade e a segurança dos serviços de Internet e fortalecer a confiança no ambiente digital. Dessa forma, o NIC.br cria condições para que os benefícios econômicos e sociais da transformação digital sejam usufruídos de maneira mais segura e sustentável por toda a sociedade brasileira.

[7] Saiba mais: https://internetsegura.br/

Artigo II

Segurança e tratamento de incidentes de segurança no Brasil: história e papel do CERT.br

Por Cristine Hoepers

Foto: Klaus Steding-Jessen

Cristine Hoepers
Gerente do CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (*Computer Security Incident Response Team* [CSIRT]) de Responsabilidade Nacional de último recurso, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), cuja missão é aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

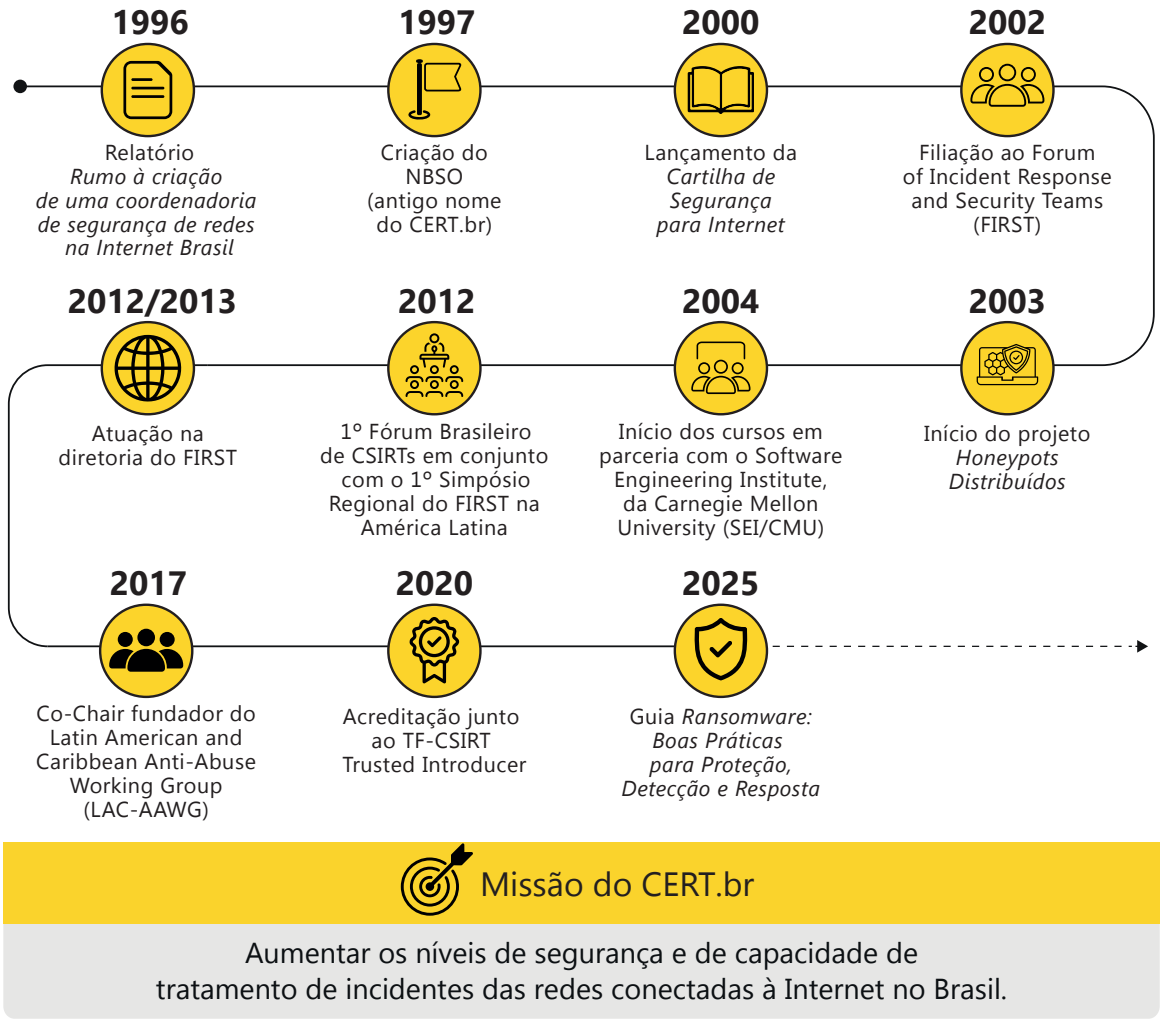
Sua história começa a ser delineada em agosto de 1996, com a publicação do relatório *Rumo à criação de uma coordenadoria de segurança de redes na Internet Brasil* (Gomide *et al*., 1996), produzido pelo Subgrupo de Trabalho de Segurança do Grupo de Trabalho em Engenharia de Redes (GTER), do Comitê Gestor da Internet no Brasil (CGI.br). Esse relatório foi fruto de um ano de debates na comunidade Internet nacional, motivado pela necessidade de lidar com o crescimento no número de incidentes de segurança em computadores, que acompanhava o vigoroso crescimento da Internet no Brasil após sua abertura para exploração comercial, em 1995. O relatório apresentou um diagnóstico da situação do país naquele momento e apontou alguns caminhos a serem seguidos para a criação de uma estrutura que auxiliasse as organizações a melhor lidar com incidentes, considerando a complexidade e a escala do cenário nacional. Esse diagnóstico descrevia os objetivos e atribuições almejados pela comunidade para um centro de coordenação de temas relacionados à segurança digital no Brasil:

> O objetivo da criação de uma organização encarregada de coordenar a segurança de redes não é que ela tome para si todas as tarefas que necessitam ser efetuadas. Esta organização deve possuir um conjunto básico de atribuições a partir dos quais ela possa atribuir ou fomentar a realização de tais tarefas por terceiros atuando apenas como coordenadora das atividades. Desta forma, é desejável que possua as seguintes atribuições:
>
> - Receber e registrar ocorrências de violação de segurança de redes;
> - Coletar estatísticas destas ocorrências e torná-las públicas;
> - Orientar tecnicamente os que a ela recorrerem para sanar falhas de segurança;
> - Intermediar o contato entre redes envolvidas em incidentes de segurança servindo como testemunha legal das ações destas;
> - Fomentar a criação de programas de treinamento e atualização em segurança de redes através de interação estreita com o Grupo de Trabalho Formação de Recursos Humanos;

- Fomentar a realização de encontros e congressos de segurança de redes;
- Representar o Brasil como um dos órgãos de segurança em âmbito nacional e internacional. (Gomide *et al*., 1996, seção Atribuições)

Essa visão das necessidades e atribuições pautou a criação, em 1 de junho de 1997, do NIC BR Security Office (NBSO), nome pelo qual o CERT.br foi conhecido até dezembro de 2005 (Figura 1).

Figura 1 - LINHA DO TEMPO CERT.br



Fonte: elaboração própria.

A fase inicial da operação foi dedicada a montar a infraestrutura, apresentar-se à comunidade Internet nacional e internacional e criar uma rede de contatos e cooperação. Em 1999, a divulgação de estatísticas regulares sobre os incidentes reportados ao centro e as primeiras atividades proativas tiveram início, incluindo a realização de palestras de conscientização e divulgação de boas práticas em eventos técnicos especializados de segurança e redes.

Refletindo sobre a história, um dos pontos que facilita até hoje o CERT.br ter a confiança da comunidade e parcerias em diversos setores foi seu início ter contado com uma abordagem participativa e *bottom-up*, que não partiu de uma única pessoa ou agência, mas de profissionais que já conversavam e trabalhavam juntos, o que contribuiu para a construção de uma cooperação forte, com o time reconhecido como parte da comunidade da Internet no Brasil.

À época, existiam apenas algumas dezenas de CSIRTs no mundo; o FIRST[8], por exemplo, contava com apenas 53 membros quase que exclusivamente da Europa e da América do Norte. Montar a operação do CERT.br e escolher os serviços que mais faziam sentido para o cenário brasileiro foi um processo gradual que envolveu focar os poucos recursos humanos disponíveis nas atividades percebidas como as de maior impacto para melhorar a postura de segurança no país, sendo elas: estabelecer-se como um ponto focal para receber e repassar notificações de incidentes para aqueles que necessitavam ser envolvidos na resolução; manter estatísticas desses incidentes, de forma a ter dados para consciência situacional; e fomentar que os Sistemas Autônomos (*Autonomous System* [AS]) e grandes organizações definissem pontos de contato para tratar incidentes e, idealmente, criassem seus próprios CSIRTs.

Desde então, times que prestam serviços de tratamento de incidentes amadureceram, a área assumiu relevância global e *frameworks* e padrões de operação foram criados, inclusive contando com a contribuição de profissionais do CERT.br. Acompanhando essa evolução, os serviços do centro foram reestruturados de acordo com esses *frameworks* e estão agrupados nas seguintes grandes áreas: Gestão de Incidentes, Transferência de Conhecimento e Consciência Situacional (Figura 2).

O principal papel do CERT.br é atuar como ponto de contato nacional de último recurso para notificações de incidentes de segurança, principalmente quando um contato mais específico não é conhecido, de forma a auxiliar a análise e encaminhar o assunto para os contatos corretos.

GESTÃO DE INCIDENTES

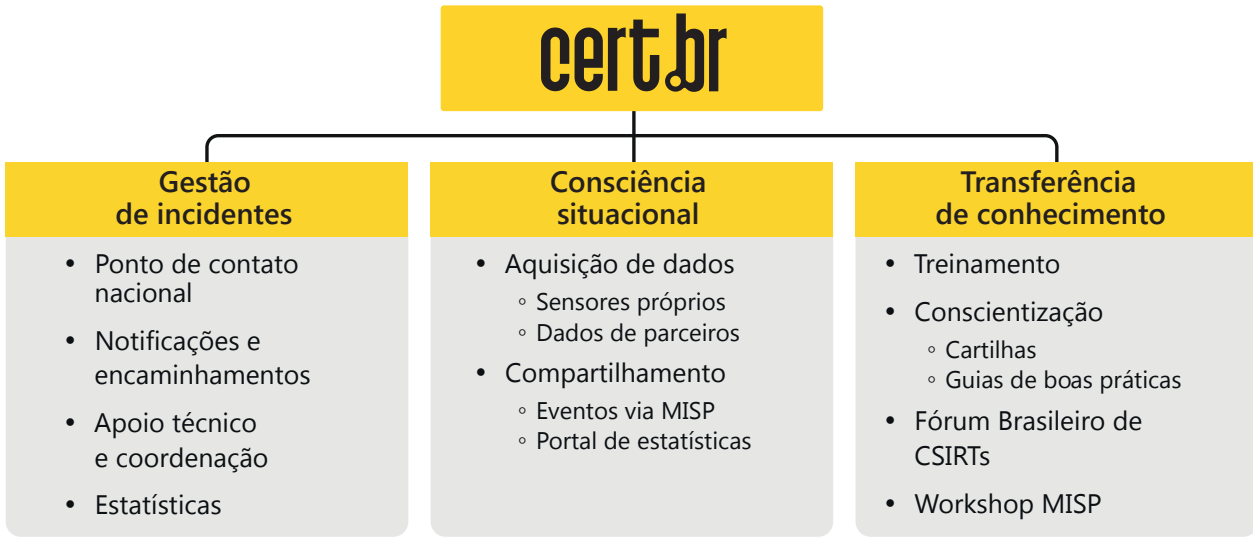
O principal papel do CERT.br é atuar como ponto de contato nacional de último recurso para notificações de incidentes de segurança, principalmente quando um contato mais específico não é conhecido, de forma a auxiliar a análise e encaminhar o assunto para os contatos corretos. Esse trabalho visa facilitar a comunicação entre profissionais, especialistas e outras equipes, no país e no exterior, que possam atuar no tratamento de um incidente de segurança.

