2020

Relatório Anual

de Segurança da Rede Nacional
de Ensino e Pesquisa (RNP)

CAIS

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

SUMÁRIO

01

Sobre

REDE NACIONAL DE ENSINO E PESQUISA (RNP)

Criada em 1989, a RNP [01] foi pioneira no uso de internet no Brasil. Ela é uma associação civil sem fins lucrativos, qualificada como Organização Social (OS) pela Presidência da República, que apoia o ensino superior, o desenvolvimento científico e tecnológico, além da pesquisa e inovação em todo o país através de um *backbone* nacional de alta capacidade, a rede Ipê; com Pontos de Presença (PoPs) em todas as unidades da federação, conecta mais de 800 organizações, distribuídas em 1,5 mil unidades conectadas. Sendo 276 instituições de ensino superior e pesquisa, 66 agências de fomento, 51 estabelecimentos de saúde com ensino e pesquisa, além de bibliotecas, museus, instituições culturais, empresas inovadoras, parques tecnológicos e ambientes promotores de inovação; oferta também serviços, soluções tecnológicas, infraestrutura e ações coordenadas para o benefício de mais de quatro milhões de usuários.

+800
Organizações Usuárias

66
Agências de Fomento

1,5 mil
Unidades conectadas

276
Instituições de ensino superior e pesquisa

55
Estabelecimentos de saúde com ensino e pesquisa

01

CAIS

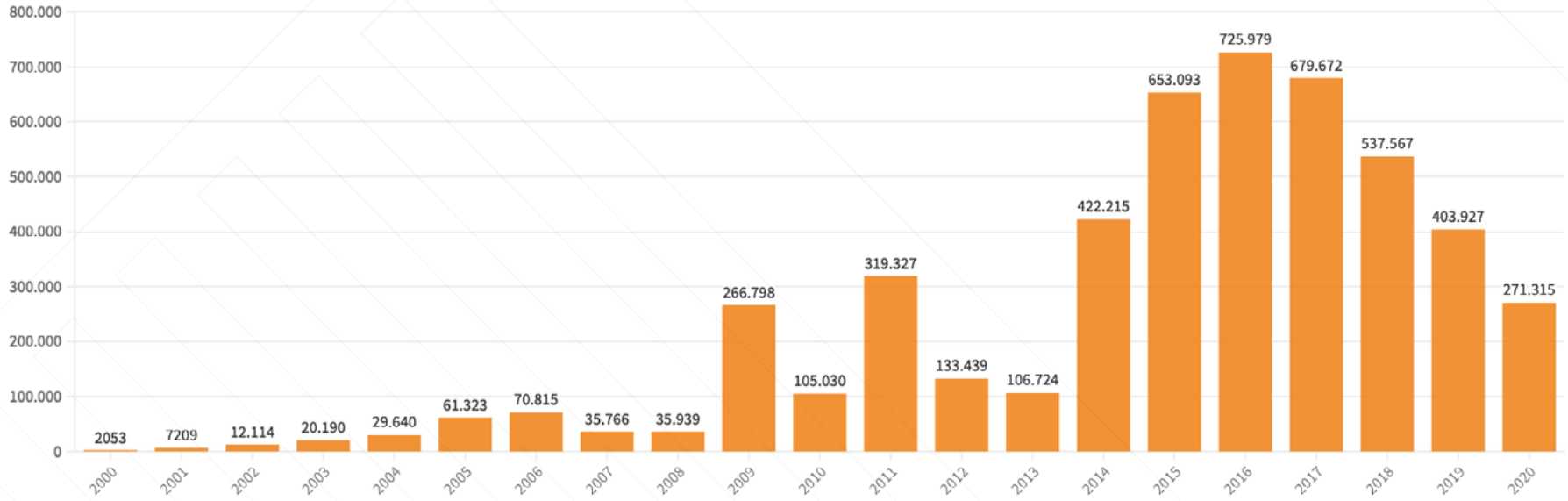
Criado em 1997, o Centro de Atendimento a Incidentes de Segurança (CAIS) é o CSIRT (Computer Security Incident Response Team) de coordenação da rede Ipê e atua na detecção, resolução e prevenção de incidentes de segurança na rede, além de elaborar, promover e disseminar práticas de segurança em redes na RNP e demais instituições a ela vinculadas. 02

Como equipe responsável pelo fomento de ações para apoio e aumento da maturidade de segurança na comunidade de instituições clientes da RNP, o chamado Sistema RNP, o CAIS provê diversos serviços de segurança, tecnologias e iniciativas de capacitação e conscientização em segurança da informação a toda essa comunidade.

02

GRÁFICO A

NOTIFICAÇÕES DE INCIDENTES E VULNERABILIDADES POR ANO



02

Resumo Executivo

RESUMO EXECUTIVO

Após três anos desde sua última edição, o Relatório Anual de Segurança da RNP 2020 traz à luz um cenário absolutamente distinto daquele de 2017. Se fossemos definir em uma só palavra a principal preocupação do setor de Tecnologia da Informação e Comunicação (TIC), certamente escolheríamos: perplexidade.

Sim, 2020 foi um ano singular em muitos aspectos. Nem precisamos rememorar a crise geopolítica do primeiro trimestre, quando o relógio do apocalipse quase alcançou finalmente o marco da meia-noite trazendo de novo a sombra da guerra. Não! Eis que - para a perplexidade do mundo - veio o mês de março e fez o tempo parar com a notícia da pandemia e da fragilidade do sistema social e econômico já quase colapsando.

Pois é, "manteve-se" o relógio do fim dos tempos há dois minutos para meia-noite, afinal, isso não é necessariamente uma boa notícia. 2020 será marcado como o ano da controversa polarização - política, social, econômica, tecnológica, identitária, ideológica e, como se pouco fosse toda essa efervescente condição, uma das questões mais controversas abordadas constantemente durante o ano foi a mudança de paradigmas das relações de trabalho, da chamada 4ª Revolução Industrial, da cibereconomia, ciberindústria e claro; cibercrime também.

Pudemos testemunhar uma enxurrada de ataques cibernéticos, de vazamentos de dados e exposição de documentos de pessoas, empresas e instituições em vários locais do mundo, sob várias circunstâncias, com os mais desastrosos efeitos colaterais para a sociedade e a economia, apresentando toda uma realidade oculta, avançada, bem organizada e criativa rede de inteligência, pesquisa e desenvolvimento focada em crimes cibernéticos.

Nunca se falou tanto em Segurança da Informação. Nunca foi tão necessário estabelecermos premissas normativas e legais sobre o uso da internet e do compartilhamento de dados entre entes reais ou digitais porque a informação tornou-se o mais valioso ativo neste Admirável Mundo Digital.

É sobre isso que vamos tratar aqui. Mas não se engane, o relatório deste ano também é um marco de 2020. Isso porque a RNP foi agente importantíssimo na viabilização de recursos técnicos e intelectuais no enfrentamento dos desafios que se apresentaram nos últimos 12 meses da história recente da nossa organização.

RESUMO EXECUTIVO

Buscamos trazer para você, mais que um relatório que reporta os principais acontecimentos, elenca dados, tendências, leituras analíticas e interessante artigo. Nas próximas páginas, você poderá desfrutar de uma leitura leve e esclarecedora, mas não menos relevante. Queremos que o significativo crescimento e a exemplar atuação do CAIS e da RNP junto à comunidade acadêmica e demais órgãos beneficiados, sejam acessíveis a quem estiver disposto a conhecê-los. Até porque, muito dessa atuação tem impacto direto na vida e no quotidiano das pessoas que compõem essas instituições, sobretudo no que diz respeito à sua segurança no ambiente da internet e da telecomunicação.

A estrutura do relatório permanece a mesma das edições anteriores. O que muda é a linguagem, a maneira com o qual, o reporte dos dados ganha uma narrativa por onde as diferentes áreas poderão se reconhecer. É uma forma, inclusive da RNP e do CAIS, valorizarem seus recursos, trazendo ao relatório um olhar crítico, didático e inovador sobre o crucial papel de cada um.

A primeira parte, portanto, aborda os principais destaques relacionados à área da segurança da informação. Como já demos spoiler anteriormente, o cibercrime é o hit do momento, e procuramos salientar como a recente mudança comportamental relacionada às novas formas de relacionamento social, de trabalho e comerciais (impulsionados pelas medidas de segurança em combate à pandemia) permitiu que práticas perniciosas da computação se valessem dessa fragilidade para atuar de maneira mais contundente e regular. 2020 foi o ano do *ransomware* na seção [Destaques] deste relatório você vai entender o porquê e ainda lembrar de alguns episódios importantes relacionados a vazamento de dados das gigantes de tecnologia e como foi a atuação da RNP frente ao ataque cibernético dirigido ao STJ em novembro do ano passado.

Após ler nossos destaques você encontrará uma análise quantitativa das notificações de incidentes e vulnerabilidades de segurança na seção [Estatísticas] onde levantamos os precisos números de vulnerabilidades desde 2018 e ainda elencamos os cinco principais casos sobre a ótica de estudo, compartilhamento de conhecimento e informação através do Projeto TOP5.

A coletânea apresentada nestas páginas elucida o processo comportamental dos ataques,

RESUMO EXECUTIVO

seus alvos, métodos e natureza, demonstrando que o advento de novas tecnologias está intimamente ligado à concepção de modelos mais robustos e eficientes de segurança.

"A sensação de segurança é a maior das ameaças".

Como a lei do caos indica a proximidade da ordem, na seção [Atualize-se] nós trouxemos um levantamento das principais e mais importantes iniciativas da RNP, através do CAIS, no tocante ao esclarecimento, divulgação, compartilhamento de informação, conhecimento e colaboração com toda comunidade atendida. Ali, as "suas configurações de acontecimentos serão atualizadas" e você poderá saber mais sobre os inúmeros esforços da RNP em se manter - como sempre - à vanguarda das incomensuráveis melhorias e estruturação que fomentam o ciclo de desenvolvimento seguro de novas tecnologias. Eis um vislumbre presente do olhar lançado ao futuro que queremos que você fique sabendo. São tantos assuntos, realizações, novos dados e atualizações sobre todos os projetos que é melhor você conferir por conta própria; cuidamos de tudo para que sua atualização seja realizada com sucesso ;)

Na sequência convidamos você ao artigo escrito pelo Diretor de Engenharia e Operações, Eduardo Grizendi sobre a Cibersegurança da RNP e o ano de 2020. Uma leitura indispensável.

Por fim a seção [Tendências] explora o que de novo - ou não tão novo assim - pode se tornar cada vez mais recorrente no ano de 2021 e seguintes. Essas tendências trazem um ponto de vista mais humanizado, onde a percepção sobre os principais acontecimentos do ano passado tomam ar de aprendizado e que ajudam a todos a obterem conhecimento para acrescentarem-se às importantes discussões da comunidade técnica e acadêmica a convergirem em soluções ágeis e cada vez mais inteligentes e seguras a todos. Estão ali, insumos valiosos sobre oportunidades e desafios que estão por vir e você saber disso já é, pra gente, a certeza que estamos no caminho certo, com as pessoas certas e principalmente à frente de propósitos duradouros para o cenário da Segurança da Informação no Brasil e no mundo.

Boa leitura!

03

Destaques do ano

INCIDENTES DE SEGURANÇA E CIBERCRIME

ACONTECEU EM 2020

O ano de 2020 trouxe transformações consideráveis para todas as organizações, por conta do grande acontecimento que foi a pandemia causada pela Covid-19. Algumas sofreram impactos maiores, pois nunca haviam testado o modelo de trabalho remoto, portanto, não possuíam infraestrutura e processos para suportar essa transformação eficientemente, com a urgência por se adaptar e a mudança com pouco planejamento, muitas dessas organizações tornaram-se alvos para a exploração de vulnerabilidades. Mesmo com as dificuldades encontradas no processo de adaptação, é possível notar que as novas condições de trabalho vieram para ficar e muitas empresas decidiram permanecer com o esquema de trabalho remoto, ao menos parcialmente.

Olhando para este cenário, um dos grandes desafios foi pensar na segurança da informação. No caso da RNP, que já estava preparada para essa passagem, pois já havia um programa de home office implantado, que será abordado mais adiante, não houve grandes dificuldades: a operação não sofreu impactos substanciais e os funcionários puderam trabalhar de casa contando com toda a estrutura de segurança necessária. Registros mostram que a RNP não teve incidentes significativos relacionados a incidentes de segurança, ou cibercrime. Esse desdobramento se deu, em grande parte, pelo trabalho contínuo do CAIS no fortalecimento da cultura de segurança, ainda mais intensificado durante o ano de 2020. Além disso, houve um cuidado ainda maior com a implantação dos acessos remotos. No entanto, ao ampliar a lente abrangendo a realidade do país, os seguintes destaques se apresentam:

ANO DO *RANSOMWARE* E *PHISHING* EM PLENA COVID-19

ACONTECEU EM 2020

Um dos maiores destaques de 2020 foi, sem dúvida, os ataques de *ransomware*. Não só pela grande quantidade de ocorrências, mas também pela evolução e combinação do ataque com outros tipos, em 2020 muitos ataques de *ransomware* foram combinados com o de vazamento de dados. Os atacantes cobraram de suas vítimas dinheiro para devolver-lhes o acesso aos seus dados e, adicionalmente, cobraram também para não vazar cópias desses dados na internet.

Também destacam-se as campanhas de *phishing*, explorando temas relativos à COVID-19.

Os alvos e métodos não mudaram muito, mas a incidência foi maior e com maior efetividade, devido principalmente à urgência dos temas explorados: pandemia, novas vacinas, planos assistenciais do governo, etc. A atenção a esses temas foi reforçado pelo cenário de isolamento social e risco iminente de contaminação.

Campanhas de *phishing* com: "CLIQUE AQUI PARA SABER DE MAIS CASOS DE COVID-19 NA SUA REGIÃO", passaram a ser frequentes durante todo o ano, assim como sites falsos, cujo foco principal era fornecer informações relacionadas à pandemia. Com isso podemos continuar destacando a prática do cibercrime explorando vulnerabilidades conhecidas de protocolos e tecnologias muito difundidas como *POP*, *IMAP* e *DRUPAL*, em muitos casos também relacionados à mineração indevida de criptomoedas.

O cenário que se fez em 2020 e que propiciou o crescimento exponencial do uso de serviços online, associado à fragilidade na segurança da informação em empresas recém-lançadas ao Home Office, facilitou a ocorrência de incidentes de segurança. No próximo bloco, reunimos outros casos de destaque em 2020.

CASES DIVERSOS

2019

Microsoft

Fev

Mar

zoom

facebook

Nintendo

Mai

twitter

JANEIRO DE 2020, MICROSOFT

Um banco de dados de suporte ao cliente com mais de 280 milhões de registros de clientes da Microsoft foi deixado desprotegido na web.

ABRIL DE 2020, ZOOM

As credenciais de mais de 500 mil contas de teleconferência (Zoom) foram encontradas para venda na *Dark Web* e em fóruns de hackers por apenas US$0,02.

ABRIL DE 2020, FACEBOOK

Mais de 267 milhões de perfis do Facebook foram listados para venda na *Dark Web* — tudo por US$600.

ABRIL DE 2020, NINTENDO

Um vazamento de informações expondo as credenciais de usuários e senhas previamente expostas da popular empresa de videogame Nintendo concedeu aos hackers acessos a mais de 160 mil contas de jogadores.

JUNHO DE 2020, TWITTER

Uma falha de segurança no Twitter fez com que as informações da conta dos usuários da empresa de mídia social fossem expostas.

Jul

Ago

RAZER

ACTIVISION

Pfizer

Nov

FIREEYE

Spotify

SETEMBRO DE 2020, RAZER

Um banco de dados com as informações de clientes de 100 mil jogadores que fizeram compras com a empresa de tecnologia de jogos, Razer, foi encontrado online e desprotegido.

SETEMBRO DE 2020, ACTIVISION

Mais de 500 mil contas de jogadores da Activision, a editora de videogame, foram alvo de um ataque de enchimento de credenciais.

OUTUBRO DE 2020, PFIZER

A empresa farmacêutica Pfizer expôs as informações pessoais e médicas de centenas de pacientes que tomam medicamentos contra o câncer por meio de um vazamento de dados.

DEZEMBRO DE 2020, FIREEYE

Uma das maiores empresas de segurança do mundo, a FireEye, revelou que um terceiro não autorizado acessou suas redes e roubou as ferramentas de software de *hacking* da empresa.

DEZEMBRO DE 2020, SPOTIFY

Um número não revelado de usuários do serviço de streaming de áudio, Spotify, teve suas senhas redefinidas depois que uma vulnerabilidade de software expôs informações da conta.

2021

AÇÕES DA RNP FRENTE AO INCIDENTE DE SEGURANÇA OCORRIDO NO STJ

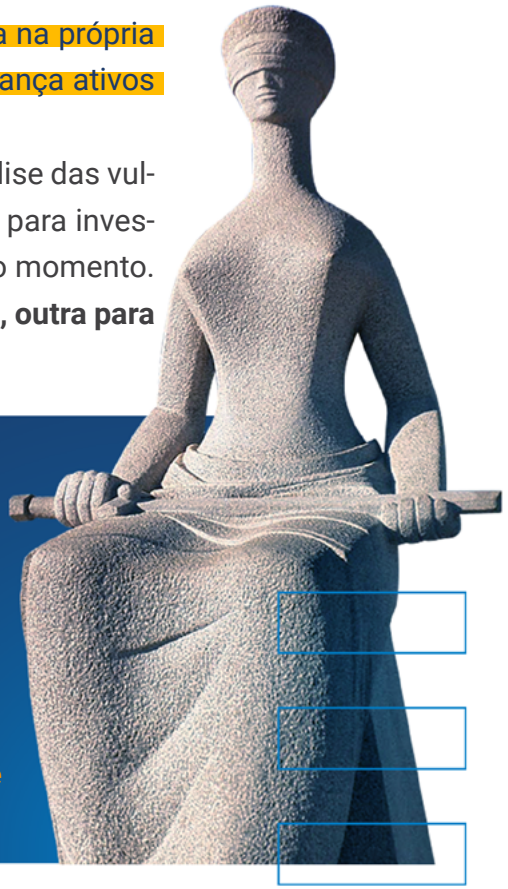
ACONTECEU EM 2020

O incidente de segurança ocorrido em novembro, no Supremo Tribunal de Justiça (STJ) não teve relação direta com a RNP ou seu time de segurança, o CAIS. Trazemos o caso para estudo, pois uma vez descoberto o incidente, e a ocorrência em série em outras instituições governamentais, o CAIS iniciou uma série de medidas internas e externas para impedir a ocorrência na própria RNP e nas demais instituições do Sistema RNP. Essas medidas evidenciam alguns benefícios de se ter times de segurança ativos e com capacidade de coordenação e colaboração no Sistema RNP.

Logo que noticiado, mesmo em grupos especializados de segurança, o CAIS mobilizou um grupo de trabalho para a análise das vulnerabilidades envolvidas e na mitigação de quaisquer ações semelhantes no Sistema RNP. O grupo logo estava pronto para investigar e entender o incidente e suas causas e também para se comunicar com demais grupos de segurança atuantes no momento. Estabeleceu-se então três linhas de ações, **uma focada na troca de informações entre equipes e *reports* aos envolvidos, outra para checagens na infraestrutura de TIC da RNP, e uma terceira para apoiar as instituições do Sistema RNP.**

Alertas de segurança foram enviados a todas as instituições do Sistema RNP, comunicando recorrentemente os passos técnicos e esclarecimentos necessários. Também se montou um plantão técnico, através de videoconferência, onde o CAIS fez esclarecimentos e orientou os interessados quanto às medidas necessárias para melhoria da segurança. Não se apurou no Sistema RNP casos com relação direta aos envolvidos no ataque do STJ, os ataques coordenados cessaram antes de afetar diretamente essas organizações. Destaca-se então as vantagens de se ter times de segurança especializados e conectados, o que diminui o tempo de resposta a ameaças cibernéticas.

Como principal aprendizado fica a lição de que é essencial manter comunicação ativa entre os times de segurança e a comunidade de tecnologia, para diminuir o tempo de resposta às ameaças, ter avaliação situacional mais clara e ser capaz de tomar medidas corretivas e preventivas com mais eficiência. A RNP, através do CAIS, busca comunicar, munir e apoiar as instituições parceiras frente às ameaças cibernéticas.



04

Estatísticas

SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

Esse capítulo apresenta os principais números relacionados aos incidentes e vulnerabilidades no Sistema RNP.

É importante lembrar que o cenário monitorado compreende todo sistema RNP, com 800 organizações no país, assim como os Pontos de presença (PoPs) e escritórios da RNP.

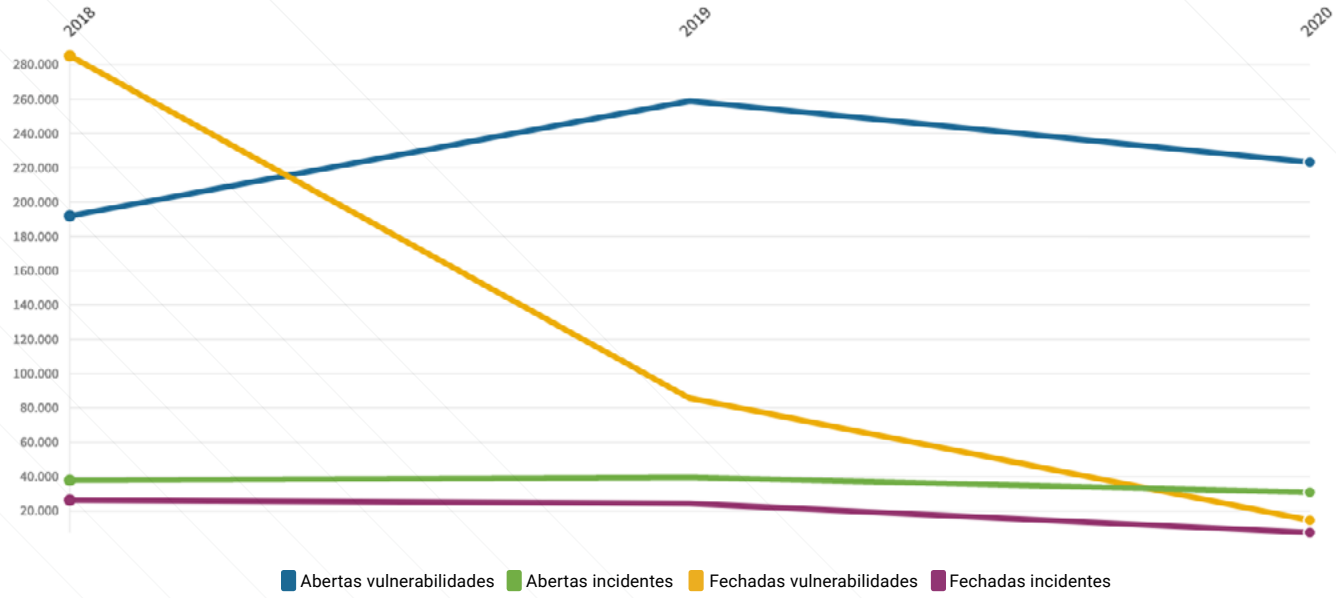
Cada vulnerabilidade ou incidente são notificados seguindo um protocolo de comunicação com foco no tratamento da fragilidade detectada. De forma simples, o responsável pelo *host* onde se detectou uma vulnerabilidade ou incidente de segurança é notificado e recebe insumos para os devidos tratamentos.