Cabe ressaltar que o CERT.br não tem acesso às instalações ou a sistemas de terceiros: sua atuação é focada em habilitar outros times a responder os incidentes da maneira mais efetiva possível. Nesse processo, a equipe técnica auxilia a comunicação efetiva para atingir a resolução do incidente através de um trabalho colaborativo, preferencialmente com os CSIRTs ou os Centros de Operações de Segurança (*Security Operations Centers* [SOCs]) estabelecidos pelas entidades envolvidas, que podem ser empresas, universidades, provedores de acesso e serviços de Internet, órgãos de governo ou outros AS que façam parte do ecossistema nacional de Internet. Nesse processo, a equipe também ajuda os envolvidos na análise de atividades maliciosas e de sistemas comprometidos, e

[8] Saiba mais: https://www.first.org/

na recomendação de linhas de ação que possam ajudar a recuperar os sistemas e mitigar os danos causados. O portal de estatísticas do CERT.br[9] conta com dados gerais sobre essas notificações voluntárias de incidentes recebidas em seu *e-mail* de contato para esses fins e também com estatísticas específicas sobre páginas falsas utilizadas em tentativas de *phishing,* que derivam dessas notificações (Figura 3).

Figura 2 - CERT.br E ÁREAS DE ATUAÇÃO



Fonte: elaboração própria.

Figura 3 - GESTÃO DE INCIDENTES: FLUXO DO PROCESSO OPERACIONAL

Fonte: elaboração própria.

[9] Disponível em: https://stats.cert.br/

TRANSFERÊNCIA DE CONHECIMENTO

O CERT.br também investe em atividades que permitam transferir para a comunidade o conhecimento adquirido com a experiência na área e com a análise de ameaças e vulnerabilidades observadas no dia a dia. Essas atividades incluem cursos, incentivo para a formação de uma comunidade de CSIRTs no país e disseminação de boas práticas e materiais de conscientização, com o objetivo de melhor prevenir e tratar incidentes de segurança.

O primeiro material publicado pelo CERT.br foi fruto de uma demanda da comunidade: a Cartilha de Segurança para Internet[10]. Sua história começou em uma reunião com representantes da Associação Brasileira de Internet (Abranet) e da Federação das Indústrias do Estado de São Paulo (FIESP) no primeiro trimestre do ano 2000, momento em que os provedores de acesso à Internet presentes externaram a dificuldade de encontrar material confiável e conciso que pudesse ser usado por seus setores de atendimento aos clientes para auxiliá-los quando tinham problemas de segurança. Após a publicação da primeira versão, seu uso ultrapassou a comunidade técnica e começou a se disseminar diretamente entre os usuários de Internet. Desde então, a cartilha passou por várias reformulações que foram acompanhando não só a evolução tecnológica e do ambiente de ameaças, mas também a evolução sobre como comunicar dicas de segurança de forma mais simples, concisa, direta e com ilustrações.

Outra atividade-chave nessa área é a parceria com o SEI/CMU, para ministrar no Brasil os treinamentos desenvolvidos pelo CERT Coordination Center (CERT/CC), atual CERT Division, que foi o primeiro CSIRT criado no mundo. Num país tão grande e diverso como o Brasil, focar no treinamento e no apoio a outras equipes é uma abordagem muito mais eficaz do que oferecer serviços *hands-on* de resposta a incidentes. Adicionalmente, em vez de tentar escrever seu próprio treinamento, a parceria com o SEI/CMU permite ao CERT.br focar em transmitir o conteúdo de boas práticas globais, mas com ênfase em como aplicá-las ao ambiente nacional.

Além disso, a parceria foi muito além, pois o material, hoje, conta com contribuições significativas de conteúdo feitas pelo time ao material ensinado nos Estados Unidos e em outros países. Esses treinamentos[11] são ministrados desde 2004 e já refletiram na capacitação de mais de 2 mil profissionais especializados para atuar em times de tratamento de incidentes. Com essa comunidade crescente, outra atividade importante é a realização anual do Fórum Brasileiro de CSIRTs[12], que ocorre desde 2012 e atualmente reúne cerca de 800 profissionais a cada edição, em um evento dedicado à construção de comunidade e à discussão de assuntos relacionados com a resiliência das organizações face a incidentes de segurança.

Outros materiais de destaque são as recomendações técnicas e boas práticas publicadas pelo centro, com destaque para o material *Ransomware: boas práticas para proteção, detecção e resposta* (CERT.br, 2025), que é focado em passos básicos que organizações de qualquer porte podem adotar para prevenir e, caso afetadas, mitigar os impactos deste tipo de ataque.

O CERT.br também investe em atividades que permitam transferir para a comunidade o conhecimento adquirido com a experiência na área e com a análise de ameaças e vulnerabilidades observadas no dia a dia. Essas atividades incluem cursos, incentivo para a formação de uma comunidade de CSIRTs no país e disseminação de boas práticas e materiais de conscientização (...).

[10] Saiba mais: https://cartilha.cert.br/
[11] Disponível em: https://cursos.cert.br/
[12] Saiba mais: https://forum.cert.br/

De forma a melhor entender o cenário de ameaças e complementar a visão obtida com notificações voluntárias, o CERT.br trabalha proativamente para obter mais fontes de dados, a fim de aumentar a capacidade de detecção de incidentes e determinação de tendências de ataques que afetem organizações conectadas à Internet no Brasil.

CONSCIÊNCIA SITUACIONAL

De forma a melhor entender o cenário de ameaças e complementar a visão obtida com notificações voluntárias, o CERT.br trabalha proativamente para obter mais fontes de dados, a fim de aumentar a capacidade de detecção de incidentes e determinação de tendências de ataques que afetem organizações conectadas à Internet no Brasil.

As primeiras atividades relacionadas com essa área iniciaram em 2003, com o início da implantação do Projeto Honeypots Distribuídos (CERT.br, s.d.), que consiste em uma rede de sensores passivos (*honeypots*) distribuídos em diversas redes do país. Esse projeto propicia um termômetro sobre as atividades maliciosas no espaço de Internet brasileiro, além de permitir a detecção de dispositivos brasileiros comprometidos e abusados por atacantes.

Além dessa fonte própria de dados sobre ataques recebidos por redes no Brasil, o CERT.br estabeleceu uma rede de parceiros globais que compartilham dados de ameaças relacionadas aos AS alocados ao Brasil, em geral indícios de sistemas que possam estar mal configurados (permitindo uso abusivo), vulneráveis ou com indícios de comprometimento. São exemplos de parceiros globais do CERT.br nessa área: Team Cymru[13], ShadowServer Foundation[14] e Spamhaus[15].

Esses dados são usados não só para o compartilhamento de estatísticas sobre o perfil dos ataques no Portal de Estatísticas do CERT.br[16], mas as redes potencialmente afetadas são regularmente notificadas pelo CERT.br com instruções sobre como testar os problemas e como se recuperar. Adicionalmente, o CERT.br compartilha algumas informações mais detalhadas com comunidades setoriais através da plataforma MISP[17], uma plataforma para compartilhamento de dados sobre ameaças amplamente utilizada entre CSIRTs. Para fomentar que esse compartilhamento cresça e beneficie cada vez mais o país, o CERT.br promove anualmente um *workshop* gratuito (Workshop MISP), realizado em conjunto com o Fórum Brasileiro de CSIRTs[18].

Impacto internacional

O CERT.br possui forte integração com as comunidades nacional e internacional de CSIRTs, o que o leva à formação de relações de confiança, ao estabelecimento de uma rede de contatos com atores-chave e ao reconhecimento da competência e da qualidade de seu trabalho. A Figura 4 ilustra as redes de colaboração nas quais o CERT.br está inscrito.

[13] Saiba mais: https://www.team-cymru.com/
[14] Saiba mais: https://www.shadowserver.org/
[15] Saiba mais: https://www.spamhaus.org/
[16] Disponível em: https://stats.cert.br/
[17] Saiba mais: https://www.misp-project.org/
[18] Saiba mais: https://forum.cert.br/

Figura 4 – CERT.br, ATORES INSTITUCIONAIS E REDES DE COLABORAÇÃO

Fonte: elaboração própria.

Ao longo dos anos, diversos profissionais contribuíram (e, em muitos casos, lideraram) para o desenvolvimento de boas práticas, normas e *frameworks* que, hoje, são referência mundial. São exemplos desse impacto:

- *Computer Security Incident Response Team (CSIRT) services framework* (FIRST, 2019);
- *Team Types Within the Context of Services Frameworks* (FIRST, 2025);
- *CSIRT Roles and Competences (Addendum)* (FIRST, 2022);
- *LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1* (Latin American and Caribbean Network Operators Group [LACNOG] & Messaging, Malware and Mobile Anti-Abuse Working Group [M³AAWG], 2019).

O CERT.br também é ativo colaborador do FIRST e seus profissionais participaram ao longo do tempo de várias formas, com destaque para o assento no Conselho Diretor (2012/2013) e a posição de *Chair* da conferência anual (2020)[19]. Atualmente, seus profissionais participam do Comitê de Filiação, da coordenação do "Capture The Flag" da conferência anual e de vários grupos de interesse especial (*Special Interest Groups* [SIG]) da organização.

[19] Saiba mais: https://www.first.org/about/organization/directors

Ao longo de quase três décadas, o CERT.br consolidou-se como um dos principais pilares técnicos da segurança da Internet no Brasil, desempenhando um papel estratégico na coordenação de incidentes, na disseminação de boas práticas e no fortalecimento da resiliência digital do país.

Considerações finais

A trajetória do CERT.br acompanha a própria evolução da Internet no Brasil e evidencia a importância de estruturas técnicas especializadas para fortalecer a segurança e a resiliência do ecossistema digital brasileiro. O CERT.br consolidou-se como um ponto focal nacional para coordenação de incidentes, articulando redes de cooperação entre provedores, empresas, academia, governo e comunidades técnicas, sempre com base em uma abordagem colaborativa e multissetorial, alinhada à natureza multissetorial do NIC.br e do CGI.br.

Ao longo de sua atuação, o CERT.br contribuiu não apenas para o tratamento de incidentes, mas também para o fortalecimento das capacidades nacionais em segurança cibernética por meio de atividades de conscientização, produção de conhecimento, formação de profissionais especializados e disseminação de boas práticas. Paralelamente, iniciativas de coleta e compartilhamento de dados sobre ameaças ampliaram a consciência situacional sobre o cenário de segurança no país e reforçaram a capacidade de prevenção e resposta das organizações conectadas à Internet.

Em um contexto marcado pela crescente complexidade das ameaças digitais, pela expansão da adoção de tecnologias emergentes como a Internet das Coisas (*Internet of Things* [IoT]) e pelo avanço da Inteligência Artificial (IA), a experiência do CERT.br demonstra que confiança, cooperação e capacitação contínua são elementos essenciais para a sustentabilidade da transformação digital. Seu reconhecimento internacional e sua contribuição para frameworks e boas práticas globais reforçam o papel estratégico do Brasil nas discussões internacionais sobre segurança cibernética.

Ao longo de quase três décadas, o CERT.br consolidou-se como um dos principais pilares técnicos da segurança da Internet no Brasil, desempenhando um papel estratégico na coordenação de incidentes, na disseminação de boas práticas e no fortalecimento da resiliência digital do país. Sua atuação colaborativa e contínua tem contribuído para tornar a infraestrutura da Internet no Brasil progressivamente mais segura, confiável e resiliente, ampliando a capacidade nacional de prevenção, deteção e resposta a ameaças cibernéticas.

Além disso, o CERT.br tornou-se uma referência internacional ao promover a cooperação entre atores nacionais e globais, apoiar o desenvolvimento de capacidades técnicas e fortalecer a confiança no ecossistema digital brasileiro. Em um cenário de crescente complexidade das ameaças digitais, preservar e fortalecer o modelo multissetorial de governança representado pelo CGI.br | NIC.br, que se baseia em coordenação técnica, cooperação, participação da comunidade e construção de consensos, é fundamental para garantir uma Internet cada vez mais segura, estável e confiável para o futuro.

Referências

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (s.d.). *Distributed honeypots project.* HoneyTARG. https://honeytarg.cert.br/honeypots/index-po.html

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2025). *Ransomware: boas práticas para proteção, detecção e resposta*. https://cert.br/docs/ransomware/

Forum of Incident Response and Security Teams. (2019). *Computer Security Incident Response Team (CSIRT) Services Framework*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Forum of Incident Response and Security Teams. (2022). *CSIRT Roles and Competences (Addendum). https://www.first.org/standards/frameworks/csirts/csirt_roles_competences*

Forum of Incident Response and Security Teams. (2025). *Team types within the context of services frameworks*. https://www.first.org/standards/frameworks/csirts/team-type_1.2

Gomide, A. C., Pinheiro, C. A. C., Vazquez, P. A. M. (1996). Rumo a criação de uma coordenadoria de segurança de redes na Internet Brasil. CERT.br. https://www.cert.br/sobre/estudo-cgibr-1996.html

Latin American and Caribbean Network Operators Group, & Messaging, Malware and Mobile Anti-Abuse Working Group. (2019). *LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1*. https://www.m3aawg.org/sites/default/files/doc_files/lac-bcop-1-m3aawg-v1.pdf

Entrevista I

Segurança da Internet no Brasil: uma trajetória de cooperação

Foto: Ricardo Matsukawa

Gilberto Zorello
Coordenador de Projetos do NIC.br

Nesta entrevista, Gilberto Zorello, coordenador de projetos do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), reflete sobre a criação e a evolução do Programa por uma Internet mais Segura, destacando seus principais marcos, estratégias e boas práticas para a promoção da segurança digital no Brasil, além de abordar o papel da colaboração entre diferentes atores do ecossistema no fortalecimento da confiança e dos avanços em segurança da Internet no país.

Panorama Setorial da Internet (P.S.I.)_ Para começar, você poderia nos apresentar o Programa por uma Internet mais Segura? Em que contexto esse programa foi criado, quando teve início e quais foram os principais objetivos que orientaram sua concepção?

Gilberto Zorello (G.Z.)_ Nos últimos anos, o número de incidentes de segurança na Internet têm crescido de forma contínua, com impactos direta ou indiretamente a estabilidade, o desempenho e a confiabilidade dos serviços que dependem da infraestrutura da rede. Incidentes de segurança podem causar prejuízos significativos, como: tempo de inatividade, necessidade de depuração e reconfiguração de equipamentos, além do consumo indevido de banda por ataques distribuídos de negação de serviço (*Distributed Denial of Service* [DDoS]) originados em outras redes e, muitas vezes, nas próprias redes. Muitas vezes, a causa desses problemas está em equipamentos mal configurados ou comprometidos por códigos maliciosos, que passam a ser utilizados em ataques a terceiros.
Os alvos desses ataques podem enfrentar indisponibilidade de serviços, danos à imagem, perdas financeiras e de credibilidade, além de dificuldades na continuidade de suas operações. Uma das principais razões para o sucesso dessas ações maliciosas é a falta de atenção às configurações de segurança dos equipamentos utilizados pelos operadores das redes, bem como às inúmeras vulnerabilidades presentes nesses dispositivos. Nesse sentido, manter o funcionamento adequado das redes é essencial para o negócio de operadoras de telecomunicações,

"O [Programa por uma Internet mais Segura] foi criado para apoiar a comunidade técnica da Internet na redução de DDoS originados em redes brasileiras, na diminuição de sequestro de prefixos, no vazamento de rotas e na falsificação de endereços de protocolo de Internet (Internet Protocol [IP]) de origem."

provedores de acesso à Internet, corporações e prestadores de serviços de dados. Diante desse cenário, o Comitê Gestor da Internet no Brasil (CGI.br) e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) lançaram no final de 2017, durante o IX Fórum 11[20], o Programa por uma Internet mais Segura, com o apoio do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel, Celular e Pessoal (Conexis Brasil Digital[21]), da Associação Brasileira de Internet (Abranet) e da Associação Brasileira de Provedores de Internet e Telecomunicações (Abrint), e em parceria com a Internet Society (organização internacional dedicada ao desenvolvimento de padrões e ao fomento de iniciativas educacionais e políticas públicas relacionadas à Internet). O programa foi criado para apoiar a comunidade técnica da Internet na redução de DDoS originados em redes brasileiras, na diminuição de sequestro de prefixos, no vazamento de rotas e na falsificação de endereços de protocolo de Internet (*Internet Protocol* [IP]) de origem. Além disso, busca reduzir vulnerabilidades e falhas de configuração nos elementos da rede, e aproximar as equipes responsáveis pela segurança e pela estabilidade da Internet, fortalecendo essa cultura de segurança entre os operadores.

Para alcançar esses objetivos, o NIC.br disponibiliza à comunidade técnica uma série de ações práticas (palestras, cursos, treinamentos e reuniões técnicas) que ajudam operadores e provedores a aprimorar seus processos de segurança e a melhorar a configuração de suas redes. O programa também mantém interação constante com associações de provedores e operadoras que apoiam suas iniciativas, ampliando o alcance das boas práticas e promovendo um ambiente de colaboração entre os diversos atores do ecossistema da Internet.

Com essas ações, o Programa por uma Internet mais segura contribui para reduzir incidentes, fortalecer a resiliência das redes e promover uma Internet mais estável, confiável e segura para todos.

P.S.I._ Como o programa evoluiu desde sua criação, quais foram os principais marcos desse percurso e como eles contribuíram para definir as atuais frentes de atuação, objetivos estratégicos e boas práticas para a promoção de uma Internet mais segura? E de que forma essas práticas são disseminadas e incentivadas entre os diferentes públicos e atores do ecossistema?

G.Z._ O Programa por uma Internet mais Segura é uma ação interna do NIC.br que envolve vários de seus departamentos técnicos: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Registro.br, Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (Ceptro.br) e IX.br (Brasil Internet Exchange). Cada área executa ações específicas que contribuem para o êxito do programa:

- **CERT.br:** Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso que define as diretrizes das melhores práticas de segurança que o Programa deve seguir. O CERT.br é também responsável pelas notificações de serviços expostos nas redes que podem ser abusados em ataques de reflexão e amplificação e por diversas estatísticas de segurança divulgadas.

[20] Saiba mais: https://forum.ix.br/2017/
[21] Anteriormente chamada de SindiTelebrasil.

- **Registro.br:** responsável pelas atividades de registro e manutenção dos nomes de domínios que usam o .br, também executa o serviço de distribuição de endereços IPv4 e IPv6 e de números de sistemas autônomos (*Autonomous System Number* [ASN]) no país. Além disso, abriga a coordenação do programa e possui um grupo de engenharia e operacional que desenvolve e mantém uma ferramenta de verificação da adoção de melhores práticas de segurança, operando a estrutura do sistema de nomes de domínios (*Domain Name System* [DNS]), da extensão de segurança do DNS (*Domain Name System Security Extensions* [DNSSEC]) e do repositório da infraestrutura de chave pública de recursos (*Resource Public Key Infrastructure* [RPKI]), importantes para a segurança de resolução de nomes e roteamento da Internet, entre outras atividades;
- **Ceptro.br:** responsável por iniciativas e projetos que apoiam ou aperfeiçoam a infraestrutura da Internet no Brasil, contribuindo para seu desenvolvimento. Entre as iniciativas do centro, está a disponibilização de ferramentas para medir a qualidade da Internet no país, a divulgação das melhores práticas operacionais e de segurança de redes por meio de cursos, treinamentos, palestras e eventos presenciais e *online*, além da disseminação do IPv6.br entre os operadores de redes e projetos, como a distribuição da hora certa (a hora legal brasileira), fundamental para a segurança das redes;
- **IX.br:** responsável pelos Pontos de Intercâmbio de Internet mantidos pelo NIC.br, implementa melhores práticas de segurança em seus 39 pontos de interconexão espalhados pelo país.

Nesse contexto, o programa desenvolve suas ações por meio das notificações dos serviços expostos realizados, pela inclusão de conteúdos de segurança em treinamentos e *workshops* presenciais em diferentes regiões do país, por conteúdos de segurança em treinamentos, *workshops* e *podcasts online*, pela realização de reuniões técnicas com operadores de redes sobre as melhores práticas de segurança que devem ser aplicadas em suas redes e, mais recentemente, por uma competição ou um desafio para a implementação de melhores práticas de segurança pelos operadores das redes.

A coordenação do programa produz estatísticas para acompanhamento das ações. No início, eram mais de 750.000 serviços expostos no país e no mês de abril de 2026, mesmo considerando o crescimento da rede no período e ataques que passaram a explorar novos serviços, a quantidade de serviços expostos está abaixo de 116.000, com tendência de queda, resultado das ações de notificação, treinamento e esclarecimentos sobre a importância da adoção das melhores práticas de segurança pelas redes.

O Programa por uma Internet mais Segura iniciou-se com as ações junto às grandes operadoras e, na sequência, com os médios e pequenos provedores de Internet, na adoção de configurações para evitar serviços expostos em suas redes. Na sequência, o programa passou a divulgar as melhores práticas de segurança recomendadas pelas Normas de Acordo Mútuo para Segurança de Roteamento (*Mutually Agreed Norms for Routing Security* [MANRS]), operacionalizado pela Global Cyber Alliance (GCA) e que visa a diminuição de problemas de segurança de roteamento das redes.

"No início, eram mais de 750.000 serviços expostos no país e no mês de abril de 2026, mesmo considerando o crescimento da rede no período e ataques que passaram a explorar novos serviços, a quantidade de serviços expostos está abaixo de 116.000, com tendência de queda, resultado das ações de notificação, treinamento e esclarecimentos sobre a importância da adoção das melhores práticas de segurança pelas redes."

"No final de 2021, foi desenvolvida a ferramenta Teste os Padrões (TOP), que visa verificar se a conexão do usuário final está seguindo as melhores práticas de segurança e se o *site* acessado ou serviço de *e-mail* utilizado está seguindo as melhores práticas de segurança mais importantes para os respectivos serviços."

Essas práticas contemplam a implementação de filtragem de anúncios de rede incorretos e de endereços de origem falsos, divulgação de pontos de contato que atendam notificações e tomem as ações necessárias com presteza e divulgação da política de roteamento das redes em bases de dados acessíveis e seguras, que auxiliam na filtragem de anúncios de rede. Hoje, mais de 320 redes do país são participantes do MANRS, e muitas outras implementaram as ações recomendadas.
No final de 2021, foi desenvolvida a ferramenta Teste os Padrões (TOP), que visa verificar se a conexão do usuário final está seguindo as melhores práticas de segurança e se o site acessado ou serviço de *e-mail* utilizado está seguindo as melhores práticas de segurança mais importantes para os respectivos serviços.
Em 2023, foi incorporada ao programa a divulgação da adoção das melhores práticas de segurança para resolução de nomes de domínios proposta pelo compartilhamento de conhecimento e instanciação de normas para DNS e segurança de nomes (*Knowledge-Sharing and Instantiating Norms for DNS and Naming Security* [KINDNS]), uma iniciativa da *Internet Corporation for Assigned Names and Numbers* (ICANN), fundamental para a segurança da navegação dos usuários na Internet.
Assim, as diversas melhores práticas de segurança foram sendo definidas ao longo do tempo pelas áreas técnicas do NIC.br em resposta ao avanço dos ataques e incidentes de segurança e das tecnologias desenvolvidas para proteção das redes.

P.S.I._ Sabemos que a colaboração é um elemento central nas iniciativas de segurança digital. Como ela se materializa no programa? De que maneira esse arranjo colaborativo contribui para fortalecer a confiança entre os atores e impulsionar avanços na segurança da Internet no Brasil?

G.Z._ A colaboração do Programa por uma Internet mais segura concretiza-se por meio de uma atuação transversal dentro do NIC.br, reunindo suas áreas técnicas e equipes de apoio — como Sistemas Web e Comunicação — em ações integradas e complementares. Essa articulação interna garante coerência, agilidade e consistência na implementação das iniciativas de segurança.
O programa também se apoia na colaboração das principais associações de provedores de Internet, entre elas a Abranet, a Abrint, a Associação Nacional das Empresas de Soluções de Internet e Telecomunicações (RedeTelesul), a Associação dos Provedores de Serviços e Informações da Internet (InternetSul), a Associação Brasileira dos Operadores de Telecomunicações e Provedores de Internet (Abramulti), a Associação Catarinense de Provedores de Internet (Apronet) e a Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas (Telcomp), ampliando seu alcance e fortalecendo o diálogo com operadores de redes em todo o país.
Além disso, instituições, como a Rede Nacional de Ensino e Pesquisa (RNP), e a comunidade técnica da Internet no Brasil contribuem ativamente, trazendo expertise, legitimidade e capilaridade às ações desenvolvidas. Esses apoios são essenciais para disseminar e implementar as melhores práticas de segurança, promovendo confiança entre os atores envolvidos e impulsionando avanços concretos na segurança da Internet no Brasil.