PROTOCOLO DE COMUNICAÇÃO

1. Informações sobre o incidente ou vulnerabilidade detectado.
2. Evidências coletadas até o momento da notificação.
3. Orientações para correção ou mitigação.
4. Demais orientações e suporte.

A primeira informação que queremos compartilhar trata do volume de notificações de vulnerabilidades e incidentes ao longo dos últimos três anos (gráfico A):

GRÁFICO A **NOTIFICAÇÕES DE VULNERABILIDADE E INCIDENTES 2018 A 2020**



SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

Nitidamente percebe-se que ao longo do período analisado, o volume de notificações reduziu significativamente, em parte resultado da elevação da maturidade de segurança do Sistema RNP, obtida através de diversas iniciativas, que serão detalhadamente descritas no decorrer desse relatório.

Nos gráficos a seguir, você poderá analisar o percentual de notificações de vulnerabilidades e incidentes ocorridos nos últimos três anos nos estados com maior número de notificações em cada região do Brasil, agrupadamente (gráfico B) e também seu volume em cada um dos anos, separadamente (gráfico C):

Os dados mostram que houve um crescimento gradual de notificações no estado do Rio de Janeiro, que representa quase a metade do volume de todas as notificações (46%), enquanto nos estados de Pernambuco e Paraná observa-se uma redução sistemática na incidência das notificações com o passar dos últimos três anos.

GRÁFICO B **NOTIFICAÇÕES POR REGIÃO 2018 A 2020**

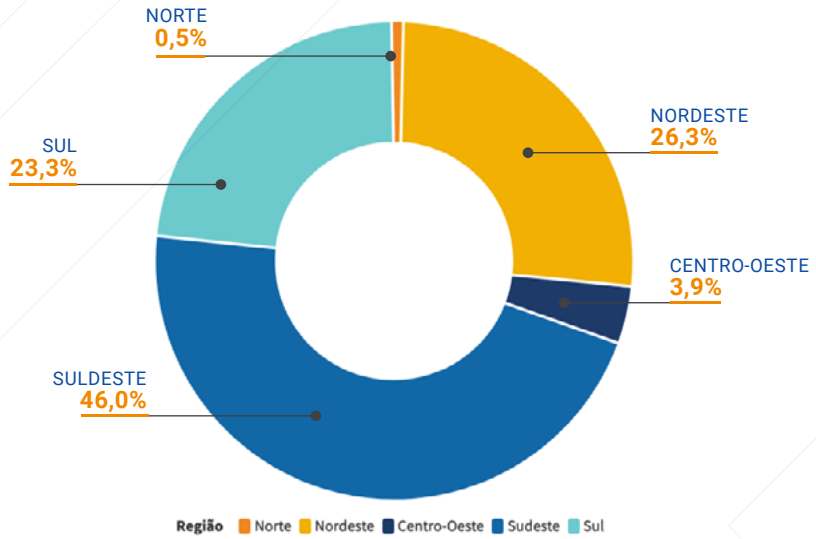
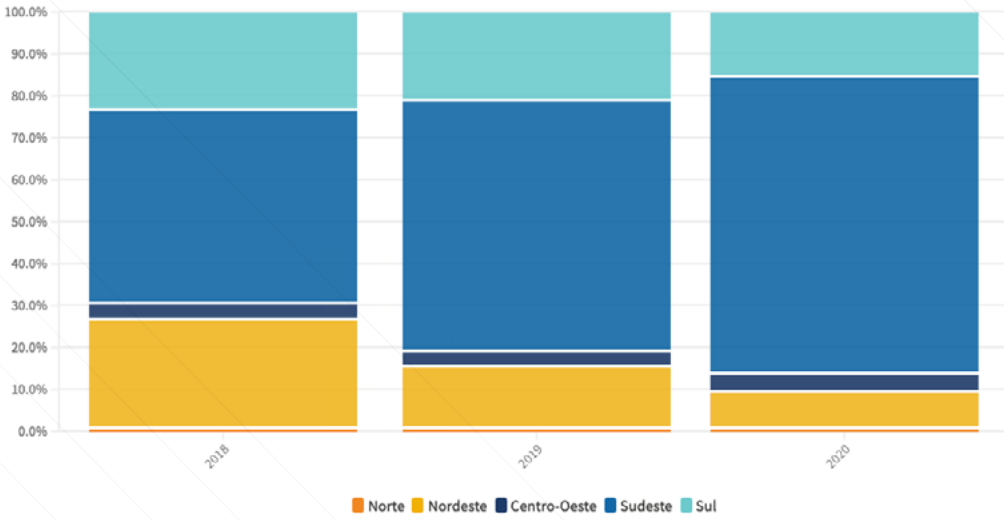


GRÁFICO C **PROPORÇÃO DE NOTIFICAÇÕES POR REGIÃO 2018 A 2020**



SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

De modo a identificar padrões entre notificações e épocas sazonais, trazemos a seguir comparativos anuais de vulnerabilidades mensais por região, nos últimos três anos:

Nota-se que o primeiro semestre concentrou o maior volume das notificações. Trazemos então, em números absolutos, o quanto essa incidência representou a mais no período:

20.715	2018
29.451	2019
18.745	2020

GRÁFICO **D**

VULNERABILIDADES MENSAIS POR REGIÃO 2018

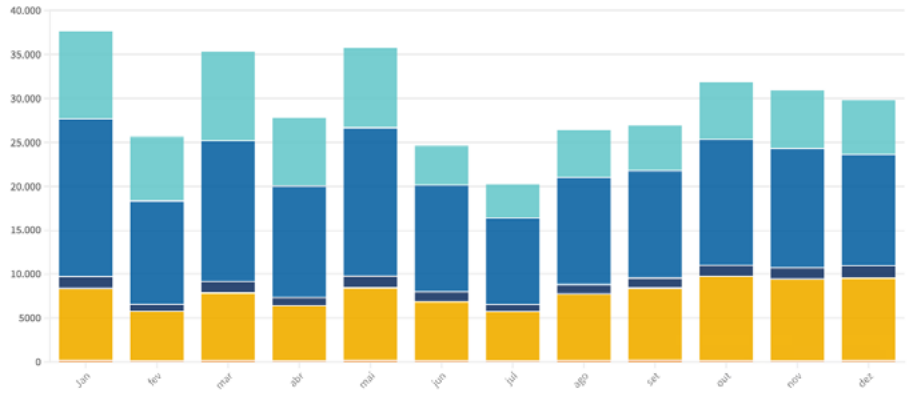


GRÁFICO **E**

VULNERABILIDADES MENSAIS POR REGIÃO 2018

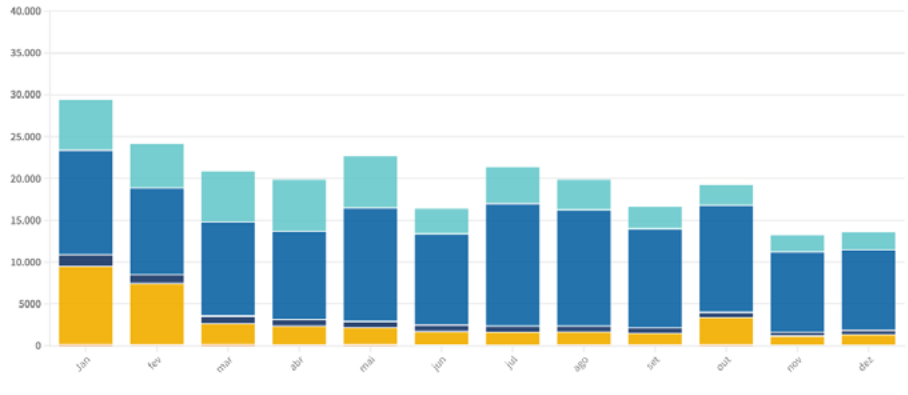
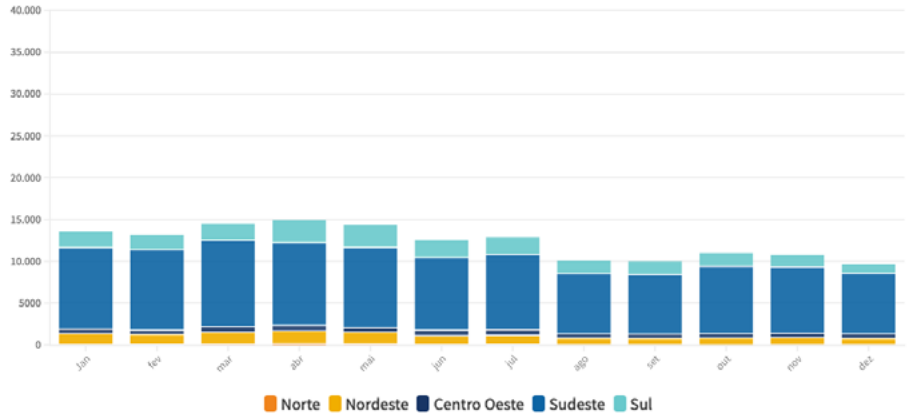


GRÁFICO **F**

VULNERABILIDADES MENSAIS POR REGIÃO 2018



SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

Outra análise possível quanto às estatísticas das notificações é que, historicamente, o primeiro trimestre é o que tem maior incidência de vulnerabilidades e incidentes, mas em 2020 esse comportamento mudou, apesar de os primeiros meses ainda concentrarem o maior número de notificações, o mês de abril teve o maior pico de notificações. Esse comportamento foi também afetado pela migração de alunos, pesquisadores e colaboradores das instituições de ensino que foram para o esquema de trabalho ou estudo remoto.

Ao analisar a distribuição mensal, os efeitos da pandemia são notórios pela quantidade decrescente de notificações nos meses em que as instituições estiveram fechadas ou com atividades reduzidas.