Entrevista II

Cooperação e confiança na gestão de incidentes de cibersegurança

Foto: Caleff

Olivier Caleff
Chair do Conselho Diretor do FIRST, especialista em CSIRT e resiliência Cibernética no CSIRT.FR, e auditor SIM3 na OpenCSIRT Foundation

Nesta entrevista, Olivier Caleff, *chair* do Conselho Diretor do FIRST[22], especialista em CSIRT e resiliência Cibernética no CSIRT.FR[23], e auditor SIM3 na OpenCSIRT Foundation[24], reflete sobre os desafios da gestão de incidentes de cibersegurança no contexto da transformação tecnológica, destacando a importância da cooperação entre Grupos de Resposta a Incidentes de Segurança (*Computer Security Incident Response Team* [CSIRTS]) e CERTs, a construção de confiança nas comunidades de cibersegurança e o papel do Modelo de Maturidade de Gestão de Incidentes de Segurança (*Security Incident Management Maturity Model* [SIM3]) no reforço das capacidades de resposta a incidentes.

Panorama Setorial da Internet (P.S.I.)_ Em sua opinião, quais são os principais desafios para a gestão de incidentes de cibersegurança em um contexto de transformação tecnológica? Em que medida esses desafios se modificaram ao longo das últimas décadas?

Olivier Caleff (O.C.)_ Em primeiro lugar, o principal desafio é a divergência entre o ritmo das mudanças e a capacidade de as organizações adaptarem recursos de segurança e resposta a incidentes. Novas tecnologias, novas arquiteturas e novos processos de negócios são frequentemente implementados mais rapidamente do que a governança, os planos de resposta a incidentes e os procedimentos conseguem evoluir.

Um segundo grande desafio é a visibilidade e o controle. Uma gestão eficaz de incidentes exige uma compreensão clara do ambiente que está sendo protegido: ativos (que rapidamente se traduzem em "superfície de ataque"), dependências, processos de negócios e fluxos de dados. Durante transformações em larga escala, os inventários, a documentação e os mapeamentos arquitetônicos costumam estar incompletos ou desatualizados; como resultado, a superfície de ataque pode se expandir, enquanto os defensores podem perder a visibilidade sobre ativos e interconexões críticas.

A transformação também aumenta a complexidade técnica. Serviços em nuvem, plataformas de *Software* como Serviço (*Software as a Service* [SaaS]), sistemas baseados em Inteligência Artificial (IA), ambientes conteinerizados e integração de terceiros introduzem novas tecnologias, componentes e vetores de ataque. Os CSIRTs, juntamente com as equipes de cibersegurança ou de defesa cibernética, podem ainda não ter experiência suficiente com essas tecnologias. Como consequência, muitas vezes os processos de qualificação, avaliação de riscos e validação de segurança têm dificuldade para acompanhar o ritmo das mudanças.

[22] Saiba mais: https://first.org/
[23] Saiba mais: https://csirt.fr/
[24] Saiba mais: https://opencsirt.org/

"Os desafios enfrentados pelas equipes de gestão de incidentes de cibersegurança não mudaram fundamentalmente em sua natureza: as organizações ainda precisam de recursos de visibilidade, detecção, resposta, comunicação e recuperação. O que mudou drasticamente nas últimas décadas foi a escala, a complexidade e a importância crítica desses desafios para os negócios."

Outro desafio significativo é de natureza organizacional. A resposta a incidentes depende de uma forte colaboração entre as equipes técnicas, de segurança, operacionais e de negócios. No entanto, a cibersegurança é, por vezes, percebida como uma restrição em vez de um facilitador, o que pode dificultar a cooperação e atrasar o estabelecimento de canais eficazes de comunicação e escalonamento. Ao mesmo tempo, funções, responsabilidades e autoridade para a tomada de decisões nem sempre são claramente definidas durante programas de transformação, criando incerteza quando ocorrem incidentes.

Os fatores humanos não devem ser subestimados. Os Centros de Operações de Segurança (*Security Operations Centers* [SOC]) e os CSIRTs frequentemente enfrentam fadiga de alertas, carga de trabalho crescente e escassez de profissionais qualificados. Quando a capacitação e a transferência de conhecimento ficam para trás em relação às mudanças tecnológicas, as equipes podem se sentir sobrecarregadas e menos capazes de responder de modo eficaz a incidentes envolvendo tecnologias desconhecidas.

Por fim, o cenário de ameaças tem evoluído em conjunto com a transformação tecnológica. Os adversários estão cada vez mais utilizando automação e IA para acelerar o reconhecimento, as campanhas de *phishing*, a descoberta de vulnerabilidades e a execução de ataques. Esse cenário levanta questões sobre a velocidade e a sofisticação das ameaças, enquanto os defensores já lidam com um ambiente em rápida transformação.

Para enfrentar esses desafios, as organizações devem investir em gestão de ativos robusta, banco de dados de gerenciamento de configuração (*Configuration Management Database* [CMDB]), lista de materiais de *software* (*Software Bill of Materials* [SBOM]), capacitação contínua, engajamento das partes interessadas e *frameworks* de governança que integrem a cibersegurança aos programas de transformação desde o início do processo. Embora não exista uma solução única, muitas áreas são abrangidas por modelos de maturidade, como o SIM3 da Open CSIRT Foundation (OCF).

Os desafios enfrentados pelas equipes de gestão de incidentes de cibersegurança não mudaram fundamentalmente em sua natureza: as organizações ainda precisam de recursos de visibilidade, detecção, resposta, comunicação e recuperação. O que mudou drasticamente nas últimas décadas foi a escala, a complexidade e a importância crítica desses desafios para os negócios.

Vamos agora destacar cinco evoluções principais: arquitetura, escala, complexidade, velocidade e impacto nos negócios.

A primeira evolução é a arquitetura, que vai desde ecossistemas centralizados até ambientes distribuídos. Quando iniciei minha carreira, há quarenta anos, a maior parte dos ativos estava concentrada em ambientes centralizados, como *mainframes* e redes privadas. A resposta a incidentes tinha como foco um perímetro relativamente bem definido e em um número muito limitado de sistemas críticos. Com o tempo, as organizações adotaram computação distribuída, arquiteturas cliente-servidor, Internet, serviços em nuvem, plataformas SaaS, dispositivos móveis, trabalho remoto e cadeias de suprimentos interconectadas. Como resultado, os responsáveis pela resposta a incidentes não investigam mais um ambiente isolado, mas um ecossistema que abrange múltiplos fornecedores, tecnologias e domínios administrativos. Uma das consequências é que a visibilidade se tornou um grande desafio. Registros críticos, telemetria e evidências forenses podem ser propriedade de terceiros, como na nuvem, criando dependências que não existiam nas gerações anteriores de tecnologia da informação (TI).

A segunda evolução é a escala, que varia de centenas a milhões de eventos. O número de ativos, usuários, aplicativos, interfaces de programação de aplicativos (*Application Programming Interface* [API]), contêineres, serviços em nuvem e dispositivos conectados aumentou exponencialmente. Com a expansão das superfícies de ataque, o volume de eventos de segurança também explodiu: o que antes podia ser investigado manualmente, com o uso de comandos como "grep", "awk" e similares do Unix, agora exige registro centralizado, poder computacional para plataformas de correlação, plataformas de gerenciamento de informações e eventos de segurança (*Security Information and Event Management* [SIEM]), inteligência de ameaças e análises. Assim, a gestão de incidentes evoluiu da análise de eventos isolados para a operação em larga escala.

A terceira evolução é a complexidade, que abrange desde sistemas conhecidos até dependências interconectadas. Atualmente, os ambientes contêm inúmeras camadas de abstração e dependências. As organizações dependem cada vez mais de componentes de *software*, bibliotecas de código aberto, serviços nativos da nuvem, API de terceiros e cadeias de suprimentos que nem sempre são plenamente compreendidas. A identidade tornou-se particularmente crítica. Embora a segurança de rede já tenha sido o foco principal, as investigações de incidentes modernas frequentemente giram em torno de sistemas de identidade, acesso privilegiado, *tokens* de sessão, autenticação federada e permissões na nuvem. A Gestão de Identidade e Acesso (*Identity and Access Management* [IAM]) está atualmente entre as fontes de evidência mais valiosas em uma investigação, assim como *logging* e *Domain Name System* (DNS) são há décadas. Essa complexidade torna a análise da causa raiz, a contenção e a recuperação significativamente mais difíceis do que nas décadas anteriores.

A quarta evolução é a velocidade, que passa de dias e semanas para minutos e horas. Talvez a mudança mais drástica seja a velocidade com que os incidentes se desenrolam. Os agentes maliciosos recorrem cada vez mais à automação, aos *frameworks* de ataque industrializados e às técnicas assistidas por IA. As vulnerabilidades são rapidamente exploradas após sua divulgação e os prazos entre a invasão e a exfiltração de dados continuam a diminuir. Casos em que os adversários passam da invasão inicial ao furto de dados em questão de horas, ou até menos, já não são exceção. Os processos manuais de resposta habituais costumam ser muito lentos para acompanhar um ritmo tão acelerado. A gestão de incidentes tende a depender cada vez mais da detecção em tempo real, da automação e da orquestração, bem como da tomada de decisões rápidas.

Por fim, a quinta evolução é o impacto nos negócios, que vai de interrupções técnicas a riscos empresariais. Historicamente, os incidentes de cibersegurança eram frequentemente considerados problemas técnicos ou operacionais. Hoje, os incidentes afetam diretamente a receita, as operações, a conformidade regulatória, a exposição legal, a reputação e a confiança do cliente a longo prazo. A convergência entre TI e tecnologia operacional, o crescimento de modelos de negócios digitais e as regulamentações cada vez mais rigorosas elevaram a resiliência cibernética a uma preocupação de nível diretivo. A gestão de incidentes atual envolve executivos, equipes jurídicas, departamentos de comunicação, órgãos reguladores, seguradoras e líderes empresariais, além de equipes técnicas.

Nas últimas décadas, tenho observado a gestão de incidentes de cibersegurança evoluir de um domínio focado principalmente na proteção de sistemas de TI por meio de uma abordagem puramente técnica para uma capacidade estratégica de negócios voltada à resiliência organizacional.

"Historicamente, os incidentes de cibersegurança eram frequentemente considerados problemas técnicos ou operacionais. Hoje, os incidentes afetam diretamente a receita, as operações, a conformidade regulatória, a exposição legal, a reputação e a confiança do cliente a longo prazo."

"O modelo de cooperação CSIRT-CERT é um *framework* colaborativo de cibersegurança construído sobre a confiança, o compartilhamento de informações e a resposta coordenada a incidentes. Embora os CSIRTs e CERTs sejam os principais atores, elas operam em conjunto com entidades complementares (...). A base do modelo é a confiança."

O objetivo principal permanece o mesmo: prevenir, detectar, conter, erradicar e recuperar. Infelizmente, o ambiente tornou-se mais distribuído, maior, mais complexo e mais rápido, impactando diretamente os negócios. Como resultado, o sucesso não é mais medido apenas pela capacidade de prevenir incidentes, mas também pela rapidez e pela eficácia com que uma organização consegue responder, se recuperar e manter a continuidade dos negócios. A recuperação e a resiliência tornaram-se tão importantes quanto a prevenção. Os CSIRTs também têm, definitivamente, um papel a desempenhar, participando dessas atividades.

P.S.I._ Como funciona o modelo de cooperação CSIRT-CERT? Além disso, de que forma os mecanismos de cooperação existentes podem aprimorar a prevenção e a gestão de incidentes cibernéticos?

O.C._ O modelo de cooperação CSIRT-CERT é um *framework* colaborativo de cibersegurança construído sobre a confiança, o compartilhamento de informações e a resposta coordenada a incidentes. Embora os CSIRTs e CERTs sejam os principais atores, eles operam em conjunto com entidades complementares, como as Times de Resposta a Incidentes de Segurança de Produtos (*Product Security Incident Response Team* [PSIRT]), os Centros de Análise e Compartilhamento de Informações (*Information Sharing and Analysis Centers* [ISAC]), os SOC e as equipes de Inteligência de Ameaças Cibernéticas (*Cyber Threat Intelligence* [CTI]). A base do modelo é a confiança. As equipes de segurança organizam-se em comunidades com base em interesses comuns, como geografia, idioma, setor ou missão. Algumas comunidades estão abertas a membros qualificados, enquanto outras são restritas a equipes governamentais, nacionais ou credenciadas. Essas comunidades fomentam relações de confiança por meio de conferências, grupos de trabalho, sessões de treinamento, exercícios e colaboração diária.
Em nível global, organizações, como o FIRST (fundado em 1990), fornecem um *framework* para a cooperação internacional e, atualmente, reúnem equipes de resposta a incidentes de mais de 110 países. Organizações regionais, como a Task Force CSIRT (TF-CSIRT)[25] (na Europa), a Africa Computer Security Incident Response Teams (AfricaCERT)[26] e a TrustBroker África (TBA)[27] (na África), fortalecem a cooperação em suas respectivas regiões, e muitos países também estabelecem associações nacionais de CSIRT, como a InterCERT France[28] (na França), o Fórum Brasileiro de CSIRTs[29] (no Brasi) e a Nippon CSIRT Association (NCA)[30] (no Japão). O aspecto operacional da cooperação depende de regras de governança acordadas, terminologia comum e mecanismos padronizados de compartilhamento. As informações podem ser trocadas manualmente ou por meio de plataformas automatizadas, como a MISP[31]. Para garantir que as informações compartilhadas sejam tratadas adequadamente, as comunidades utilizam padrões e *frameworks* estabelecidos, incluindo:

[25] Saiba mais: https://tf-csirt.org/
[26] Saiba mais: https://www.africacert.org/
[27] Saiba mais: https://www.trustbroker.africa/
[28] Saiba mais: https://intercert-france.fr/
[29] Saiba mais: https://forum.cert.br
[30] Saiba mais: https://www.nca.gr.jp/en/index.html
[31] Saiba mais: https://www.misp-project.org/

- o *Traffic Light Protocol* (TLP)[32] e o *Permissible Actions Protocol* (PAP)[33] para o tratamento e a disseminação de informações;
- a *Structured Threat Information Expression* (STIX) e a *Trusted Automated Exchange of Intelligence Information* (TAXII) para troca estruturada e automatizada de informações de inteligência sobre ameaças; e
- o *Common Vulnerability Scoring System* (CVSS)[34] e o *Exploit Prediction Scoring System* (EPSS)[35] para avaliação e priorização de vulnerabilidades.

Esses mecanismos permitem que as equipes compartilhem rapidamente indicadores e informações, incluindo indicadores de ataque futuro (*Indicators of Future Attack* [IOFA]), indicadores de ataque (*Indicators of Attack* [IOA]), indicadores de comportamento (*Indicators of Behavior* [IOB]), indicadores de comprometimento (*Indicators of Compromise* [IOC]) e táticas, técnicas e procedimentos (*Tactics, Techniques, and Procedures* [TTPs]) do adversário.

Quando os incidentes ultrapassam fronteiras organizacionais ou nacionais, as relações de confiança estabelecidas por meio dessas comunidades permitem a comunicação direta e as atividades de resposta coordenadas. Em casos de grandes incidentes cibernéticos, campanhas em larga escala ou vulnerabilidades críticas, várias equipes podem formar forças-tarefa *ad hoc* para coordenar os esforços de análise, mitigação, divulgação e comunicação.

Para concluir, gostaria de insistir no ponto de que o modelo de cooperação CSIRT-CERT é global e baseado em confiança, padrões e colaboração, constituindo, assim, uma tríade. Isso facilita a troca segura de informações acionáveis[36], melhora a consciência situacional coletiva e permite respostas coordenadas a ameaças e incidentes de cibersegurança.

Os mecanismos de cooperação existentes melhoram significativamente tanto a prevenção quanto a gestão de incidentes cibernéticos, permitindo que as organizações antecipem ameaças, coordenem respostas e fortaleçam continuamente a resiliência coletiva.

O primeiro benefício é a antecipação. A prevenção eficaz depende da visibilidade das ameaças emergentes em tempo hábil. Por meio de redes de cooperação confiáveis, é possível que CSIRTs, CERTs, ISAC, equipes de CTI e outras partes interessadas em segurança troquem rapidamente informações sobre ameaças, vulnerabilidades, indicadores, TTPs de adversários e lições aprendidas com incidentes. A detecção antecipada permite que as organizações aumentem seu nível de alerta, fortaleçam o monitoramento, refinem suas capacidades de detecção, implementem estratégias de mitigação, corrijam sistemas vulneráveis e preparem planos de resposta antes de um ataque se materializar. Em muitos casos, também possibilita atividades proativas, como a busca de ameaças e a realização de avaliações de risco direcionadas.

"A prevenção eficaz depende da visibilidade das ameaças emergentes em tempo hábil. Por meio de redes de cooperação confiáveis, é possível que CSIRTs, CERTs, ISAC, equipes de CTI e outras partes interessadas em segurança troquem rapidamente informações sobre ameaças, vulnerabilidades, indicadores, TTPs de adversários e lições aprendidas com incidentes."

[32] Saiba mais: https://www.first.org/tlp/
[33] Saiba mais: https://www.cert.ssi.gouv.fr/csirt/sharing-policy/
[34] Saiba mais: https://www.first.org/cvss/v4.0/
[35] Saiba mais: https://www.first.org/epss/
[36] Consulte o documento da European Union Agency for Cybersecurity (ENISA), de 2015, intitulado *Informações acionáveis para resposta a incidentes de segurança* e disponível em: https://www.enisa.europa.eu/publications/actionable-information-for-security

"Embora nem todos os incidentes exijam intervenção judicial, a colaboração entre as equipes de resposta a incidentes e as autoridades policiais pode ajudar a compreender melhor o contexto de determinados tipos de atividades maliciosas, apoiar investigações, facilitar a preservação de provas e, não menos importante, contribuir para a desarticulação de infraestruturas criminosas."

A cooperação também melhora a consciência situacional. Organizações individuais geralmente observam apenas uma pequena parte do cenário de ameaças, enquanto uma comunidade de parceiros confiáveis pode identificar coletivamente campanhas de ataque mais amplas, tendências emergentes e riscos sistêmicos. Ao correlacionar observações de múltiplos setores, regiões ou países, as comunidades podem detectar ameaças mais cedo e compreender seu impacto potencial com maior precisão.

Ademais, os mecanismos de cooperação aceleram a resposta e a recuperação. Canais de comunicação confiáveis permitem que as equipes troquem rapidamente informações técnicas, indicadores de comprometimento, medidas corretivas e orientações operacionais. Essas ações reduzem a duplicação de esforços, melhoram a tomada de decisões e possibilitam ações coordenadas entre as organizações afetadas. Durante grandes crises cibernéticas ou vulnerabilidades em larga escala, as comunidades podem estabelecer forças-tarefa dedicadas para sincronizar as atividades de análise, mitigação, divulgação e comunicação.

A cooperação com as agências de aplicação da lei é outro aspecto importante. Embora nem todos os incidentes exijam intervenção judicial, a colaboração entre as equipes de resposta a incidentes e as autoridades policiais pode ajudar a compreender melhor o contexto de determinados tipos de atividades maliciosas, apoiar investigações, facilitar a preservação de provas e, não menos importante, contribuir para a desarticulação de infraestruturas criminosas. Relações sólidas estabelecidas antes da ocorrência de um incidente ou crise melhoram significativamente a eficácia dessa colaboração; por isso, é importante participar de eventos e conferências organizados pela comunidade.

O nível de preparação também é reforçado por meio de exercícios conjuntos, ambientes de simulação cibernética (*cyber-ranges*), exercícios *tabletop* (*tabletop simulations*) e capacitações em gestão de crises. Essas atividades permitem que as organizações testem procedimentos, identifiquem pontos fracos, validem canais de comunicação e melhorem a coordenação entre as partes interessadas. Igualmente importante: elas criam relações pessoais e confiança entre os profissionais, o que muitas vezes se revela inestimável durante incidentes reais.

Por fim, os mecanismos de cooperação contribuem para o fortalecimento da comunidade e o desenvolvimento de capacidades a longo prazo. Comunidades CSIRT consolidadas investem esforços significativos no compartilhamento de conhecimento, na publicação de melhores práticas, na orientação de novas equipes e no desenvolvimento de programas de capacitação. Isso contribui para o aumento da maturidade geral do ecossistema e do número de defensores capacitados disponíveis para responder a ameaças futuras. Iniciativas como o *Community and Capacity Building Program* (CCB)[37], o Programa CORE[38] e o Programa de Bolsas[39] do FIRST, bem como o programa de incubação do InterCERT-France[40], demonstram por que investir em pessoas e organizações hoje fortalece a resiliência coletiva da comunidade de cibersegurança futuramente.

[37] Saiba mais: https://www.first.org/global/ccb-initiatives/
[38] Saiba mais: https://www.first.org/global/core/
[39] Saiba mais: https://www.first.org/global/fellowship/
[40] Saiba mais: https://www.intercert-france.fr/incubateur-intercert-france/

Lembre-se desses cinco mecanismos de cooperação: antecipação (novamente), consciência situacional, preparação, resposta coordenada e capacidade da comunidade. Durante quatro décadas, os fundamentos da gestão de incidentes basearam-se em esforços coletivos, na crença de que os profissionais de segurança alcançam maior eficácia quando colaboram e compartilham informações. E, adivinhe só: os agentes maliciosos também fazem isso há pelo menos tanto tempo quanto nós. Eles estão cada vez mais colaborando e trocando informações entre si. A cooperação não é medida pelo volume de informações compartilhadas, mas pela capacidade de transformar informações compartilhadas em medidas práticas e em decisões operacionais coordenadas. Qualidade, portanto, é melhor que quantidade.

P.S.I._ Quais são os valores mínimos compartilhados pelas comunidades CSIRT globais e regionais, e qual o papel desempenhado pela comunidade no fomento da confiança entre os participantes?

O.C._ As comunidades CSIRT globais e regionais são geralmente construídas em torno de três valores fundamentais: confiança, cooperação e compartilhamento seguro de informações.
Confiança é a base de todo o ecossistema. Espera-se que os membros lidem com as informações compartilhadas de forma responsável, respeitem os requisitos de confidencialidade e cumpram as regras de interação da comunidade. Quebras de confiança são levadas a sério e podem, em última instância, resultar na exclusão da comunidade. Além da confidencialidade, espera-se que os membros demonstrem profissionalismo, integridade e conduta ética em suas atividades de resposta a incidentes, práticas operacionais e comunicações.
Cooperação é o mecanismo pelo qual a comunidade gera valor. Abrange o compartilhamento de conhecimento, experiência, inteligência de ameaças, lições aprendidas, melhores práticas e capacidades técnicas. A cooperação eficaz depende da comunicação oportuna, da capacidade de responder aos pedidos de assistência e da habilidade de coordenar atividades além das fronteiras organizacionais e nacionais. Desse modo, a precisão, a confiabilidade e a relevância das informações trocadas são cruciais; em última análise, o objetivo é fornecer informações acionáveis que possibilitem uma tomada de decisões embasada e uma resposta eficaz.
Compartilhamento seguro de informações é a base tanto da confiança quanto da cooperação. Independentemente de a troca de informações ser feita verbalmente, por meio de comunicações escritas ou de plataformas automatizadas, como o MISP, espera-se que os membros sigam as regras de governança e os procedimentos de tratamento de informações acordados. Embora as tecnologias, as plataformas e os canais de comunicação continuem a evoluir, os princípios subjacentes permanecem consistentes: garantir que a informação correta chegue às pessoas certas, no momento certo, com o nível adequado de proteção e os devidos controles de disseminação.

"As comunidades CSIRT globais e regionais são geralmente construídas em torno de três valores fundamentais: confiança, cooperação e compartilhamento seguro de informações. Confiança é a base de todo o ecossistema."