GRÁFICO **G** **COMPARATIVOS ANUAIS DE VULNERABILIDADE**
(RECORTE 1º MÊS COM MAIS INCIDÊNCIA)

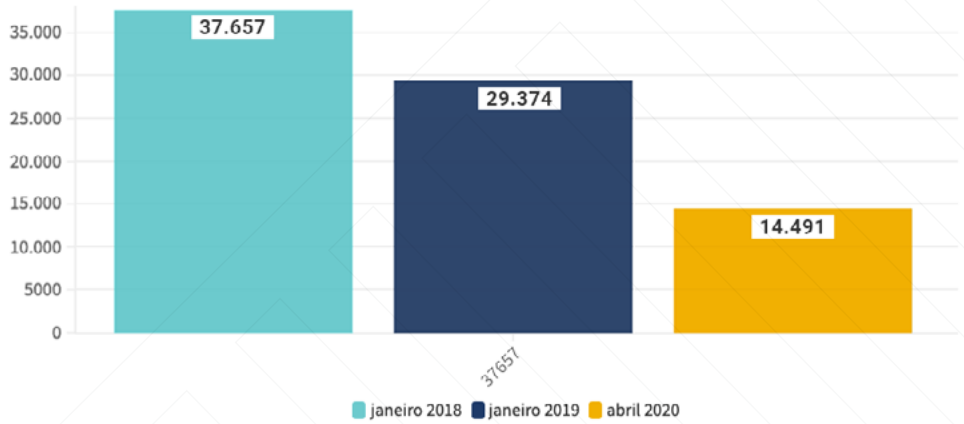
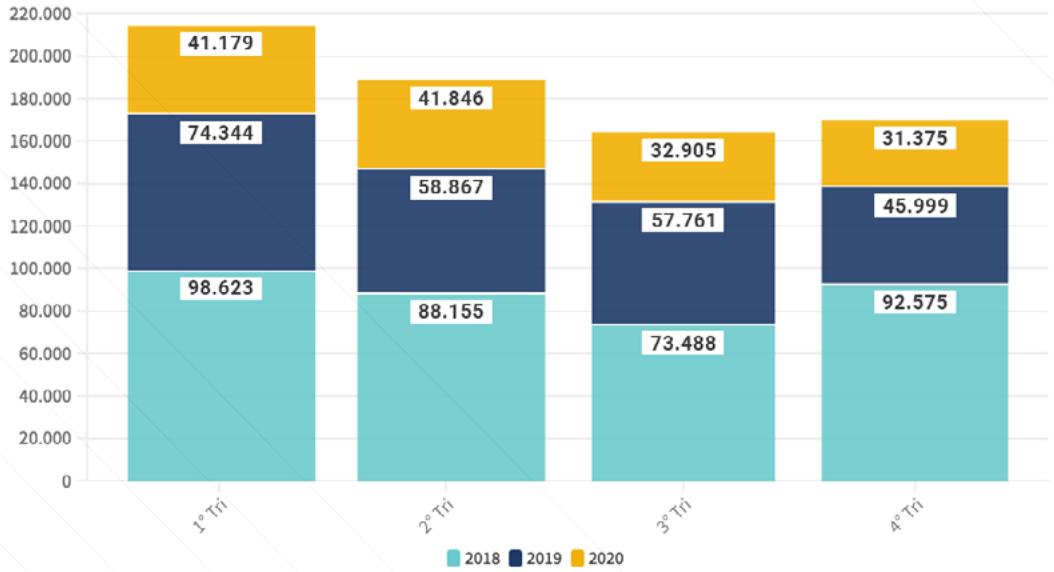


GRÁFICO **H** **COMPARATIVOS TRIMESTRAIS DE VULNERABILIDADE**



SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

Dada análise quantitativa das notificações de vulnerabilidade, faz-se *mister* apontar as categorias em que elas incidem, sendo assim, trazemos a análise das 5 maiores vulnerabilidades nos anos de 2018, 2019 e 2020 (gráfico I, J e K):

GRÁFICO I **TOP5 CATEGORIAS DE VULNERABILIDADE 2018**

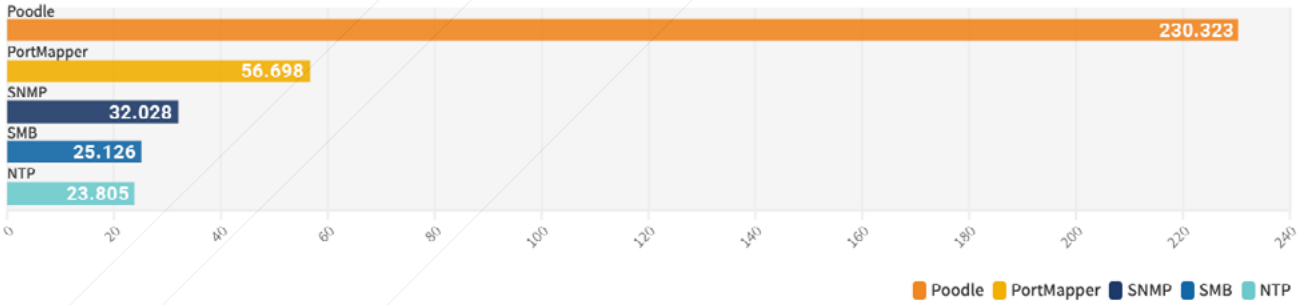


GRÁFICO J **TOP5 CATEGORIAS DE VULNERABILIDADE 2019**

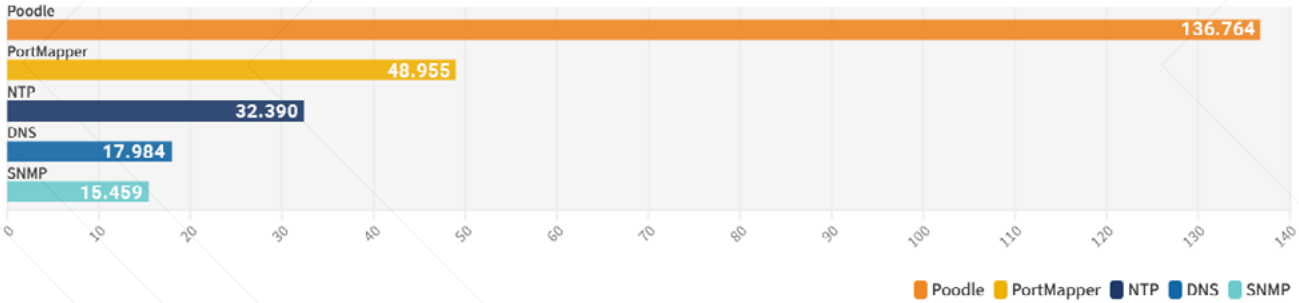
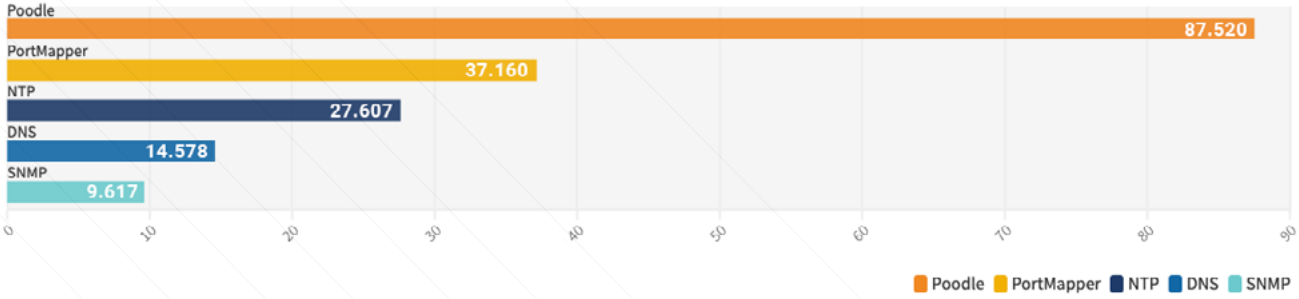


GRÁFICO K **TOP5 CATEGORIAS DE VULNERABILIDADE 2020**

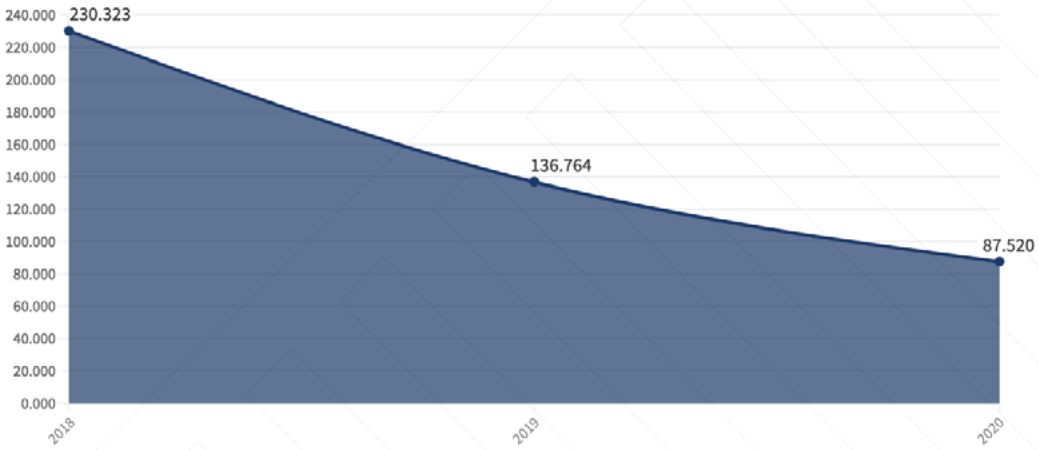


SEGURANÇA EM NÚMEROS

NOTIFICAÇÕES

Quando analisamos os cinco principais tipos de vulnerabilidades nos últimos três anos, nota-se que a vulnerabilidade *Poodle* continua sendo a principal fragilidade reportada. Essa vulnerabilidade está relacionada com a versão 3 do *SSL* (Secure Socket Layer), um protocolo de criptografia vastamente utilizado na internet, mas que já pode ser substituido pelo seu sucessor, o *TLS* (Transport Layer Security), o que ocasiona uma diminuição expressiva em sua incidência (gráfico L).

GRÁFICO **L** **VULNERABILIDADE POODLE 2018 A 2020**



Como a exploração dessa vulnerabilidade na maioria das vezes é silenciosa, existe uma maior dificuldade dos administradores das redes e sistemas na percepção e detecção de um ataque através do *Poodle*. Porém, a exploração dessa vulnerabilidade traz riscos gravíssimos, permitindo o vazamento de dados através do acesso indevido à informação.

Corrigir essa vulnerabilidade pode ser difícil em casos de sistemas legados, mas existem ações de contorno para limitar o acesso e exploração dessa vulnerabilidade, quando não é possível corrigi-la. Faz-se necessário para corrigir essa vulnerabilidade, a atualização para *TLS*, assim como é imprescindível desabilitar cifras frágeis.

Recomendamos sempre avaliar se os sistemas e serviços precisam estar de fato acessíveis através da internet, lembrando que independente do acesso público os sistemas devem ter uma rotina de verificação e atualização dos seus sistemas operacionais, aplicações e ferramentas utilizadas, pois as atualizações trazem *patches* de segurança, além das correções de bugs.

Ressaltamos uma iniciativa específica relacionada diretamente a diminuição das notificações de vulnerabilidades, a seguir:

SEGURANÇA EM NÚMEROS

PROJETO **TOP5**

Projeto criado para atuar nas instituições que mais têm incidentes ou vulnerabilidades em aberto, de acordo com o volume de notificações de incidentes ocorridas no ano anterior. Dado que, nos últimos anos, o número de vulnerabilidades foi maior que o de incidentes, o TOP5 tem sido focado em cima das vulnerabilidades.

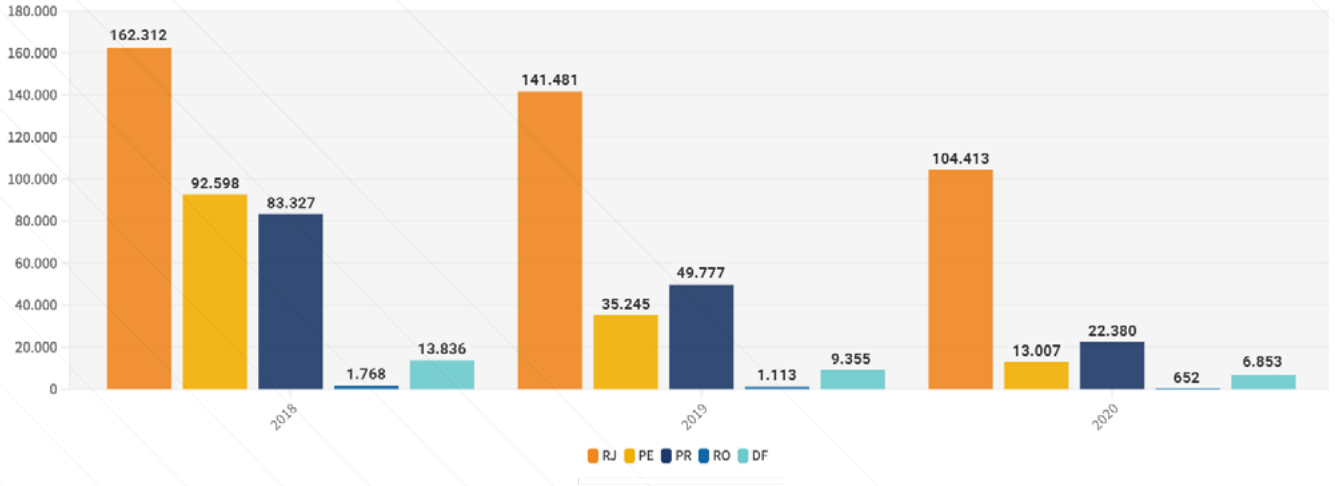
Para fins analíticos, e demonstrando também a eficácia do projeto TOP5, trazemos a seguir o recorte histórico da incidência de notificações de vulnerabilidades que foram enviadas às instituições nos 5 estados onde o projeto TOP5 foi executado. (Gráfico M).

Como reforçamos no início deste capítulo, a diminuição das notificações de maneira geral ocorreu ao longo dos últimos anos expressivamente, devido a uma série de iniciativas realizadas em conjunto com as áreas da RNP, que serão melhor comentadas no capítulo [Atualize-se].

O MÉTODO: são identificadas as **cinco instituições mais notificadas em cada uma das cinco regiões do país, e as cinco categorias de vulnerabilidades mais notificadas entre elas,** e com base nisso, é realizado um acompanhamento técnico para a aplicação das correções necessárias, um trabalho a quatro mãos com a instituição.

Uma vez aplicadas as correções, tanto a vulnerabilidade deixa de ser detectada e reportada, como também incidentes de segurança, relacionados a elas, deixam de existir.

GRÁFICO **M** **NÚMERO ABSOLUTO DE NOTIFICAÇÕES DOS 5 PRIMEIROS ESTADOS COM MAIS NOTIFICAÇÕES NO ANO**



05

Atualize-se

INICIATIVAS INTERNAS

IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER E RECUPERAR

Tecnologia

RNP ADERE AO SIRTFI

A RNP aderiu e se autodeclarou SIRTFI, uma ação de grande relevância, relacionado ao serviço CAFe e que em muito se adapta à LGPD. O que significa a autodeclaração SIRTFI? O SIRTFI é um *framework* que estabelece uma rede de confiança para o tratamento de incidentes de segurança entre os membros das diversas redes federadas, como a CAFe. A autodeclaração ocorre após a instituição atender uma série de requisitos de segurança do *framework*. Com essa ação, a RNP elevou seu nível de maturidade em segurança atendendo a exigentes padrões internacionais de segurança. Essa medida reflete mais segurança aos milhões de alunos e pesquisadores que utilizam a CAFe para acesso aos acervos e sistemas de diversas instituições nacionais e internacionais.

Primeiro, para quem não está familiarizado com o termo, CAFe significa Comunidade Acadêmica Federada, um serviço oferecido e mantido pela RNP que proporciona aos seus usuários uma solução única de acesso e gerenciamento de identidade para centenas de serviços web, oferecidos pelas instituições do Sistema RNP e de muitas outras instituições em todo o mundo, eliminando a necessidade de diversos cadastros e senhas de acesso.

INICIATIVAS INTERNAS

IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER E RECUPERAR

Tecnologia

MANRS E RPKI

Outro destaque, em consonância com o anterior, é que a RNP aderiu ao Mutually Agreed Norms for Routing Security (MANRS) e ao Resource Public Key Infrastructure (RPKI).

Atualmente, é apoiada por um grande número de provedores de internet no mundo todo e define um conjunto de práticas para aumentar a segurança, e facilitar a validação de informações de roteamento por outras redes em escala global, essas práticas dividem-se em: filtragem, *anti-spoofing*, coordenação e validação global.

O MANRS é uma comunidade comprometida em tornar a infraestrutura de roteamento global mais robusta e segura. A iniciativa é apoiada pela Internet Society (ISOC) e oferece suporte para reduzir as ameaças de segurança mais comuns em roteamento.

O Resource Public Key Infrastructure (RPKI) um sistema de certificação de recursos, que valida os anúncios de roteamento IP de origem e permite evitar ataques de segurança de sequestro de bloco, conhecidos como *hijacking*, está entre as iniciativas de 2020, pois a RNP atingiu um importante marco no projeto RPKI com o registro de todos os seus 39 blocos IP, na infraestrutura RPKI mundial.

INICIATIVAS INTERNAS

IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER E RECUPERAR

Tecnologia

CICLO DE DESENVOLVIMENTO SEGURO

A RNP atualiza sua esteira de desenvolvimento de software, trazendo ganhos significativos em automação e principalmente segurança. A solução utilizada para fornecer a base da codificação das aplicações para os arquitetos de software sofreu atualizações importantes, incorporando o *know-how* de segurança implementado no projeto Alunos Conectados.

Cabe ressaltar entre os destaques o aprimoramento da solução App Starter, utilizada para fornecer a base da codificação das nossas aplicações aos nossos arquitetos de software. O fato se dá, pois, em 2020, foi incorporado à aplicação todo *know-how* de segurança implementado no projeto Alunos Conectados, que será melhor explorado adiante. Dessa forma, a partir de uma série de aprendizados diretamente ligados à complexidade do projeto citado, a esteira de desenvolvimento das nossas soluções foi atualizada trazendo ganhos significativos em automação e principalmente segurança, pois permite que uma série de camadas de proteção e segurança com padrões globais estejam codificadas desde o início do desenvolvimento de todas as aplicações.

O Projeto Alunos Conectados foi desenvolvido pela RNP, atendendo uma demanda do Ministério da Educação de desenvolver uma plataforma para fornecer acesso à internet aos 400 mil alunos do ensino superior no país que estão em situação de vulnerabilidade socioeconômica, uma importante ação de política pública.

INICIATIVAS INTERNAS

IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER E RECUPERAR

Tecnologia

PROJETO FTS

A Gerência de Operações de Redes da RNP (GO), num trabalho conjunto com o CAIS, GER e os PoPs finalizou a primeira fase do projeto Força Tarefa de Segurança (FTS). O projeto tem por objetivo aumentar a segurança nos componentes de rede que formam o *backbone* da RNP, a rede Ipê. Nessa fase, foram mapeadas e corrigidas importantes vulnerabilidades em diversos PoPs do *backbone*. A iniciativa formou um grupo de especialistas de redes e de segurança que desenvolveu e aplicou técnicas de *hardening* nos equipamentos, além disso, o grupo gerou uma série de guias para uso das instituições do Sistema RNP. O projeto foi um sucesso devido ao engajamento, dedicação e sinergia entre as equipes envolvidas e resultou na mitigação de 93,99% das vulnerabilidades de segurança encontradas nos equipamentos dos PoPs.

2020:

981 VULNERABILIDADES IDENTIFICADAS E 922 (93,99%) CORRIGIDAS

Principais vulnerabilidades avaliadas, revisadas e corrigidas quando necessário:

1.	Gerência web: acesso aos roteadores através da interface gráfica, disponível através da Internet;
2.	Acesso aos roteadores via Telnet, deveria ser desabilitado e sem acesso através da Internet;
3.	Versão antiga ou má configuração do *SSH*;
4.	Permissões de usuários padrão pelo fabricante e/ou usuários que não mais deveriam ter acesso ao ativo;
5.	Disponibilização do servidor *NTP* publicamente e mal configurado (disponibiliza sincronização de data/hora com outros serviços e servidores);
6.	Configuração padrão e disponibilização através da Internet do *SNMP* - serviço utilizado para monitoramento dos ativos de TIC;
7.	Roteador sem configuração de *antispoofing*, permitindo forjar os endereços de origem e destino, facilitando um ataque de negação de serviço;
8.	Configuração mínima ou incompleta do *firewall*, permitindo acessos maliciosos.

INICIATIVAS INTERNAS

IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER E RECUPERAR

Pessoas e Processos

COFRE DE SENHAS, MAC WIFI E IMPRESSÃO POR APROXIMAÇÃO

Três outras iniciativas que refletem a constância no aprimoramento dos processos de segurança tiveram resultados relevantes em 2020: A expansão do uso de cofre de senhas — usado pelos administradores de ambientes e serviços de TIC — permite maior controle e rastreabilidade no uso de contas privilegiadas. Atualmente mais de 70 usuários são geridos por essa solução; A primeira fase do MAC Wi-fi, que permitiu maior visibilidade e rastreabilidade nos acessos às redes wi-fi nas dependências da RNP; por fim, através do uso de *RFID*, foi implantada a impressão por aproximação, o que contribui para diminuir a exposição de informações impressas nas dependências da RNP. Na solução adotada, a impressão de um colaborador é liberada mediante a identificação do mesmo por aproximação.

GAMIFICAÇÃO

Na busca de uma melhor forma de se conectar às pessoas para disseminar e ganhar aderência ao cumprimento de boas práticas na segurança da informação, houve uma mudança na estratégia de conscientização de todos os colaboradores da RNP. Instituiu-se a gamificação como estratégia para maior engajamento dos assuntos relacionados à segurança da informação. Houve então, uma mudança na forma como os funcionários acessam os conteúdos, estrategicamente compartilhados e que ficam disponíveis para o acesso no momento em que se preferir, o que permite maior ganho de flexibilidade para as equipes. Além disso, por meio da gamificação há maior aderência e engajamento para o fortalecimento da cultura de segurança corporativa. Ao final, o colaborador ainda é recompensado pelas tarefas concluídas.

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

ALUNOS CONECTADOS

O Alunos Conectados é uma plataforma desenvolvida pela RNP que viabiliza o repasse de créditos de pacotes de dados de telefonia móvel ou chips de pacotes de dados para alunos do ensino superior federal em situação de vulnerabilidade socioeconômica, para garantir o acesso à educação durante o período de pandemia. Considerando a relevância do projeto para a sociedade, foram implementados controles de segurança e privacidade desde a concepção do projeto, foram implementados critérios rígidos de segurança na arquitetura da plataforma e ferramentas de segurança e qualidade durante o processo de desenvolvimento da mesma, além das ações já presentes de análises de segurança, gerenciamento de vulnerabilidades com foco em aplicações web e adequação à Lei Geral de Proteção de Dados — (LGPD).

ICPEdu - Certificado Pessoal

A Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) é o serviço de certificação digital oferecido pela RNP, que provê infraestrutura para a emissão de certificados digitais e chaves de segurança. Em 2020, a RNP lançou a modalidade da ICPEdu de Certificado Pessoal. O Certificado Pessoal é a identidade virtual gratuita, emitida online e que pode ser usada para validar a identificação de usuários em diversos procedimentos digitais, como assinaturas eletrônicas, cifragem de documentos e fazer login em sistemas eletrônicos específicos. O certificado pessoal ICPEdu é um importante serviço de gerenciamento de identidade e segurança oferecido pela RNP e que pode ser usado por mais de 4,5 milhões de alunos, professores, pesquisadores e colaboradores que utilizam a CAFe.

DIPLOMA DIGITAL

É considerado um marco na transformação digital para alunos de Instituições de Ensino Superior (IES). A RNP desenvolveu o serviço em conjunto com o Laboratório de Aplicações de Vídeo Digital (Lavid) da Universidade Federal da Paraíba (UFPB) uma solução tecnológica que permite a emissão e autenticação dos diplomas acadêmicos em formato digital.

Desta forma, além de desburocratizar o processo de geração do diploma, a tecnologia proporciona mais agilidade e segurança aos alunos e Instituições de Ensino Superior. Além de permitir a agilidade e transparência também é uma solução mais sustentável resultando em mais economia e fácil acesso.

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

SISU NA NUVEM

O Sistema de Seleção Unificada (SiSU) é um dos processos seletivos do Ministério da Educação e uma das principais formas de ingresso à educação superior federal, utilizando as notas do Exame Nacional do Ensino Médio (Enem). Trata-se do sistema informatizado do MEC por meio do qual instituições públicas de ensino superior oferecem vagas a participantes do exame e os aspirantes a alunos selecionam suas opções de ingresso. Em 2020, em um projeto coordenado pela RNP, o sistema foi migrado para a nuvem, o que provocou melhorias estruturais significativas no sistema, relacionadas à capacidade e disponibilidade, além de novas funcionalidades, como a possibilidade de acesso via celular ou tablet. O SiSU na nuvem foi construído em uma tecnologia que permite que as inscrições sejam feitas por aparelhos mobile.

Qualquer consulta por qualquer estudante em qualquer lugar do país pode ser feita por celular ou tablet, permitindo assim maior rapidez e simplicidade na consulta de vagas por meio do sistema de busca.

No que tange à segurança, foi desenvolvido uma arquitetura segura para suportar os requisitos de disponibilidade, confidencialidade e integridade das informações processadas. Com isso, o MEC pode usufruir de uma infraestrutura resiliente, elástica, escalável, estável, ágil além de segura, fornecen-do assim 100% de disponibilidade de acesso para os usuários na segunda edição do processo.

O resultado dessa mudança de tecnologias e abordagens foi um sucesso que será perpetuado para as próximas edições do SiSU.

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

APOIO NA ADEQUAÇÃO À LGPD

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro dando ainda mais destaque à importância da privacidade e do uso responsável dos dados pessoais dos cidadãos no Brasil. No cumprimento de seu papel de apoiar as instituições do Sistema RNP, a RNP passou a ofertar apoio metodológico, consultorias e capacitações para ajudar instituições parceiras na adequação às novas normas. Foram realizados uma série de encontros em webinares e reuniões online para a troca de conhecimento e compartilhamento de artefatos, políticas e orientações às entidades que integram o Sistema RNP, sem qualquer custo adicional ou necessidade de contratação, para auxiliar com essa questão.

A RNP desenvolveu também um e-book 03 exclusivo e gratuito, que conta o que muda com a LGPD, as obrigações das instituições, quais sanções para quem não as cumprir e alguns passos fundamentais para a adequação, segundo o Método LGPD para a RNP.

Podemos destacar ainda a criação do Grupo de Interesse Especial (SIG, no inglês) LGPD. Esta iniciativa faz parte do Programa LGPD da RNP. Trata-se de um fórum que reúne representantes de 23 instituições convidadas da comunidade de ensino e pesquisa (17 instituições associadas e 6 organizações privadas).

O SIG visa discutir tópicos relacionados aos temas: privacidade de Dados Pessoais e Lei Geral de Proteção de Dados Pessoais (LGPD). É um espaço que promove fortemente a troca de experiências visando apoiar as instituições participantes no desafiador processo de adequação à LGPD. Além disso, o SIG tem se tornado um instrumento chave na construção colaborativa e validação do chamado Método LGPD para RNP, citado anteriormente.

Em dezembro de 2020, o SIG LGPD@RNP registrou a participação ativa de: 15 instituições associadas e 05 instituições privadas. Foram também capacitadas 462 pessoas no curso LGPD, na prática, envolvendo cerca de 100 instituições do Sistema RNP e quase todas as áreas da RNP.

03

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

POLÍTICAS DE SEGURANÇA E DE PRIVACIDADE DO SISTEMA RNP

A RNP publicou em 2020, duas importantes políticas para o Sistema RNP: a Política de Segurança da Informação do Sistema RNP [04] e a Política de privacidade do Sistema RNP. [05]
Considerando a interconectividade entre as instituições, o compartilhamento de recursos e infraestruturas e visando o crescimento individual dessas instituições, os documentos estabelecem as diretrizes dos referidos temas a serem adotados por todas as instituições que compõem o Sistema RNP, de forma a aumentar o nível de maturidade do Sistema RNP na totalidade.

As políticas estão disponíveis no site da RNP. [06]

RNPSeg

O evento RNPSeg, realizado pelo CAIS, é voltado para os gestores executivos e tomadores de decisão de TIC e segurança das instituições que compõem o Sistema RNP. O objetivo é promover um espaço de interação e reflexões estratégicas sobre a segurança da informação no cenário internacional e nacional, a partir da perspectiva de gestores e executivos com grande referência na área.

Em 2020 foi realizada a segunda edição do evento, no mês de novembro, em formato 100% online e com o tema a "Resiliência e Continuidade de Negócios", assistido ao vivo por mais de 200 pessoas, no canal da RNP no YouTube. [07]

DISI

O Dia Internacional de Segurança em Informática (DISI) é realizado anualmente desde 2005 pela Rede Nacional de Ensino e Pesquisa (RNP), por meio do CAIS, em parceria com importantes organizações nacionais e de outros países. Reúne especialistas para compartilhar seus conhecimentos e, dessa forma, conscientizar usuários sobre o uso seguro da internet. O público-alvo é o usuário final de computadores, e o objetivo é conscientizar a sociedade quanto ao uso seguro da internet e tecnologias.
Em março de 2020, em sua primeira edição digital, o DISI teve como tema: "Quem sou eu na internet?". O evento contou com a participação de Marcelo Tas, jornalista e comunicador, Cristina Sleiman, especialista em Direito Digital, e Anchises de Moraes, ciberevangelista. O evento foi acompanhado ao vivo por mais de duas mil pessoas em 10 países e teve alcance de 5 milhões de pessoas nas redes sociais. Assista aqui!

04
05
06
07

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

PARCERIA COM A EMBRAPII

A RNP conduziu com a Empresa Brasileira de Pesquisa e Inovação Industrial (EMBRAPII), um projeto voltado à estruturação e ampliação do arcabouço normativo de segurança da informação e Plano Diretor de TIC da instituição. Também foram realizadas ações relacionadas à continuidade de negócios e conscientização dos colaboradores.

PARCERIA COM A EBESERH

Responsável pelo gerenciamento dos 40 hospitais universitários existentes no Brasil, A Empresa Brasileira de Serviços Hospitalares (EBSERH) contou com a RNP para importantes ações de segurança da informação, incluindo a estruturação da Equipe de Tratamento de Incidentes de Segurança de Rede, aprimorando a governança de segurança da informação da instituição com políticas, processos e procedimentos integrados entre as unidades.

WEBINARES, WTRS E WORKSHOP

Uma série de eventos online foram realizados em 2020 com o intuito de disseminar e fortalecer a cultura de segurança da informação. Destacam-se duas dessas iniciativas:

Webinares: Série de conversas que reuniram especialistas e técnicos em torno de temas relevantes e com acesso gratuito a todos.

Mais informações na próxima página. >>>>>>>>

WTRs: evento de capacitação técnica dos Pontos de Presença da RNP em cada estado. Contou em 2020 com palestras do CAIS focadas em segurança e também um Workshop “Identificando e Mitigando Ataques de Negação de Serviço”. Massificadas em 2019, essas ações foram migradas em 2020 para o formato online.

INICIATIVAS PARA A COMUNIDADE

MARCOS EM 2020

Projetos e Eventos

WEBINARES

TÍTULO	DATA
TROCANDO IDEIAS SOBRE SEGURANÇA COM CAIS E CONVIDADOS.	13/04/2020
CIBERSEGURANÇA E O NOVO CORONAVÍRUS: PRESENTE E FUTURO	14/04/2020
SEGURANÇA NA INFRAESTRUTURA DAS INSTITUIÇÕES	15/04/2020
SEGURANÇA E MELHORES PRÁTICAS DO MCONF	22/04/2020
COLOQUEI MEUS SERVIÇOS NA NUVEM, ENTÃO AGORA ESTOU SEGURO?	28/08/2020
IMPLEMENTAÇÃO DE SEGURANÇA NA NUVEM	03/09/2020
ATAQUES DE NEGAÇÃO DE SERVIÇO - DDoS	17/09/2020
TOP5 VULNERABILIDADES TÉCNICAS EM 2020	05/11/2020
VOCÊ CONHECE OS RISCOS DA SUA ORGANIZAÇÃO?	08/11/2020
PROGRAMA LGPD	19/11/2020

06

Artigo

ARTIGO

A CIBERSEGURANÇA DA RNP E O ANO DE 2020

Por, Eduardo Grizendi
Diretor Executivo de Engenharia e Operações da RNP

Junto com os imensos benefícios da Internet vieram os grandes problemas com ela. Simples assim, mas ao mesmo tempo, tão amplo, intenso, complexo e doloroso, também assim.

Os problemas com a segurança da informação e com a privacidade e proteção dos dados, estão entre estes grandes problemas que ela nos trouxe. Os ataques cibernéticos, o vazamento e roubo de dados, a sua falta de proteção, a usurpação dos dados pessoais e seu desrespeito quanto à sua privacidade, as *fake news*, o preconceito e a incitação à violência pela Internet, enfim, todos estes malefícios que ela nos trouxe, estão conosco. Como combatê-los? O que podemos fazer para reduzir estas atividades na Internet, minimizando seus impactos, se não podemos assegurar sua inexistência ou a segurança e proteção total contra eles?

Por trás destas atividades, existem estratégias. Ataques, como os DDoS - *Distributed Denial of Service*, às vezes são usados para distrair as operações de segurança cibernética de uma organização, enquanto outras atividades criminosas, como roubo de dados ou infiltração de rede, estão em andamento. Como identificar estas estratégias e estabelecer contra estratégias para eliminá-las?

Além do que devemos fazer, em nossas instituições, o que o Estado precisa fazer, e em muitos países, inclusive o Brasil, já estão fazendo, para isto? Regulações de segurança e de privacidade de dados são obviamente importantes para combatê-las. Uma delas, a LGPD – Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, criada para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, alterou alguns artigos do Marco Civil da Internet e estabeleceu novas regras para empresas e órgãos públicos no que diz respeito ao tratamento da privacidade e segurança das informações de usuários e clientes. Ela entrou em vigor em

ARTIGO

A CIBERSEGURANÇA DA RNP E O ANO DE 2020

Por, Eduardo Grizendi
Diretor Executivo de Engenharia e Operações da RNP

setembro de 2020, porém, devido à pandemia, por força da Lei 14.010, de 10 de junho de 2020, as sanções entrarão em vigor somente a partir de 1º de agosto de 2021. Em 2020 a RNP, neste contexto, iniciou o desenvolvimento de uma metodologia de adequação à esta lei, para si e para suas instituições usuárias, já sendo aplicada em um Projeto Piloto, apoiado pela criação e posto em marcha do SIG-LGPD@RNP, com encontros virtuais sendo realizados periodicamente.

O próprio Marco Civil da Internet, Lei n° 12.965, sancionada em 23 de abril de 2014, já regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

No entanto, a invasão do Capitólio dos Estados Unidos, ocorrida em 6 de janeiro de 2021, incitado pelo Presidente Trump em suas redes sociais, teve resposta, primeiro do Facebook e depois do Twitter, que o "descodificaram", como Ben Thompson descreveu em seu artigo *Internet 3.0 and the Beginning of (Tech) History,* postado em seu blog em 12 de janeiro de 2021, "um dia depois, Apple, Google e Amazon expulsaram Parler, outra rede social onde apoiadores de Trump se reuniram e em parte planejaram a ação de quarta-feira, fora de suas App Stores e serviço de hospedagem, respectivamente, eliminando efetivamente o serviço". Segundo ele, "a ação coletiva da tecnologia em resposta aos eventos da última quarta-feira foi uma solução exclusivamente americana para a crise".

O aprendizado disto é que o mundo todo e, naturalmente, nós brasileiros, não devemos esperar pelas ações voluntárias de Big Techs. Em entrevista ao Tele.Síntese, agora em 19 de janeiro de 2021, Pablo Ortellado, professor de Gestão de Políticas Públicas da Universidade de São Paulo, comentou que o banimento do então Presidente Trump das redes sociais constituiu uma censura privada.

ARTIGO

A CIBERSEGURANÇA DA RNP E O ANO DE 2020

Por, Eduardo Grizendi
Diretor Executivo de Engenharia e Operações da RNP

Isso porque “as regras da comunidade não foram aplicadas de maneira uniforme, com sanções sucessivas que culminassem na suspensão de sua conta”. O professor defende que as mídias sociais deixem transparentes suas regras e diretrizes, bem como a escala de sanção. Já a médio prazo, segundo ele, “é preciso uma regulação do Poder Público sobre as plataformas, pois, argumenta, elas se transformaram em “espaço público”.

Assim, por lei e dentro de nosso legislativo e executivo, pela governança exercida pelo CGI – Comitê Gestor da Internet, no Brasil, e por regras e diretrizes transparentes das redes sociais, nós, como sociedade, é que devemos nos municiar e nos proteger através destas regulações para que fatos como este não ocorram.

Mas ainda que estas regulações – leis, regulamentações, diretrizes, etc., sejam importantes, a ampla sensibilização, a massiva capacitação e o aumento da resiliência e a intensidade das atividades de Segurança da Informação, Proteção e Privacidade de Dados, são, na verdade, a base para combatê-las.

Como exemplo de estratégia para o aumento da resiliência e da intensidade das atividades de Segurança da Informação, a RNP, foi aceita no fim de 2019, como membro da iniciativa MANRS - *Mutually Agreed Norms for Routing Security,* uma comunidade comprometida em tornar a infraestrutura de roteamento global mais robusta e segura. A iniciativa é apoiada pela Internet Society (ISOC) e oferece suporte para reduzir as ameaças de segurança mais comuns em roteamento. Atualmente, a MANRS é apoiada por um grande número de provedores de internet a nível mundial. Ela define um conjunto de práticas para aumentar a segurança, e facilitar a validação de informações

ARTIGO

A CIBERSEGURANÇA DA RNP E O ANO DE 2020

Por, Eduardo Grizendi
Diretor Executivo de Engenharia e Operações da RNP

de roteamento por outras redes em escala global. A partir daí a RNP vem trabalhando intensamente para seguir as recomendações da MANRS em quatro conjuntos de ações: filtragem, *anti-spoofing*, coordenação e validação global, integrando-se a ele, se juntando na colaboração entre os participantes e no aproveitamento de suas melhores práticas.

Em 2020, o foco do trabalho foi a melhoria do *anti-spoofing* para o aumento da segurança da rede acadêmica, a implementação do *RPKI* e o *BGP* com validação de origem usando certificados, que é a quarta ação sugerida pelo MANRS em 2020. Em dezembro de 2020 conclui uma Força-Tarefa de Segurança (FTS), onde foi possível mitigar 93,99% das vulnerabilidades de segurança encontradas em equipamentos de sete PoPs – Alagoas, Rio Grande do Norte, Distrito Federal, Santa Catarina, Pará, Piauí e Pernambuco. Além disso, dos 187 dispositivos auditados, 104 deles foram atualizados para versões de software mais atuais.

A força-tarefa envolveu 22 pessoas, entre elas analistas da GO, do CAIS e dos PoPs e, por causa da pandemia, alguns obstáculos adicionais precisaram ser superados, como por exemplo a ausência de suporte técnico nas instituições. Ao todo, foram 981 brechas de segurança identificadas, e 922 delas corrigidas, entre elas o controle de acessos não autorizados, problemas em criptografia, atualização de sistemas operacionais e mecanismos *anti-spoofing* e anti-looping.

Finalmente, a sensibilização e a capacitação também foram priorizadas pela RNP. O Dia Internacional de Segurança em Informática – DISI 2020, evento ocorrido em 13 de março de 2020, levantou o debate sobre segurança e educação digital, reunindo em uma roda de conversa o jornalista e comunicador Marcelo Tas, a advogada e educadora digital Cristina Sleiman, e o ciber-evangelista Anchi-

ARTIGO

A CIBERSEGURANÇA DA RNP E O ANO DE 2020

Por, Eduardo Grizendi
Diretor Executivo de Engenharia e Operações da RNP

ses Moraes, teve um público de cerca de 2 mil acessos simultâneos, na transmissão online. Também o RNPSeg, evento da RNP ocorrido em 11 de novembro de 2020, promovido pelo CAIS - Centro de Atendimento a Incidentes de Segurança, exclusivo para gestores executivos de Segurança da Informação e de TI (C-Level), promoveu reflexões estratégicas para o setor de cibersegurança, em torno do tema do evento - Resiliência e Continuidade de Negócios, a partir da perspectiva de gestores de referência nacional.

A ESR – Escola Superior de Redes, no ano de 2020, desenvolveu a maioria de sua capacitação, à distância, transpondo a oferta de cursos presenciais para EaD de 95% do portfólio, em 149 turmas realizadas, totalizando 3.218 alunos capacitados em 2020. O planejamento inicial, naturalmente que sem a pandemia do Covid-19, era de capacitar 2.500 alunos, realizando 85% das turmas na modalidade presencial e 15% em EaD. Dentre estes cursos, destacam-se os de Governança de TI relacionados à segurança da informação, proteção e privacidade de dados e os específicos de Segurança da Informação, propriamente ditos, incluindo os de Teste de Invasão de Aplicações Web, Tratamento de Incidentes de Segurança e Engenharia Reversa de Código Malicioso.

Enfim, 2020 foi mais um ano intenso de atividades relacionadas à cibersegurança na RNP. E certamente 2021 não será diferente disto.

07

Tendências

OPORTUNIDADES E DESAFIOS

Neste capítulo coloca-se o desafio de apresentar temas e circunstâncias que, à luz da análise de cenários e pontos de vista de diversos especialistas de segurança, estima-se destacar no ano que se inicia. Essa tarefa é desafiadora e buscou afastar-se de especulações frágeis, mantendo o compromisso do relatório de oferecer informações relevantes sobre segurança.

PRINCIPAIS TENDÊNCIAS PARA 2021:

CONFIANÇA ALGORÍTMICA E SEGURANÇA COGNITIVA

Esses temas seguirão ganhando espaço e aplicação, uma vez que a confiança cognitiva visa tratar de uma maneira eficiente a segurança e privacidade necessária decorrente do aumento da exposição de dados, de notícias e vídeos falsos e do uso tendencioso da inteligência artificial. Fazem parte desta tendência a proteção dos dados, a garantia de procedência de ativos com o uso de *blockchain*, a identidade e autenticação de pessoas e coisas. Já a segurança cognitiva, com a integração da inteligência artificial para a prevenção, detecção e resposta de incidentes de segurança. O aumento da complexidade dos ambientes e também da quantidade de dados para análise faz com que o aprendizado contínuo com algoritmos de inteligência artificial possibilite não somente a detecção mais assertiva de ataques, como também possibilita uma resposta mais rápida que limita ataques em andamento.

IDENTIDADES DIGITAIS

Aumento do abuso de identidades digitais, com as pessoas sendo cada vez mais o alvo dos ataques, seja para o furto das suas credenciais de acesso, ou para usurpação de identidades a partir do uso de dados pessoais vazados para a criação de credenciais falsas. A identidade digital é o nosso passaporte para o acesso aos serviços digitais, com as validações da identidade sendo feitas pela autenticação, como a senha ou a biometria.

OPORTUNIDADES E DESAFIOS

BLOCKCHAIN

O aumento do uso de *blockchain* possui um papel tecnológico importante para a evolução da confiança e da reputação digitais, principalmente para um mundo virtual mais descentralizado e seguro. Há mecanismos de segurança que podem tirar proveito das características do *blockchain*, como a identidade digital semi soberana, verificações de integridade, validação de procedências e segurança de mensagens privadas, por exemplo.

USO INTENSIVO DA NUVEM, INCIDENTES E FALSA SENSAÇÃO DE SEGURANÇA

O uso da nuvem é um recurso presente nos ambientes empresariais há anos, porém tornou-se fundamental em 2020, deixando de ser um debate de "se" será utilizado para "quando" será implementado. Nesse contexto, faz-se importante uma observação, que trata da falsa sensação de segurança que a nuvem pode gerar tanto para o usuário, quanto para o administrador. É comum o pensamento de que estar na nuvem é estar seguro, pois, os ataques estão mais no nível da aplicação do que de *datacenter* e da rede. O que não é uma regra absoluta, uma vez que o provedor e o administrador devem seguir, manter e garantir o cumprimento de boas práticas em segurança da informação. Sendo assim, é importante considerar a gestão da segurança de ponta a ponta do ambiente hospedado na nuvem.

AUMENTO DO USO DA SEGURANÇA EM NUVEM

Incluindo segurança de conexões e acesso remoto ou Secure Access Service Edge (SASE), que considera a distribuição e a necessidade de tratar os dispositivos como de confiança zero (*zero trust network access*) e o uso de mecanismos de virtualização de redes. Necessidade de controle de acesso mais adequado ao ambiente de múltiplos provedores de nuvem e necessidade de proteção de dados. Um dos caminhos é o uso de *security brokers*.

GCN: AUMENTO DE MATURIDADE E DESMISTIFICAÇÃO

A A Gestão de Continuidade de Negócios é uma medida antiga que vem sendo cada vez mais apontada como essencial na construção de uma empresa com solidez de mercado e perenidade. A pandemia instalada em 2020 forçou as instituições a "arrumarem um jeito" de continuar operando. Elas tiveram que adaptar processos, tecnologias e até alguns modelos de negócio. Esse fenômeno provocou uns "primeiros passos" das instituições mais imaturas no tema, que seguirão em 2021 evoluindo nele. A necessidade de adaptação como fator decisivo para a existência de várias instituições acabou por desmistificar a GCN como algo grandioso, caro e complexo, elas percebem ser possível começar com o básico e ir evoluindo conforme nível de maturidade e apetite a riscos.

OPORTUNIDADES E DESAFIOS

MAIOR POPULARIZAÇÃO DO PRIVACY BY DESIGN E DEVSECOPS

Embora seja uma metodologia da década de 90, a incorporação do *privacy by design* na legislação europeia GDPR e na brasileira LGPD provocará um aumento na popularização e aplicação dos conceitos de *privacy by design* no Brasil. Isso porque, a metodologia traz como premissa a proteção da privacidade como centro no desenvolvimento de todo produto ou serviço, o que só é benéfico a toda cadeia. A preocupação com incidentes de segurança e privacidade no cenário do desenvolvimento mitiga o impacto com os riscos causados pelo vazamento de informações. Os requisitos mínimos de segurança na entrega de softwares estão ficando cada vez mais complexos e passando a ser incorporados ao processo de desenvolvimento de forma cada vez mais relevante. A segurança no estágio inicial contribui para que as aplicações tenham um custo menor posteriormente, devido a possíveis explorações de vulnerabilidades com incidentes decorrentes desses ataques. Tradicionalmente a análise de segurança acontece ao final do processo de desenvolvimento de software. Essa integração da equipe de segurança no processo, no dia a dia do desenvolvimento, se torna cada vez mais importante passando a ser um requisito básico para uma equipe de desenvolvimento, e é aí que entra o *DevSecOps* (Desenvolvimento + Segurança + Operação).

HOME OFFICE: AUMENTO DA EXPLORAÇÃO DE VULNERABILIDADES

Uma vez que a pandemia irrompeu ou acelerou o processo de trabalho remoto nas instituições e também intensificou os modelos de negócio baseados nessa premissa, é esperado que os cibercrimes e incidentes de segurança também se foquem nesse ambiente. Entende-se que, geralmente, as redes domésticas são menos protegidas que as redes corporativas, e com os processos de negócio agora sendo processados nessas redes, o aumento de ataques seja crescente e muitas vezes efetivo.

MALWARES INTELIGENTES

Aumento de ataques por *malwares* inteligentes, que adotam técnicas avançadas de camuflagem e disseminação, incluindo o uso de algoritmos de inteligência artificial para dificultar a sua detecção e aumentar as oportunidades de contaminação dos sistemas e de ativação por engenharia social. Além disso, os *malwares* poderão tirar proveito da maior superfície de ataques, com a conexão permanente e de toda variedade de dispositivos.

08

Termos e Definições

TERMOS E DEFINIÇÕES

Backbone | A interconexão central de uma rede internet. Pode ser entendido como uma espinha dorsal de conexões que interliga pontos distribuídos de uma rede, formando uma grande via por onde trafegam informações.

CAFe | Comunidade Acadêmica Federada, serviço de gestão de identidade que reúne instituições de ensino e pesquisa brasileiras.

Cibercrime | Do inglês cybercrime, define os crimes praticados por meio da rede mundial de computadores

Cibersegurança | Proteção dos ativos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas de informação que estão interligados. De acordo com a definição proposta pela Information Systems Audit and Control Association (ISACA).

General Data Protection Regulation (GDPR) | Regulamento Geral de Proteção de Dados, em português, que regulamenta desde 2018, na Europa, a proteção dos dados pessoais, incluindo os processos de coleta, armazenamento e compartilhamento de informações.

Lei Geral de Proteção de Dados Pessoais (LGPD) | A Lei nº 13.709/2018, que regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade da pessoa natural.

Organização Social (OS) | Entidade de direito privado, sem fins lucrativos, formada por membros da sociedade civil, que visa representar seus interesses no relacionamento com a sociedade e o Estado.

Pontos de presença (PoPs) | Componente do Sistema RNP hospedado em uma Organização Usuária, instituição de educação ou pesquisa (instituição-abrigo), integrado à sua estrutura e atuante em cada Unidade da Federação que realiza a representação e a articulação institucional e a oferta de serviços do Sistema RNP. Possui papel de liderança e promoção de ações estaduais em benefício das organizações usuárias, da comunidade acadêmica e de políticas públicas. Os Pontos de Presença atuam de forma integrada entre si e com ao RNP e são corresponsáveis pela implementação dos procedimentos e tecnologias necessários ao cumprimento das Políticas da RNP.

Rede Ipê | Infraestrutura nacional de serviços avançados de redes de comunicação de dados que interliga as organizações usuárias entre si e, internacionalmente, com o sistema global de redes de pesquisa nacionais e regionais. A rede Ipê também oferece acesso de alta qualidade para a Internet, por meio de acordos de trânsito e troca de tráfego com outras redes privadas e públicas.

Segurança da Informação | A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações armazenadas ou que trafegam no Sistema RNP.

Sistema RNP | Conjunto de entidades alvo do apoio do Programa Interministerial da RNP – PRORNP regulamentado pela Portaria Interministerial nº 3825 de 12/12/2018.

09

Créditos

CRÉDITOS

Nelson Simões
Diretor-geral

Eduardo Grizendi
Diretor de Engenharia e Operações

Antônio Carlos Fernandes Nunes
Diretor de Serviços e Soluções

Emilio Tissato Nakamura
Diretor de Cibersegurança

Realização

Centro de Atendimento a Incidentes de Segurança (CAIS)

Edilson Lima
Gerente de Segurança da Informação do CAIS

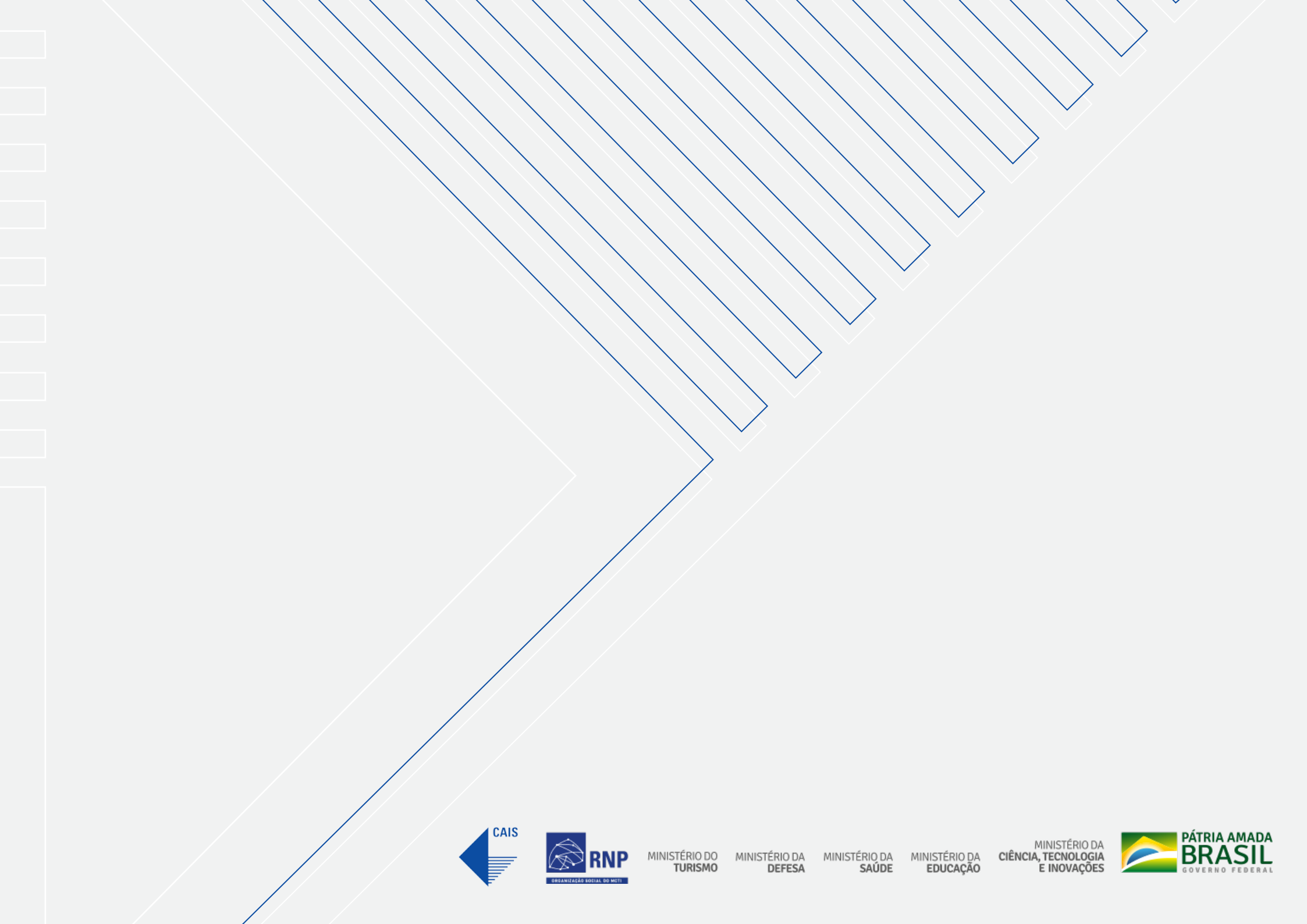
Nicole Rieckmann
Analista de Segurança da Informação do CAIS

Pesquisa, Redação, Revisão, Edição e Diagramação

Bird Comunicação Inventiva
Sobre a coordenação da Gerência de Comunicação Corporativa (GCC) e do Centro de Atendimento a Incidentes de Segurança (CAIS).

Metodologia

Durante o período de cinco semanas foram realizadas 12 entrevistas com 21 colaboradores de diversas áreas da RNP. Esse método foi reflexo do aspecto colaborativo com o qual o tema de segurança é tratado na RNP. Apesar do papel central do CAIS, a segurança da informação é desenvolvida, executada e está presente em muitas áreas da organização. Assim, foram ouvidos colaboradores das áreas: DACS, DAGSER, DAGSOL, ESR, GER, GO, GSC, GTI, PESI. Ao todo, as entrevistas resultaram em aproximadamente 20 horas de áudio com insumos que transcritos, decupados e analisados resultaram nesse relatório.


CAIS
RNP
ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
PÁTRIA AMADA BRASIL
GOVERNO FEDERAL