"Uma responsabilidade fundamental de qualquer comunidade CSIRT é facilitar a resposta coordenada a incidentes e a gestão de crises. (...) Não se perde tempo valioso estabelecendo legitimidade, negociando canais de comunicação ou validando relacionamentos, visto que essas bases já foram construídas por meio do engajamento comunitário."

As comunidades CSIRT desempenham um papel central no estabelecimento, no fortalecimento e na manutenção da confiança entre seus membros por meio de uma combinação de governança, práticas operacionais e relações interpessoais. No âmbito da governança, as comunidades definem códigos de conduta, requisitos de adesão, padrões operacionais e *frameworks* de compartilhamento de informações. As comunidades estabelecem regras comuns para o tratamento de informações sensíveis, geralmente baseadas em protocolos como TLP e, em alguns casos, em PAP. Essas regras compartilhadas criam um ambiente previsível e confiável no qual os membros podem trocar informações com segurança.

Além disso, as comunidades também investem muito na construção de relações. Conferências, *workshops*, grupos de trabalho, sessões de treinamento, competições de *capture-the-flag* (CTF), exercícios teóricos e simulações de crises cibernéticas oferecem oportunidades valiosas para que os participantes interajam regularmente e desenvolvam relacionamentos tanto profissionais quanto pessoais. Essas interações ajudam a transformar a confiança organizacional em confiança humana, o que muitas vezes se torna um fator decisivo durante incidentes graves.

Algumas comunidades vão ainda mais longe, implementando mecanismos de revisão por pares, acreditação, certificação ou mentoria. Essas iniciativas permitem que as equipes compreendam melhor as capacidades, os modelos operacionais e as limitações umas das outras, além de aumentar a credibilidade e a confiança na comunidade. A confiança surge mais naturalmente quando as organizações trabalham juntas, analisam as práticas umas das outras e demonstram seu compromisso com padrões comuns.

Uma responsabilidade fundamental de qualquer comunidade CSIRT é facilitar a resposta coordenada a incidentes e a gestão de crises. Quando ocorre um incidente significativo, a existência de confiança e de canais de comunicação preestabelecidos permite que as equipes cooperem de forma imediata e eficaz. Não se perde tempo valioso estabelecendo legitimidade, negociando canais de comunicação ou validando relacionamentos, visto que essas bases já foram construídas por meio do engajamento comunitário.

Por fim, uma das contribuições mais impactantes das comunidades CSIRT é o desenvolvimento de capacidades por meio de programas de mentoria, bolsas de estudo e compartilhamento de conhecimento. Times e profissionais experientes apoiam equipes mais novas ou em desenvolvimento, compartilhando conhecimento especializado, melhores práticas, lições aprendidas e experiência operacional. Isso acelera o desenvolvimento de capacidades, ajuda a evitar erros comuns e fortalece a resiliência geral do ecossistema.

Tendo participado e apoiado iniciativas desse tipo por duas décadas, tanto em contextos nacionais quanto internacionais, considero a mentoria um dos aspectos mais valiosos de nossa comunidade. Todos os envolvidos se beneficiam: os mentorados ganham conhecimento, confiança e apoio, enquanto o mentor amplia seus horizontes, aprimora as próprias práticas e continua aprendendo com essa experiência.

P.S.I._ Como você descreveria o SIM3 e quais são os principais desafios atualmente identificados para os CSIRTs com base nesse modelo?

O.C._ O SIM3 é o *framework* de avaliação de maturidade mais amplamente adotado na comunidade internacional de CSIRT, utilizado por organizações e comunidades, como a TF-CSIRT, o FIRST e a CSIRTAmericas Network[41], cujos princípios têm sido aplicados além dos CSIRTs, abrangendo equipes operacionais relacionadas, como PSIRT, SOC e ISAC. Ele fornece um método estruturado, objetivo e mensurável para avaliar a maturidade da capacidade de resposta a incidentes.

O SIM3 pode ser usado para autoavaliação, desenvolvimento de capacidades, auditorias externas, programas de certificação e definição de roteiros de melhoria. Em vez de avaliar apenas a expertise técnica, ele também verifica se as capacidades de uma equipe estão devidamente organizadas, documentadas, formalizadas, gerenciadas, mensuradas e continuamente aprimoradas.

Um equívoco comum é considerar que o SIM3 mede o quão tecnicamente avançado é um CSIRT; entretanto, ele não foi concebido para medir a capacidade técnica de uma equipe ou estabelecer um suposto grau de excelência técnica. O SIM3 mede a maturidade operacional e a sustentabilidade. Uma equipe altamente qualificada pode apresentar um desempenho ruim se seu objetivo não for claro, os processos não estiverem documentados, o conhecimento estiver concentrado em poucos indivíduos ou os mecanismos de governança forem fracos. Uma equipe madura é aquela que consegue prestar serviços de forma consistente, independentemente da rotatividade de pessoal e das mudanças organizacionais, e que pode confiar em processos e procedimentos escritos, validados e bem compreendidos.

O modelo avalia 45 parâmetros organizados em quatro domínios:

- **Organização (O):** 11 parâmetros que abrangem governança, mandato, público atendido, definição de serviços, apoio à gestão, posicionamento estratégico, etc.;
- **Humano (H):** 7 parâmetros que abrangem recursos humanos, competências, capacitação, resiliência, planejamento de sucessão, desenvolvimento de equipe, etc.;
- **Ferramentas (T, do inglês *tools*):** 10 parâmetros que abrangem capacidades técnicas, infraestrutura, monitoramento, automação, tecnologias de suporte, etc.;
- **Processos (P):** 17 parâmetros que abrangem fluxos de trabalho operacionais, procedimentos de tratamento de incidentes, mecanismos de escalonamento, coordenação, comunicação, garantia da qualidade, melhoria contínua, etc.

Como auditor certificado do SIM3, realizando avaliações e auditorias há quase uma década, descobri que o maior valor do modelo não é a certificação em si, mas sua capacidade de orientar a melhoria. O SIM3 fornece uma linguagem comum para discutir maturidade, identificar lacunas, priorizar investimentos e construir roteiros realistas. É igualmente valioso tanto para projetar um novo CSIRT "do zero" quanto para ajudar uma equipe já estabelecida a implementar uma abordagem de melhoria contínua ou de gestão da qualidade. O modelo também facilita a criação de objetivos mensuráveis, indicadores e indicadores-chave de desempenho (*Key Performance Indicator* [KPI]), os quais podem ser acompanhados ao longo do tempo.

"O SIM3 mede a maturidade operacional e a sustentabilidade. Uma equipe altamente qualificada pode apresentar um desempenho ruim se seu objetivo não for claro, os processos não estiverem documentados, o conhecimento estiver concentrado em poucos indivíduos ou os mecanismos de governança forem fracos."

[41] Saiba mais: https://csirtamericas.org/

"Do ponto de vista organizacional, o desafio mais comum continua sendo a falta de um objetivo e de um *framework* de governança claramente definidos. Muitas equipes ainda operam com autoridade ambígua, patrocínio insuficiente da alta administração, definições pouco claras de partes interessadas ou responsabilidades sobrepostas a outras funções de segurança."

Um dos pontos fortes do SIM3 é o equilíbrio entre essas quatro dimensões. A experiência demonstra que as fragilidades em uma área muitas vezes limitam o amadurecimento nas demais. Permita-me dar três exemplos rápidos:

- analistas altamente qualificados têm dificuldades para operar de forma eficaz sem governança clara, atribuições bem definidas e apoio organizacional na "O";
- as fases iniciais do tratamento de incidentes são lentas ou ineficientes se o mapeamento do ambiente de TI ou tecnologia operacional (TO) do público atendido for deficiente e as relações com as partes interessadas não estiverem bem estabelecidas ("O", "T" e "P");
- investir em ferramentas avançadas não trará os benefícios esperados se "P" não for bem definido, visto que a tecnologia costuma ser mais fácil de adquirir do que a maturidade operacional sustentável.

Diversas linhas de base do SIM3 foram desenvolvidas para atender a contextos operacionais específicos. Além da base de certificação original estabelecida pela TF-CSIRT, perfis personalizados foram definidos para CSIRTs nacionais e governamentais na Rede de CSIRTs da ENISA[42] (para o FIRST) e, mais recentemente, na CSIRTAmericas Network. Essas linhas de base ajudam a garantir que as expectativas de maturidade estejam alinhadas às missões e responsabilidades das equipes avaliadas.

Em relação aos principais desafios identificados por meio das avaliações SIM3, embora as conclusões específicas variem entre as organizações, vários temas recorrentes emergem.

- Do ponto de vista organizacional, o desafio mais comum continua sendo a falta de um objetivo e de um *framework* de governança claramente definidos. Muitas equipes ainda operam com autoridade ambígua, patrocínio insuficiente da alta administração, definições pouco claras de partes interessadas ou responsabilidades sobrepostas a outras funções de segurança. Essas questões representam grandes obstáculos na coordenação de incidentes e situações de crise.
- Do ponto de vista humano, muitas equipes continuam altamente dependentes de um pequeno número de especialistas-chave. Essa concentração de conhecimento gera riscos operacionais, limita a escalabilidade, aumenta o estresse e pode levar à exaustão profissional. Ao mesmo tempo, a rápida evolução tecnológica, incluindo ambientes nativos da nuvem, tecnologias relacionadas à IA, sistemas industriais e agentes de ameaça cada vez mais sofisticados, continua a criar lacunas de competências difíceis de preencher.
- Do ponto de vista das ferramentas, as organizações frequentemente enfrentam dificuldades de visibilidade e integração. As infraestruturas modernas estão cada vez mais distribuídas entre ambientes locais, em nuvem, SaaS e de terceiros, o que dificulta o monitoramento abrangente. Além disso, muitas equipes ainda dependem de conjuntos de ferramentas fragmentados que exigem processamento manual significativo, apesar dos avanços em orquestração e automação.

[42] Saiba mais: https://csirtsnetwork.eu/

- Do ponto de vista dos processos, as fragilidades recorrentes incluem procedimentos de escalonamento desatualizados, diretórios de contatos incompletos, coordenação insuficiente com as partes interessadas externas, cobertura limitada de incidentes na cadeia de suprimentos e de terceiros, e atividades de lições aprendidas, realizadas de forma inconsistente. Muitas organizações também têm dificuldade em manter os manuais de procedimentos (*playbooks*) e de operação (*runbooks*) atualizados no mesmo ritmo da realidade operacional, o que resulta em procedimentos que já não refletem com precisão a forma como os incidentes são tratados.

Em todos os quatro domínios, dois grandes desafios aparecem de forma consistente. O primeiro é a lacuna entre os processos documentados e as práticas operacionais reais. O segundo é manter a melhoria contínua ao longo do tempo. Algumas equipes conseguem estabelecer processos e documentação durante a fase inicial de desenvolvimento, mas têm dificuldades em mantê-los atualizados à medida que seu ambiente, tecnologias e missão evoluem.

Logo, o SIM3 não é apenas um *framework* de avaliação ou certificação cujo único objetivo é a "conformidade": ele é uma ferramenta de gestão e melhoria que ajuda os CSIRTs a desenvolverem capacidades operacionais sustentáveis.

Os desafios mais frequentemente identificados por meio das avaliações SIM3 raramente são de natureza técnica; geralmente são transversais e estão relacionados à governança, aos indivíduos, à disciplina de processos, à gestão do conhecimento e à capacidade de adaptação contínua a um cenário de ameaças em constante evolução.

Em conclusão, o SIM3 pode ser usado como uma ferramenta de diagnóstico para destacar problemas, e como um recurso de suporte à construção ou melhoria, permitindo o aumento da maturidade. Nesse sentido, o SIM3 vai além de uma certificação do tipo "aprovado ou reprovado": ele pode auxiliar no crescimento da equipe e da capacidade de se adaptar às transformações tecnológicas.

"Em conclusão, o SIM3 pode ser usado como uma ferramenta de diagnóstico para destacar problemas, e como um recurso de suporte à construção ou melhoria, permitindo o aumento da maturidade. Nesse sentido, o SIM3 vai além de uma certificação do tipo "aprovado ou reprovado": ele pode auxiliar no crescimento da equipe e da capacidade de se adaptar às transformações tecnológicas."

Relatório de Domínios

A dinâmica dos registros de domínios no Brasil e no mundo

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), monitora mensalmente o número de nomes de domínios de topo de código de país (*country code Top-Level Domain* [ccTLD]) registrados entre os países que compõem a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o G20[43]. Considerados os membros de ambos os blocos, as 20 nações com maior atividade somam mais de 98,40 milhões de registros. Em maio de 2026, os domínios registrados sob .de (Alemanha) chegaram a 17,96 milhões. Em seguida, aparecem China (.cn), Reino Unido (.uk) e Rússia (.ru), com, respectivamente, 12,12 milhões, 8,98 milhões e 6,11 milhões de registros. O Brasil teve 5,75 milhões de registros sob .br, ocupando a sexta posição na lista, como mostra a Tabela 1[44].

[43] Grupo composto pelas 19 maiores economias mundiais e a União Europeia. Saiba mais: https://g20.org/

[44] A tabela apresenta a contagem de domínios ccTLD segundo as fontes indicadas. Os valores correspondem ao registro publicado por cada país, tomando como base os membros da OCDE e do G20. Para países que não disponibilizam uma estatística oficial fornecida pela autoridade de registro de nomes de domínios, a contagem foi obtida em: https://research.domaintools.com/statistics/tld-counts. É importante destacar que há variação no período de referência, embora seja sempre o mais atualizado para cada localidade. A análise comparativa de desempenho de nomes de domínios deve considerar ainda os diferentes modelos de gestão de registros ccTLD. Assim, ao observar o *ranking, é preciso atentar para a diversidade de modelos de negócio existentes.*

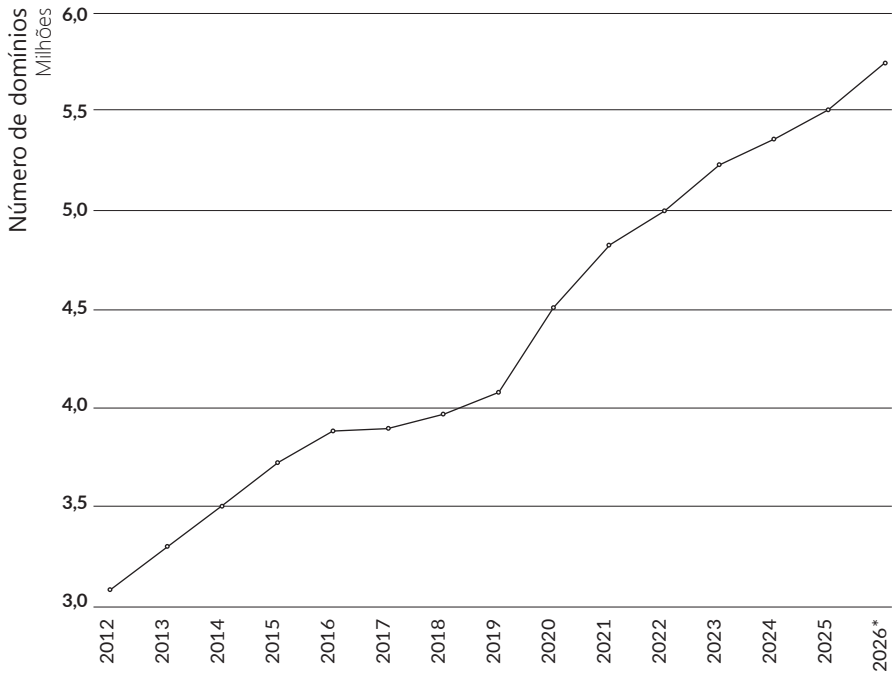
Tabela 1 – TOTAL DE REGISTROS DE NOMES DE DOMÍNIOS ENTRE OS PAÍSES DA OCDE E DO G20

Posição	País	Número de domínios	Data de referência	Fonte (*website*)
1	Alemanha (.de)	17.968.945	01/06/2026	https://www.denic.de
2	China (.cn)	12.125.420	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
3	Reino Unido (.uk)	8.986.855	30/04/2026	https://nominet.uk/reports-and-statistics/
4	Rússia (.ru)	6.114.524	01/06/2026	https://cctld.ru
5	Países Baixos (.nl)	6.081.616	31/05/2026	https://stats.sidnlabs.nl/en/registration.html
6	**Brasil (.br)**	**5.755.795**	**31/05/2026**	**https://registro.br/dominio/estatisticas/**
7	França (.fr)	4.466.907	30/05/2026	https://www.afnic.fr/en/observatory-and-resources/statistics/
8	Austrália (.au)	4.368.740	01/06/2026	https://www.auda.org.au/
9	União Europeia (.eu)	3.683.208	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
10	Itália (.it)	3.592.180	01/06/2026	http://nic.it
11	Canadá (.ca)	3.575.127	01/06/2026	https://www.cira.ca
12	Índia (.in)	3.419.117	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
13	Colômbia (.co)	3.151.207	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
14	Suíça (.ch)	2.614.611	15/05/2026	https://www.nic.ch/statistics/domains/
15	Polônia (.pl)	2.573.378	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
16	Espanha (.es)	2.183.603	30/04/2026	https://www.dominios.es/es/sobre-dominios/estadisticas
17	Portugal (.pt)	2.148.852	01/06/2026	https://www.dns.pt/en/statistics/
18	Estados Unidos da América (.us)	2.036.354	28/02/2026	https://www.about.us/stats-trends
19	Japão (.jp)	1.860.215	01/06/2026	https://jprs.co.jp/en/stat/
20	Bélgica (.be)	1.702.749	01/06/2026	https://www.dnsbelgium.be/en

Data de coleta: 01 de junho de 2026.

O Gráfico 1 apresenta o desempenho do .br desde o ano de 2012.

Gráfico 1 – TOTAL DE REGISTROS DE DOMÍNIOS DO .BR – 2012 a 2026*



*Data de coleta: 31 de maio de 2026.
Fonte: Registro.br
Recuperado de: https://registro.br/dominio/estatisticas

Em maio de 2026, os cinco principais domínios genéricos (*generic Top-Level Domain* [gTLD]) totalizaram mais de 201,65 milhões de registros. Com 163,19 milhões de registros, destaca-se o .com, conforme apontado na Tabela 2.

Tabela 2 – TOTAL DE REGISTROS DE DOMÍNIOS DOS PRINCIPAIS gTLD

Posição	gTLD	Número de domínios
1	**.com**	163.198.805
2	**.net**	12.248.331
3	**.org**	11.909.496
4	**.xyz**	7.823.909
5	**.top**	6.478.286

Data de coleta: 01 de junho de 2026.
Fonte: DomainTools.com
Recuperado de: research.domaintools.com/statistics/tld-counts

Marcadores da Internet no Brasil

Indicadores do Sistema de Medição de Tráfego Internet (SIMET)

As medições realizadas pelos usuários do SIMET apoiam a produção de indicadores e estudos que contribuem para o monitoramento da conectividade e o aperfeiçoamento de políticas públicas digitais.

O Centro de Estudos e Pesquisa em Tecnologia de Redes e Operações (Ceptro.br)[45], departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), é responsável pelo Sistema de Medição de Tráfego de Internet (SIMET)[46]. A plataforma permite avaliar a qualidade da conexão à Internet por meio da coleta de métricas como latência, *jitter*, perda de pacotes e velocidades de *download* e *upload*.

O SIMET foi desenvolvido para fornecer uma avaliação independente da qualidade da conexão. Para isso, utiliza uma metodologia voltada à isenção e à neutralidade das medições. Atualmente, em função da distribuição de sua rede de servidores, a maior parte dos testes é realizada fora da rede da operadora ou do provedor de acesso, reduzindo a influência da infraestrutura do próprio provedor sobre os resultados obtidos.

As medições podem ser realizadas por meio do SIMET Web ou do aplicativo SIMET Mobile, disponível para Android e iOS. Nos últimos seis meses, foram registradas 447.559 medições considerando ambas as modalidades. Além de realizar os testes, o SIMET Mobile auxilia o usuário na interpretação dos resultados, indicando se a conexão é adequada para atividades como trabalho remoto, videoconferências, *streaming* e jogos *online*.

O aplicativo também explica o significado dos principais indicadores de qualidade, apresenta orientações quando são identificados problemas de desempenho e mantém um histórico das medições organizado por local de uso, permitindo acompanhar a evolução da conexão ao longo do tempo e comparar seu desempenho em diferentes ambientes, como residência e trabalho.

Ao utilizar o SIMET, o usuário não apenas obtém um diagnóstico da qualidade da sua conexão, como também contribui para uma base de dados que apoia o monitoramento da conectividade no Brasil. De forma anônima e agregada, essas medições subsidiam iniciativas do NIC.br voltadas ao acompanhamento da qualidade da Internet em serviços públicos essenciais, como escolas e unidades de saúde, contribuindo para a produção de indicadores que apoiam estudos e políticas públicas. A Figura 1 apresenta a cobertura de medições voluntárias usando o SIMET: dos 5.571 municípios brasileiros (incluindo o Distrito Federal), 4.374 (78,51%) tiveram ao menos uma medição no período, ao passo que a Figura 2 mostra o número de medições por município.

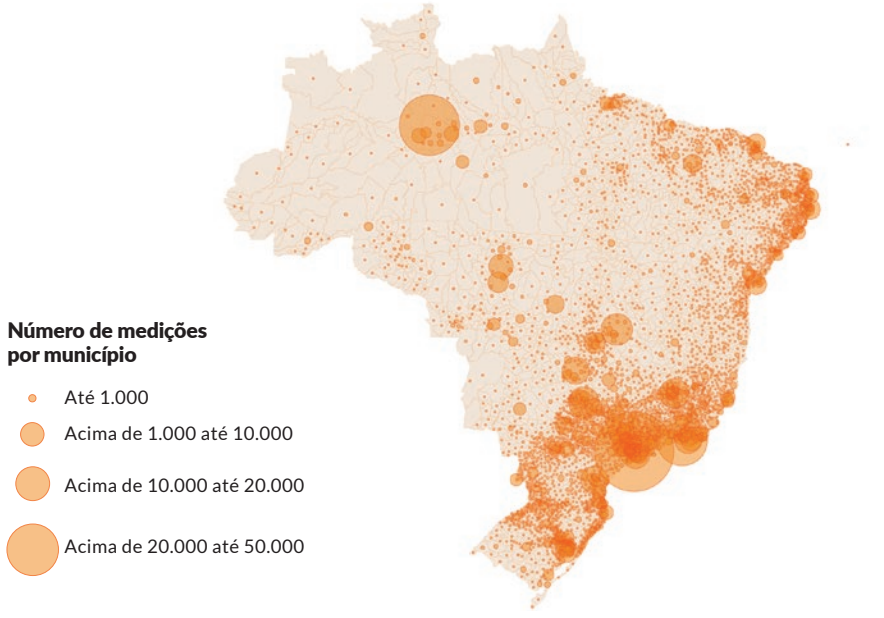
[45] Saiba mais: https://ceptro.br/
[46] Saiba mais: https://medicoes.nic.br/

Cada medição com localização autorizada pelo usuário amplia o conhecimento sobre a conectividade no Brasil e contribui para identificar desigualdades regionais no acesso à Internet.

Figura 1 – REGISTROS DE MEDIÇÕES A PARTIR DOS MEDIDORES *WEB* E *MOBILE*, POR MUNICÍPIO

Período de coleta: dezembro de 2025 a maio de 2026.
Fonte: Ceptro.br | NIC.br

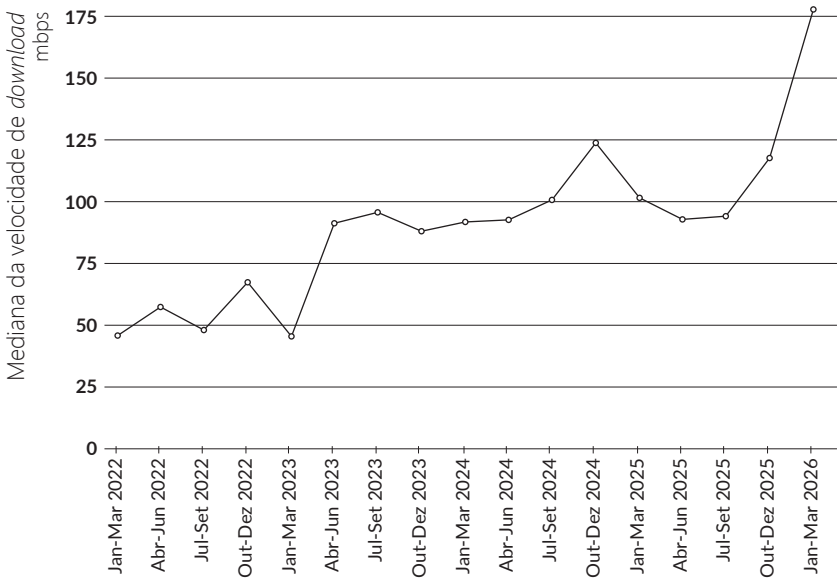
Figura 2 – NÚMERO DE MEDIÇÕES A PARTIR DOS MEDIDORES *WEB* E *MOBILE*, POR MUNICÍPIO



Período de coleta: dezembro de 2025 a maio de 2026.
Fonte: Ceptro.br | NIC.br

A velocidade de *download*, uma das métricas para analisar a qualidade da Internet, refere-se à taxa de transmissão de dados ou velocidade com que ocorrem as transações entre os servidores de medição e o dispositivo medido. Quanto maior a velocidade, melhor a conexão. O Gráfico 1 apresenta a mediana do total de medições de velocidade de *download* por trimestre desde 2022, enquanto a Figura 3 mostra a mediana da velocidade de *download* dos últimos seis meses para cada Unidade da Federação (UF).

Gráfico 1 – MEDIANA DA VELOCIDADE DE *DOWNLOAD* POR TRIMESTRE – 2022 A 2026[47]

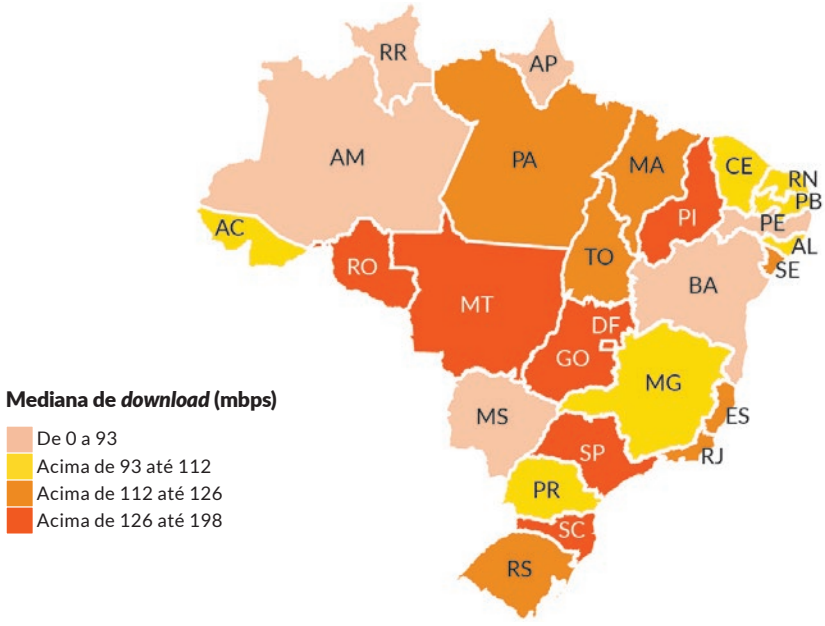


Período de coleta: janeiro de 2022 a março de 2026.
Fonte: Ceptro.br | NIC.br

A evolução da velocidade de *download* é um importante indicador do desenvolvimento da infraestrutura de Internet. Conexões mais rápidas e estáveis ampliam o acesso a serviços digitais, melhoram a experiência dos usuários e favorecem a adoção de aplicações que exigem maior capacidade de transmissão de dados. O acompanhamento desse indicador ao longo do tempo permite monitorar o progresso da conectividade no país.

[47] As flutuações observadas refletem variações existentes na proporção de medições via medidor *mobile* e medidor *web* em cada trimestre. Apesar disso, nota-se uma clara tendência geral de incremento na velocidade de *download* ao longo do tempo.

Figura 3 – MEDIANA DA VELOCIDADE DE *DOWNLOAD*, POR UF



Período de coleta: dezembro de 2025 a de maio de 2026.
Fonte: Ceptro.br | NIC.br

A qualidade da Internet não é homogênea. Diferenças entre regiões refletem características da infraestrutura, da oferta de serviços e das tecnologias de acesso. Mapear essas variações é um passo essencial para compreender os desafios da conectividade e orientar políticas públicas baseadas em evidência.

As medições realizadas pelos usuários são um subsídio essencial para estudos, análises e políticas públicas. Quanto maior o número de medições distribuídas pelos municípios brasileiros, mais precisas são as estimativas da qualidade da Internet no país.

O que você precisa saber sobre

Times de segurança e tratamento de incidentes

Com o papel cada vez mais relevante da tecnologia e da conectividade para todas as atividades da sociedade, os ataques a sistemas na Internet aumentaram em frequência e complexidade. Para detectar os ataques e tratar os incidentes de segurança, existem diversos tipos de times, com particularidades relativas ao público que atendem e ao tipo de serviços prestados[48]. Esses times utilizam em seus nomes acrônimos globalmente associados aos serviços prestados pelo time e, na maior parte dos casos, o nome do time já é o cartão de visitas necessário nos contatos com seus pares. Existe certa confusão e alguns mitos sobre as raízes e os significados desses acrônimos, de forma que segue uma discussão sobre as origens e os usos desses termos pela comunidade.

CERT

Computer Emergency Response Team

O primeiro time criado foi o CERT Coordination Center (CERT/CC), em 1988, como uma das necessidades identificadas na resposta ao *Morris Worm*[49]. Alguns anos depois, a sigla tornou-se marca registrada do Software Engineering Institute, da Carnegie Mellon University (SEI/CMU), por conta de atacantes terem tentado usar o acrônimo para se passarem por um CERT e terem acesso privilegiado a organizações-alvo. Desde então, para usar a sigla, é praxe pedir permissão à CERT Division do SEI/CMU. Fora isso, não há nenhuma diferença entre um time ser chamado CERT, *Computer Security Incident Response Team* (CSIRT), *Computer Incident Response Team* (CIRT), *Incident Response Team* (IRT) ou outras siglas que fazem alusão a times de tratamento de incidentes.

CSIRT

Computer Security Incident Response Team

Um CSIRT oferece serviços de gestão de incidentes de segurança com foco em prevenção, tratamento (isto é, detecção, análise e resposta) e/ou coordenação das ações necessárias para o tratamento efetivo de incidentes. Outras siglas usadas com frequência são CERT, CIRT, *Computer Incident Response Center* (CIRC) ou variações, com base nos objetivos da organização que criou o time. É importante destacar que o acrônimo CSIRT foi criado em 1998, quando o SEI/CMU publicou o *Handbook for Computer Security Incident Response Teams* (CSIRTs)[50], documento seminal que, pela primeira vez, definiu e formalizou o trabalho de tratamento de incidentes. A sigla CSIRT e sua expansão foram criadas pelos autores para se referir, de forma genérica, a times de tratamento de incidentes, uma vez que CERT é uma marca registrada.

[48] As definições dos tipos de times têm como base o documento Team Types within the context of services frameworks, do Forum of Incident Response and Security Teams. Disponível em: https://www.first.org/standards/frameworks/csirts/team-type_1.2

[49] Saiba mais: https://www.fbi.gov/history/cases-and-criminals/morris-worm e https://alumni.cornell.edu/cornellians/morris-worm/

[50] Disponível em: https://www.sei.cmu.edu/library/handbook-for-computer-security-incident-response-teams-csirts/

Desde então, CSIRT é um dos acrônimos mais utilizados para se referir a times de resposta e tratamento de incidentes. Muitos times, por pragmatismo, adotam como nome simplesmente "CSIRT Organização", de forma a indicar o tipo de trabalho que realizam. Dependendo das escolhas da organização, o CSIRT pode também realizar tarefas que usualmente são realizadas por um SOC.

ISAC

Information Sharing and Analysis Center

Um ISAC é um centro dedicado a um setor específico (por exemplo, financeiro, elétrico ou industrial) e foca em coletar, analisar e compartilhar informações relativas a ameaças cibernéticas específicas para o setor a que atende. Pode atuar também como um facilitador da cooperação setorial.

SOC

Security Operations Center

Um SOC é um time que foca na gestão de eventos de segurança, ou seja, na monitoração e na detecção de ataques. Para isso, um SOC precisa ter acesso aos registros de eventos (*logs*) da organização. É o time que, em geral, trata de alertas de sistemas de detecção de intrusão e monitoração de *endpoints* (como *security information and event management* [SIEM], *endpoint detection and response* [EDR], *extended detection and response* [XDR], *firewall,* etc.). Algumas organizações optam por implementar funções de tratamento de incidentes como parte das atividades do SOC.

PSIRT

Product Security Incident Response Team

Um PSIRT é um time que foca na identificação, na avaliação e no tratamento de riscos associados com vulnerabilidades de segurança dos produtos desenvolvidos por uma organização e, em geral, está associado a um fornecedor de *software*, que pode ser comercial ou de código aberto.

CTIR e ETIR

Equipe de Tratamento e Resposta a Incidentes Cibernéticos

No Brasil, estes são dois acrônimos que têm sido utilizados por entidades ligadas ao governo para designar seus CSIRTs. CTIR foi o acrônimo escolhido por ocasião da criação do CTIR Gov[51], CSIRT mantido pelo Gabinete de Segurança Institucional, e, originalmente, era expandido para Centro de Tratamento de Incidentes em Redes do Governo Federal e, atualmente, foi expandido para Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Já a sigla ETIR começou a ser utilizada após a publicação da Instrução Normativa n. 1 do GSI/PR[52], que define que todo órgão ou entidade da Administração Pública Federal deveria instituir uma ETIR. Como essas siglas não são conhecidas internacionalmente, boa parte dos times que as utiliza no Brasil precisa se identificar de alguma forma alternativa quando os interlocutores são de outros países.

[51] Saiba mais: https://www.gov.br/gsi/pt-br/assuntos/ctir

[52] Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN01_consolidada.pdf

/Créditos

REDAÇÃO

RELATÓRIO DE DOMÍNIOS

Thiago Meireles (Cetic.br | NIC.br)

INFOGRAFIA

Andre Martini Martins (Comunicação | NIC.br)

DIAGRAMAÇÃO

Grappa Marketing Editorial

EDIÇÃO DE TEXTO EM PORTUGUÊS

Érica Santos Soares de Freitas

TRADUÇÃO INGLÊS-PORTUGUÊS

Prioridade Consultoria Ltda.: Isabela Ayub, Lorna Simons, Luana Guedes, Luísa Caliri e Maya Bellomo Johnson

COORDENAÇÃO EDITORIAL

Alexandre F. Barbosa, Graziela Castello, Javiera F. M. Macaya, Manuela Cortez da Cunha Cruz, Rodrigo Brandão e Mariana Galhardo Oliveira (Cetic.br | NIC.br)

AGRADECIMENTOS

Javiera F. Medina Macaya (Cetic.br | NIC.br)

Cristine Hoepers (CERT.br | NIC.br)

Olivier Caleff (FIRST, CSIRT.FR, and Open CSIRT Foundation)

Gilberto Zorello (NIC.br)

SOBRE O CETIC.br

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br (https://www.cetic.br/), departamento do NIC.br, é responsável pela produção de estudos e estatísticas sobre o acesso e o uso da Internet no Brasil, divulgando análises e informações periódicas sobre o desenvolvimento da rede no país. O Cetic.br atua sob os auspícios da UNESCO.

SOBRE O NIC.br

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br (https://nic.br/) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no país. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

SOBRE O CGI.br

O Comitê Gestor da Internet no Brasil – CGI.br (https://cgi.br/), responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

*As ideias e opiniões expressas nos textos dessa publicação são as dos respectivos autores e não refletem necessariamente as do NIC.br e do CGI.br.

unesco
Centro sob os auspícios da UNESCO

cetic.br
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

ISSN - 2965-2642

POR UMA INTERNET CADA VEZ MELHOR NO BRASIL

CGI.BR, MODELO DE GOVERNANÇA MULTISSETORIAL

https://cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK