DOCUMENTO TÉCNICO · ESTRUTURA PROPOSTA · VERSÃO 1.0

Da detecção à mitigação

Uma arquitetura mensurável para a resposta ao DNS Abuse: proveniência das evidências, ação proporcional, prestação de contas pública e recurso rápido — concebida para ser testada, não apenas declarada.

- Publicado em 2 de agosto de 2026
- PhishDestroy Pesquisa
- Versão preliminar para consulta pública
- Não foi submetido à revisão por pares

PD-WP-2026-01 · Version 1.0 · 2026-08-02
https://phishdestroy.io/pt-br/dns-abuse-enforcement-framework

RESUMO

PROPOSTA INDEPENDENTE · NÃO É UM PROGRAMA DA ICANN

Conclusão direta. O ecossistema contratual de gTLD apresenta uma lacuna mensurável entre o uso malicioso de um domínio, validado tecnicamente, e a mitigação efetiva. Estudos publicados mostram que muitas campanhas de phishing operam por horas ou dias, enquanto os procedimentos de conformidade contratual podem se estender por períodos equivalentes a dias úteis. O modelo de cenário divulgado mostra como o atraso aumenta os retornos esperados da campanha; a faixa de 60% a 85% é a estimativa central e testável do artigo sobre os danos pós-notificação, e não uma estatística estabelecida para todas as fraudes globais. A estimativa de engenharia de US$ 100 a 150 refere-se à coleta e ao processamento inicial de um corpus definido de dados de zona, Certificado de Transparência e feeds públicos, e não ao custo total da análise jurídica ou da aplicação da lei. O artigo propõe evidências assinadas, metas de resposta mensuráveis, escalonamento automático de casos validados, medidas corretivas proporcionais, prestação de contas pública e recurso rápido. Ele não propõe conceder aos denunciantes acesso direto aos controles de suspensão de domínios.

FONTE PRIMÁRIA
Comprovado diretamente por um documento oficial ou estudo publicado.

MODELO ILUSTRATIVO
Um cálculo reproduzível cujos dados de entrada são premissas, e não médias de mercado.

PROPOSTA DE POLÍTICA
Um projeto apresentado para consulta, testes e revisão.

01 Questão de pesquisa, escopo e padrão de prova

A questão é mais específica do que “quem falhou?”: **quais atrasos observáveis entre evidências validadas e ação proporcional são evitáveis, e qual intervenção reduz os danos às vítimas sem gerar falsos positivos ou danos colaterais inaceitáveis?**

O escopo abrange o ecossistema contratual dos gTLDs: registrantes, revendedores, registradores, registros e a função de conformidade contratual da ICANN. Provedores de hospedagem, CDNs, navegadores, serviços de pagamento, plataformas de publicidade, CERTs nacionais e autoridades policiais são incluídos apenas quando afetam a cadeia de evidências ou de resposta. Os TLDs de

código de país têm governança diferente e não se presume que estejam sujeitos aos contratos gTLD da ICANN.

Situação das teses centrais

- O artigo analisa a ICANN como uma instituição de governança privada e de cumprimento contratual no ecossistema da gTLD. A ICANN não é um órgão regulador governamental nem uma autoridade de fiscalização, mas credencia registradores, celebra contratos com operadores de registro e faz cumprir esses acordos; essa competência limitada não isenta a instituição de sua responsabilidade.
- A faixa de 60 a 85% é uma estimativa quantitativa central no modelo de danos apresentado no artigo. Ela é apresentada como uma estimativa verificável, derivada de suposições explícitas e observações de casos — e não como uma estatística já estabelecida para todas as fraudes globais. A publicação de um conjunto de dados no nível dos incidentes que alinhe os registros de data e hora de detecção, notificação, mitigação e danos é o próximo passo probatório.
- O valor de US$ 100–150 é uma estimativa orçamentária de engenharia verificável para coleta contínua e triagem inicial sobre um conjunto definido de dados de zonas acessíveis, Certificado de Transparência e feed público em infraestrutura de commodities. Não se trata do custo da visibilidade global completa, revisão jurídica, recursos, alta disponibilidade ou fiscalização. O artigo, portanto, trata esse valor como uma referência a ser reproduzida com uma carga de trabalho publicada, um inventário de fontes e um registro de custos — e não como um preço universal já comprovado. Essa distinção restringe a afirmação sem eliminar a assimetria de custos que está sendo testada.
- A comparação de três semanas apresentada no artigo diz respeito à latência no atendimento, e não a um SLA universal para o bloqueio de domínios. O artigo de ICANN Perguntas frequentes sobre conformidade contratual afirma que a maioria dos tipos de reclamação pode passar por três períodos sucessivos de resposta de cinco dias úteis antes de ser encaminhada para uma instância superior, enquanto muitas campanhas maliciosas permanecem ativas por horas ou dias. Os contratos exigem, separadamente, medidas de mitigação imediatas e adequadas após a apresentação de evidências que justifiquem uma ação. [2] [4]
- No caso de um registro malicioso comprovado e com um único objetivo, `serverHold` está entre as medidas de remediação mais disruptivas no nível do DNS, pois remove a delegação da zona. Não é uma solução universal: também pode causar interrupções no e-mail, nos subdomínios e em serviços legítimos; as respostas armazenadas em cache podem permanecer até o vencimento do TTL; e serviços comprometidos ou compartilhados podem exigir medidas de mitigação mais específicas. [4] [7]

> CONTRIBUIÇÃO PARA A PESQUISA
>
> A proposta é falsificável. Um estudo piloto pode comparar as coortes de tratamento e controle quanto ao tempo até a triagem, tempo até a mitigação, indicadores de perdas de vítimas, recorrência, falsos positivos, tempo de reversão e impacto colateral.

02

O que as fontes primárias comprovam

$165.1M

Financiamento operacional da ICANN no ano fiscal de 2027

Orçamento aprovado para o ano fiscal de 2027. Escala contextual; não representa gastos com DNS Abuse. [1]

191,561

Reclamações relacionadas a phishing/spoofing no IC3 em 2025

Maior categoria de reclamações do IC3 em número; US$ 215,8 milhões em prejuízos atribuídos diretamente. [10]

24 horas

Vida útil mediana em um estudo de 2021

Resultado específico de um conjunto com 1.288 domínios de phishing; não é uma duração universal. [11]

Sem SLA fixo

Prazo universal de desativação

As alterações de 2024 exigem mitigação "tempestiva" e "adequada", não um único prazo global. [2] [3]

PROPOSTA	STATUS	O QUE SE PODE AFIRMAR
Phishing é DNS Abuse	VERIFICADO	Phishing é explicitamente uma das cinco categorias cobertas pelas alterações contratuais de 2024 aplicáveis aos gTLD. [2]
Os registradores devem agir	VERIFICADO	Os registradores devem agir prontamente quando dispuserem de evidências acionáveis de que um nome por eles patrocinado está sendo usado para DNS Abuse. [2]
Os operadores de registro devem agir	VERIFICADO	Os operadores de registro devem agir prontamente quando determinarem de forma razoável, com base em evidências acionáveis, que um nome registrado está sendo usado para DNS Abuse; a medida adequada continua dependente do contexto. [3]
`serverHold` revoga a delegação	VERIFICADO	Trata-se de um status EPP definido pelo servidor. As respostas em cache do DNS podem permanecer até o vencimento, e a ação afeta todo o domínio registrado. [7]
Todo DNS Abuse pode ser observado no CZDS ou no CT	FALSO	CZDS e Certificate Transparency são sensores valiosos, mas não oferecem uma visão completa nem em tempo real de todo uso de domínios. [8] [9]

O primeiro relatório semestral da ICANN sobre a implementação das alterações de 2024 registrou 192 investigações, mais de 2.700 domínios suspensos, mais de 350 páginas de phishing desativadas e duas notificações formais de violação contratual (Notices of Breach). Esses números não comprovam que os controles atuais sejam suficientes, mas descartam a alegação absoluta de que o sistema não age. [5]

03

Por que a latência de resposta continua sendo um tema de pesquisa válido

Algumas campanhas de phishing operam em um intervalo de tempo de horas ou dias. Bijmans et al. relataram uma duração média observada de 45 horas e uma mediana de 24 horas para 1.288 domínios de phishing em um estudo de 2021. Um estudo de 2026 sobre domínios de phishing recém-registrados relatou uma distribuição altamente assimétrica: para 14.112 domínios com tempo de vida mensurável, a média foi de 8,6 dias e a mediana, de um dia. Nenhuma das amostras pode ser generalizada para todas as classes de ameaças, mas ambas mostram por que um processo medido apenas em dias úteis pode deixar de detectar campanhas de curta duração. [11] [12]

O DESFASAMENTO TEMPORAL MEDIDO

Esses estudos não determinam a proporção do prejuízo financeiro que ocorre após a notificação, mas identificam um descompasso temporal: um processo cujas etapas iniciais de conformidade informal podem levar até quinze dias úteis não pode, por si só, servir como resposta a incidentes para campanhas com duração média próxima a um dia. O prazo de 21 dias mencionado abaixo é, portanto, um cenário de latência na conformidade, e não uma designação para um "SLA ICANN" universal.

FIGURA 1 · RESULTADO CUMULATIVO ILUSTRATIVO DA CAMPANHA

MODELO · ESPAÇAMENTO TEMPORAL DO TIPO LOGARÍTMICO

A curva ilustra o cenário descrito na Seção 4; não se trata de dados de mercado observados. O posicionamento horizontal comprime intervalos longos para facilitar a leitura. Fonte: modelo reproduzível com entradas divulgadas.

CAUTELA CAUSAL

Um tempo de vida mais curto do domínio não significa automaticamente que se evitou uma perda financeira. Os invasores podem migrar, utilizar sites comprometidos, alterar os canais de distribuição ou realizar saques antes de serem detectados. O efeito causal deve ser medido, e não inferido apenas a partir da rapidez da remoção.

04 A economia das operações fraudulentas como cenário reproduzível

O ativo economicamente relevante muitas vezes não é a taxa de registro, mas o tráfego, os materiais criativos, a infraestrutura e a confiança acumulados ao redor de um domínio. Essa premissa é plausível, mas sua magnitude varia entre operações fraudulentas. Por isso, a calculadora expõe cada dado de entrada em vez de apresentar um resultado hipotético como média observada.

DEFINIÇÃO DO MODELO

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Calculadora de cenários

Altere qualquer premissa. Os valores são meramente ilustrativos e não representam estimativas do mercado típico de phishing.

MODELO ILUSTRATIVO

Orçamento da campanha (USD)

5000

Visitas diárias

2000

Taxa de conversão das vítimas (%)

1.5

Prejuízo médio por vítima (USD)

2400

Perdas no cash-out (%)

25

Tempo de ação (horas)

24

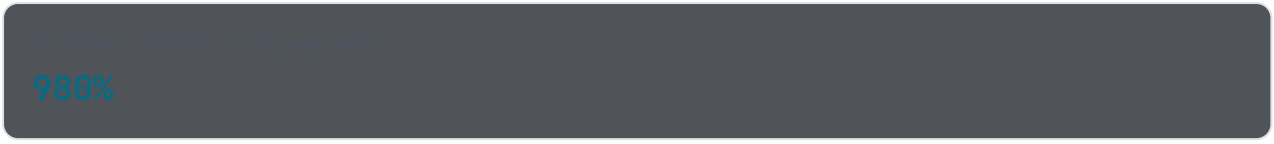
Vítimas
2,000

Vítimas recuperadas
30

Prejuízo evitado
$54,000

Prejuízo líquido
$49,000

Tempo de exposição do investimento
2.2 h



O número esperado de vítimas pode ser fracionário porque o modelo expressa um valor esperado. O modelo omite redução do tráfego, retroalimentação da detecção, migração, vítimas repetidas e distribuições de incerteza.

▶ Exibir a tabela de origem do modelo

05 Medir os danos evitáveis sem inventar precisão

A “perda após a detecção” só se torna um resultado útil se detecção, entrega e dano forem definidos de modo consistente. O timestamp de uma lista de bloqueio não prova que o registrador recebeu evidências acionáveis. Uma transação de carteira não é automaticamente atribuível a um domínio. A indisponibilidade de um domínio não identifica qual ator provocou a mudança.

Esquema mínimo de eventos

EVENTO	TIMESTAMP OBRIGATÓRIO	EVIDÊNCIA MÍNIMA
Primeira observação	`t_obs`	Sensor, hash de solicitação/resposta, método de captura, fonte de tempo.
Validação técnica	`t_valid`	Indicador reproduzível, identidade do revisor, categoria de ameaça e nível de confiança.
Notificação entregue	`t_notice`	Comprovante de entrega autenticado e versão do evidence envelope.
Confirmação pelo ator responsável	`t_ack`	ID do caso e função destinatária: host, registrador, registro, plataforma ou autoridade.
Mitigação observada	`t_mitigate`	Estado de DNS, HTTP, pagamentos ou plataforma, medido a partir de vários pontos de observação.
Recurso / restauração	`t_restore`	Fundamento da decisão, alteração das evidências e verificação da restauração.
Evento de dano	`t_harm`	Relatório da vítima sem identificação, transação atribuível ou outro indicador documentado.

MÉTRICA DE RESULTADO PROPOSTA

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

O numerador e o denominador devem seguir a mesma regra de atribuição. Os resultados devem relatar a coorte, o intervalo de confiança, a censura à direita, as fontes ausentes, o tratamento de vítimas duplicadas e a sensibilidade à janela de observação. O termo “prevenível” deve ser reservado para um desenho causal ou, no mínimo, uma comparação pareada — e não para qualquer evento após a notificação.

ESTIMATIVA CENTRAL DO MODELO · 60–85%

O artigo mantém o intervalo de 60% a 85% como sua estimativa central para a parcela de danos atribuíveis que ocorrem após a detecção e a notificação na classe de incidentes que está sendo modelada. Trata-se de uma estimativa de cenário derivada de premissas divulgadas e observações de casos — não de uma estatística medida para todas as fraudes em todo o mundo. Ela deve ser utilizada para análise de sensibilidade até que um conjunto de dados no nível do incidente alinhe observações, evidências validadas, entrega, mitigação e registros temporais dos danos. A publicação desse conjunto de dados é o teste probatório da tese, não um motivo para descartá-la.

06 O mapa institucional: a capacidade é distribuída

Nenhum agente isolado tem visão completa ou controle sobre todo o incidente. O registrador conhece a relação com o registrante; o registro controla o status dos domínios sob sua jurisdição; o host e o CDN controlam a entrega de conteúdo; os navegadores e os fornecedores de segurança controlam os avisos; os provedores de pagamento e carteiras digitais podem interromper as transferências; as autoridades podem exigir a preservação ou apreensão. A ICANN redige e faz cumprir contratos no ecossistema gTLD, mas não opera um plano de controle EPP universal.

01 · SINAL

Pesquisadores & sensores

Observam indicadores de conteúdo, infraestrutura e vítimas; preservam a proveniência.

02 · SERVIÇO

Host / CDN / plataforma

Pode remover conteúdo ou bloquear o acesso rapidamente, muitas vezes sem alterar o domínio.

03 · PATROCINADOR

Registrador

Analisa o abuso, contata o registrante e pode definir o status no lado do cliente.

04 · ZONA

Operador de registro

Controla o status do EPP definido no registro e a delegação da zona do TLD.

05 · CONTRATO

Conformidade Contratual da ICANN

Investiga a conformidade das partes contratadas; não julga cada caso de fraude.

06 · DIREITO

CERT / autoridades

Coordenam a resposta e exercem os poderes jurídicos próprios de cada jurisdição.

A capacidade distribuída não significa responsabilidade dissolvida. Um registrador patrocinador não se exime de suas obrigações contratuais ao delegar o tratamento de abusos a um revendedor; o registro controla o status do EPP definido no servidor; ICANN garante o cumprimento contratual. A trilha de auditoria deve registrar não apenas quem agiu, mas também quem recebeu evidências passíveis de ação, redirecionou o caso, deixou de responder ou deixou de cumprir uma obrigação atribuída. A autoridade legal permanece com o agente habilitado a aplicar uma medida; a responsabilização também abrange o descumprimento documentado.

Concentração de recursos e uma hipótese verificável sobre conflito de incentivos

$165.1M

Financiamento para as operações do "ICANN" no ano fiscal de 27

Foi aprovado o orçamento do cenário base para o ano fiscal de 27. [1]

≈98.1%

fluxos de receita do registro e do registrador

Aproximadamente US$ 162,0 milhões do plano de financiamento de US$ 165,1 milhões. [1]

70.7%

apenas as taxas por transação

$116.8M tied to billable domain transactions. [1]

A estrutura de financiamento está, portanto, altamente concentrada nos pagamentos das partes contratadas cujos acordos a ICANN faz cumprir, e uma grande parte varia de acordo com as transações de registro faturáveis. Isso cria uma dependência estrutural e levanta uma questão legítima de conflito de incentivos. Isso faz com que *não*, por si só, comprovam uma aplicação intencionalmente insuficiente da lei ou uma "captura regulatória" consumada. A hipótese da captura deve ser testada com base nos tempos de resposta em cada caso, nos resultados da fiscalização, nas sanções, na reincidência de abusos e no papel das partes interessadas financiadas nas decisões sobre políticas e implementação.

07 A linha de base contratual de 2024 — e o que ela não especifica

As alterações globais de abril de 2024 ao Registrar Accreditation Agreement e ao Base Registry Agreement estabeleceram obrigações expressas para mitigar DNS Abuse. Os registradores devem agir prontamente quando dispuserem de evidências acionáveis de que um nome por eles patrocinado está sendo usado para DNS Abuse. Os operadores de registro devem agir prontamente quando determinarem de forma razoável, com base em evidências acionáveis, que um nome registrado está sendo usado para DNS Abuse. Em ambos os casos, a medida adequada depende do contexto, da gravidade e do impacto colateral. [2] [3]

Três linhas do tempo que costumam ser confundidas

LINHA DO TEMPO	A QUE SE APLICA	O QUE ISSO NÃO SIGNIFICA
24 horas	Análise, nos termos da seção 3.18.3 do RAA, de denúncias bem fundamentadas de atividade ilegal («Illegal Activity») enviadas ao contato dedicado por autoridades policiais, de defesa do consumidor, quase governamentais ou similares.	Não se trata de um prazo universal de suspensão de 24 horas.
“Prontamente”	Adotar mitigação adequada depois que o limiar aplicável de evidências acionáveis for atingido.	Não é um número fixo de horas e não exige o mesmo remédio em todos os casos.
21 dias	Pode ser considerado um prazo de correção após uma notificação formal de violação contratual.	Não se trata do tempo de vida normal atribuído a todos os domínios maliciosos relatados.

Essa flexibilidade traz benefícios: um domínio universitário comprometido não deve ser tratado da mesma forma que um domínio de phishing de finalidade única recém-registrado. O problema em termos de prestação de contas é que os termos “imediato” e “adequado” são difíceis de comparar sem registros de data e hora publicados, categorias de casos e códigos de resultado. A proposta a seguir acrescenta mecanismos de avaliação e revisão, sem pretender que um único prazo sirva para todos os casos.

08 O problema dos limites: o phishing está incluído; algumas formas de fraude financeira podem não estar

Phishing está expressamente incluído na definição contratual de DNS Abuse. A fronteira mais difícil envolve sites que enganam sob um nome original em vez de se passarem por um terceiro identificável: algumas plataformas falsas de investimento, lojas fraudulentas, golpes de recuperação e esquemas para obter assinaturas de carteiras. Dependendo dos fatos, podem ser tratados como abuso de

conteúdo web, fraude contra o consumidor ou outra categoria jurídica, e não como DNS Abuse contratual.

> TERMO DE PESQUISA PROPOSTO
>
> **Verified Financial Harm Abuse (VFHA)**: uso documentado de um domínio para obter, por fraude, fundos, credenciais de pagamento, chaves privadas ou frases-semente, independentemente da falsificação de identidade de marca. VFHA não pertence à terminologia atual da ICANN e não cria, por si só, autoridade contratual.

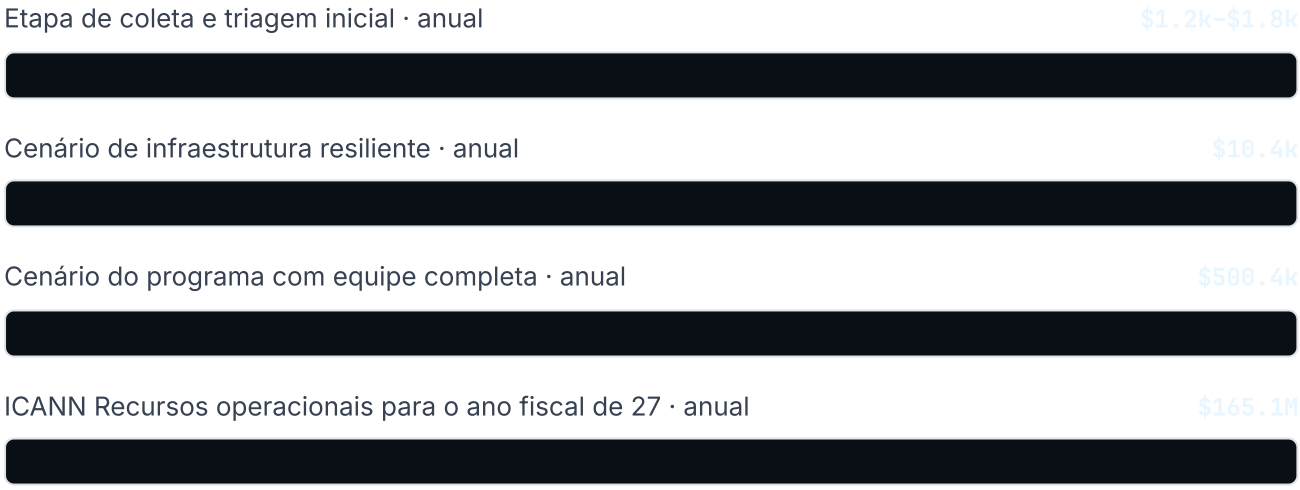
Uma consulta de política pública poderia avaliar se uma categoria estreita e amparada por evidências, como VFHA, deve integrar contratos futuros, um marco de encaminhamento intersetorial ou a legislação nacional. Qualquer ampliação deveria exigir teste preciso do dano, evidências confiáveis, remédios proporcionais, revisão jurisdicional e recurso. Rótulos vagos como “golpe” são insuficientes.

09 O que a alegação de monitoramento de US$ 100–150 por mês deve comprovar — e o que ela não pode comprovar

Um servidor padrão pode baixar instantâneos acessíveis dos arquivos de zona participantes do gTLD e calcular as alterações localmente, importar eventos selecionados do Certificate Transparency e feeds abertos, normalizar cadeias de caracteres, calcular hashes e priorizar candidatos. Trata-se de um parâmetro de referência de engenharia útil e testável — não de um “monitoramento completo da Internet”. No segundo trimestre de 2026, a Verisign relatou 401,6 milhões de registros em todos os TLDs; o CZDS abrange os arquivos de zona participantes do gTLD, e não todos os TLDs, e o CT registra certificados ou pré-certificados registrados publicamente, e não todos os domínios ativos ou maliciosos. [8] [9] [17]

CAPACIDADE	PROTÓTIPO EM INFRAESTRUTURA COMUM	SERVIÇO DE PRODUÇÃO DE INTERESSE PÚBLICO
Ingestão de zonas/CT/feeds	Viável para um conjunto definido de fontes	Coletores redundantes, contratos com fontes e monitoramento de lacunas
Triagem de strings/hashes	Viável	Avaliação comparativa, detecção de desvio, estudos de falsos negativos
Renderização do navegador	Pequeno subconjunto amostral	Frota isolada, pontos estratégicos regionais, contenção de malware
Determinação jurídica	Não incluído	Revisores qualificados, jurisdição e mapeamento de competências
Alta disponibilidade / retenção de evidências	Normalmente ausente	Assinaturas protegidas por HSM, registros de auditoria, backups e resposta a incidentes
Recursos e restabelecimento	Não incluído	Operações 24 horas por dia, 7 dias por semana, escalonamento independente e metas de atendimento

FIGURA 2 · CONTEXTO DE ORDEM DE GRANDEZA — LARGURA LOGARÍTMICA · CUSTOS NÃO COMPARÁVEIS



As larguras logarítmicas mantêm os valores pequenos visíveis. Os três primeiros valores são premissas técnicas ou programáticas divulgadas que exigem um parâmetro de referência publicado e não constituem cotações de fornecedores. ICANN O financiamento das operações é um valor verificado em escala institucional. Trata-se de orçamentos deliberadamente não equivalentes: a comparação testa se a coleta básica e a triagem representam um custo inerentemente proibitivo, e não se um programa completo de fiscalização custa US$ 100 por mês.

10 Marco proposto de resposta a abusos verificados

O marco proposto é uma arquitetura de referência, não um “interruptor de desligamento” global automático. Ele padroniza o evidence envelope, o registro de decisão e os timestamps, permitindo que o operador autorizado escolha a medida eficaz com menor impacto colateral.

01 · CAPTURA

Adquirir e preservar

Coletar relatórios e observações; gerar hash de artefatos brutos; sincronizar relógios.

02 · PROVENIÊNCIA

Normalizar as evidências

Registre a origem, o método, o histórico de manuseio e as dependências da fonte.

03 · VALIDAR

Corroborar

Reproduzir o comportamento prejudicial e identificar as evidências independentes.

04 · AVALIAR

Risco & impacto colateral

Classificar registros maliciosos, serviços comprometidos, hospedagem compartilhada e gravidade.

05 · RESPONDER

Notificar e mitigar

Designar o responsável, o prazo previsto e a medida eficaz que cause o mínimo de transtorno.

06 · REVISAR

Auditoria & recurso

Publicar metadados de resultados, medir o impacto e viabilizar reversão rápida.

Níveis de evidência

E1 **Sinal não verificado**

Informação isolada, correspondência lexical ou alegação de reputação. Adequado para observação, mas nunca suficiente por si só para justificar uma suspensão.

E2 **Comportamento reproduzido**

Captura com registro de data e hora que mostra o roubo de credenciais, a disseminação de malware ou um caminho de transação fraudulento.

E3 **Corroboração independente**

Pelo menos duas fontes genuinamente independentes ou uma prova técnica reproduzível, além de verificações de titularidade e contexto.

E4 **Confirmação qualificada**

Autoridade, serviço afetado, titular da marca ou evidências validadas de vítimas, com cadeia de custódia compatível com a privacidade.

REGRA DA INDEPENDÊNCIA

Três feeds que copiam a mesma lista negra de origem constituem uma única fonte, e não três. O gráfico de proveniência deve indicar a origem compartilhada, a sincronização e a republicação pelo fornecedor.

11 Um evidence envelope mínimo e uma API interoperável

O “API” deve criar um caso verificável e iniciar um cronômetro de resposta auditável; um denunciante não deve poder emitir um comando de suspensão diretamente. Se um caso E3/E4 se referir a um registro malicioso com finalidade única e expirar sem uma decisão fundamentada ou mitigação efetiva, o sistema o encaminha automaticamente ao operador do registro ou a outro agente com autoridade contratual ou legal. A `serverHold` O comando só pode ser emitido por um agente autorizado. A escalonamento automático e a autoridade do registro para agir no vencimento são propostas de alteração de política, e não alegações sobre autoridade existente. Cada transição de estado é assinada e anexada ao log de auditoria.

POST /V1/CASES · EXEMPLO

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Uma resposta bem-sucedida retorna o ID do caso, o ator destinatário, o nível de evidência, os erros de completude, o prazo previsto para análise e uma URL pública de transparência. Ela não deve prometer um remédio específico antes que um ator competente avalie sua competência e o impacto colateral.

12 Metas de resposta propostas, não prazos universais de desativação

As metas de nível de serviço devem distinguir *confirmação de recebimento*, *triagem*, *decisão* e *mitigação eficaz*. Isso permite medir o desempenho sem pressupor que a suspensão seja sempre o resultado correto.

PERFIL DO CASO	CONFIRMAÇÃO	META DE TRIAGEM	META DE DECISÃO	OPÇÕES TÍPICAS DE RESPOSTA
Roubo E3/E4 de credenciais de pagamento ou frase-semente por registro malicioso de finalidade única	15 min	1 h	4 h	Bloqueio de conteúdo; suspensão pelo registrador ou operador de registro, quando autorizada; alertas de navegador e pagamento.
Phishing de marca E3 ou distribuição de malware	30 min	2 h	6 h	Remoção por host/CDN, mitigação do domínio, sinkhole ou alerta conforme o ponto de controle.
Domínio legítimo comprometido ou locatário de SaaS compartilhado	1 h	4 h	12 h	Isolamento de caminho/conta e recuperação pelo proprietário; evite, sempre que possível, a suspensão do domínio registrado.
Fraude financeira com classificação contestada	4 h	12 h	24 horas	Preservação, intervenção na plataforma/pagamento, encaminhamento à autoridade competente e decisão fundamentada.
Sinal E1 ou relatório incompleto	Auto	24 horas	Nenhum até ser validado	Monitorar, complementar e solicitar comprovantes.

Essas são metas piloto. Os valores corretos devem ser calculados com base na duração observada das ameaças, no quadro de pessoal, no custo dos erros e nas restrições legais, sendo depois divulgados por meio de distribuições de cumprimento, em vez de uma única média.

13 Segurança, devido processo legal, privacidade e modos de falha

Uma resposta rápida sem medidas de proteção pode transformar dados incorretos em censura, sabotagem comercial ou interrupções na infraestrutura. Uma arquitetura adequada, portanto, trata os falsos positivos e os danos colaterais como falhas de segurança de primeira ordem.

MODO DE FALHA	CONTROLE OBRIGATÓRIO	MEDIDA AUDITÁVEL
Denúncia maliciosa contra um concorrente	Autenticação dos denunciantes, reputação das fontes, reprodução independente e sanções por abuso	Taxa de relatórios rejeitados por denunciante; casos confirmados de manipulação
Circularidade de feeds apresentada como consenso	Grafo de proveniência e deduplicação de fontes upstream	Contagem de fontes independentes antes e depois da correção de linhagem
Suspensão generalizada de domínio legítimo comprometido	Classificação da intenção de registro e preferência por mitigação no nível do caminho	Proporção de domínios comprometidos; serviços legítimos afetados
Dados das vítimas ou detalhes da exploração foram divulgados publicamente	Divulgação em níveis, supressão de informações, provas sob sigilo e prazos de retenção	Incidentes de privacidade; resultados da análise de supressão de informações
Uma ação indevida persiste	Recebimento de recursos 24/7, revisor independente e processo autenticado de restauração	Tempo mediano e no 95º percentil para reversão
Uma suspensão no nível do registro interrompe e-mail ou subdomínios	Inventário de impacto colateral, proporcionalidade do remédio e monitoramento posterior à ação	Serviços interrompidos por ação; taxa de reversão

Garantias mínimas do devido processo legal

1. O código do motivo, o nível de evidência e o responsável pela decisão são registrados para cada medida restritiva.
2. O registrante pode obter uma fundamentação compatível com a privacidade e apresentar contraevidências.
3. Os recursos de urgência são analisados por uma pessoa que não tomou a decisão original.
4. A reversão se propaga pelo mesmo canal assinado da ação original.
5. As estatísticas agregadas de erros e restaurações são públicas; as evidências confidenciais continuam sujeitas a controle de acesso.

14 De um “índice de toxicidade” a um Índice de Qualidade da Resposta que permite a prestação de contas

Uma pontuação pública atribuída a um registrador pode melhorar a prestação de contas, mas classificações simplistas são distorcidas pelo tamanho da carteira, pela cobertura dos feeds, pelo perfil da clientela e pela distinção entre registro malicioso e comprometimento posterior. Uma pontuação nunca deve justificar o bloqueio coletivo de todos os clientes de um registrador.

VETOR DE QUALIDADE PROPOSTO

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Se for necessário utilizar um índice composto para fins de governança, os pesos devem ser definidos antes da avaliação, submetidos a testes de sensibilidade e testados retrospectivamente com casos não utilizados na avaliação. Os resultados devem ser estratificados por TLD, tamanho do registrador, classe de ameaça e fonte das evidências. O resultado é um indicador de responsabilidade — e não um veredicto automatizado sobre o domínio.

15 Base Pública de Transparência sobre DNS Abuse em níveis

Um registro de transparência pode eliminar controvérsias sobre se uma notificação existiu, quando foi entregue e quais medidas foram tomadas em seguida. A publicação de todos os elementos, no entanto, poderia expor vítimas, dados pessoais, métodos de investigação e caminhos de exploração ativos. A solução é o acesso em níveis.

P **Registro público**

ID do caso, indicador, categoria ampla, timestamps principais, nível de evidência, funções dos atores, código de resultado, status do recurso e hashes dos artefatos lacrados.

C **Visão do contratante**

Evidências técnicas reproduzíveis, canal de contato, contexto colateral e instruções de preservação.

R

Visão restrita às autoridades

Dados de vítimas, atribuição financeira, material de investigações ativas e cadeia de custódia sem supressões.

Cada atualização é do tipo “somente acréscimo”, possui registro de data e hora e é assinada. As correções não apagam o histórico; elas adicionam um registro que substitui o anterior. A pesquisa pública deve respeitar as regras de retenção, impedir a identificação em massa de vítimas e oferecer reparação em caso de dados pessoais imprecisos.

16 Projeto-piloto de seis meses com avaliação pré-registrada

Um projeto-piloto útil deve ser pequeno o suficiente para ser governável e amplo o suficiente para testar a cadeia causal. Escopo sugerido: três registradores voluntários, dois operadores de registro, um parceiro de hospedagem/CDN, dois feeds independentes de pesquisa e um painel qualificado para análise de recursos. O protocolo do estudo e as definições dos resultados devem ser registrados antes da distribuição dos casos.

MÊS 1

Mapeamento de protocolos e aspectos jurídicos

Definir categorias, autoridades, níveis de evidência, avaliação de impacto sobre a privacidade e condições de interrupção.

MÊS 2

Instrumentar o processo existente

Medir timestamps e resultados de referência sem alterar o comportamento da resposta.

MÊS 3

Testar o evidence envelope

Introduzir proveniência assinada, deduplicação e classificação do impacto colateral.

MÊS 4

Testar metas de resposta

Randomizar os casos elegíveis ou usar implantação em etapas; monitorar os erros diariamente.

MÊS 5

Exercitar recursos e modos de falha

Realizar simulados de restauração, simulações de denúncias maliciosas conduzidas por um red team e auditorias dos controles de acesso.

MÊS 6

Avaliação independente

Publicar os tamanhos dos efeitos, os intervalos de confiança, os dados ausentes, os eventos adversos, os custos e os materiais de replicação.

Resultados primários do estudo piloto

- Tempo mediano e do 90º percentil entre a evidência validada e a mitigação efetiva.
- Diferença no dano atribuível após a notificação ou em um indicador pré-especificado de exposição da vítima.
- Taxa de falsos positivos, gravidade das ações indevidas e tempo mediano de restauração.
- Recorrência no mesmo registrante, no mesmo cluster de infraestrutura e na mesma campanha.
- Custo operacional direto por caso validado e por medida de mitigação eficaz.

REGRA DE DECISÃO

Ampliar somente se o projeto-piloto demonstrar mitigação eficaz substancialmente mais rápida sem exceder os limites pré-registrados de falsos positivos, incidentes de privacidade, atrasos nos recursos ou interrupções colaterais do serviço.

17 Conclusões e recomendações verificáveis

A resposta ao DNS Abuse não é um filtro puramente técnico nem um problema que uma única instituição possa resolver sozinha. Os contratos vigentes desde 2024 estabeleceram obrigações relevantes de mitigação, mas deixam ampla discricionariedade quanto às evidências, ao momento da ação e ao remédio. Essa discricionariedade é necessária à proporcionalidade; sem registros comparáveis, também dificulta a avaliação do desempenho.

1. **Padronizar o evidence envelope.** Adotar campos comuns de proveniência, timestamp e resultado entre denunciantes, registradores, registros e provedores de infraestrutura.
2. **Medir as etapas separadamente.** Publicar os tempos de confirmação, triagem, decisão, mitigação e recurso por classe de ameaça e nível de evidência.
3. **Distinguir um registro malicioso de um comprometimento.** Dê preferência à correção por meio de caminhos/contas para serviços legítimos comprometidos e reserve medidas que abranjam todo o domínio para os casos em que elas sejam proporcionadas.

4. **Testar metas de resposta em projeto-piloto.** Avaliar objetivos em escala horária para registros maliciosos de finalidade única e alta confiança, em vez de declarar um prazo universal.
5. **Publicar dados de prestação de contas compatíveis com a privacidade.** Usar um registro de transparência em níveis, com históricos assinados e evidências restritas.
6. **Avaliar o impacto causal.** Não se deve equiparar uma suspensão mais rápida à economia de dinheiro até que um estudo pré-registrado avalie os resultados relativos ao impacto sobre as vítimas e ao deslocamento.

A conclusão construtiva não é que o problema original desapareça assim que suas alegações forem matizadas. É que as alegações centrais agora podem ser testadas: a faixa de danos pós-detecção de 60 a 85% é uma hipótese quantitativa explícita; $100–150 é uma suposição orçamentária de engenharia testável para uma camada definida de sensores e triagem; e metas de resposta na escala de horas podem ser testadas para registros maliciosos de alta confiança e com finalidade única. Publique a carga de trabalho, os custos, os carimbos de data/hora e os resultados, compare-os com uma linha de base e avalie o desvio e o erro. A confirmação justificaria mudanças contratuais e nas políticas; a rejeição identificaria qual suposição falhou.

Divulgação editorial e metodológica. PhishDestroy é um projeto independente e não comercial de inteligência de ameaças. Esta publicação é uma proposta de política pública e engenharia, não aconselhamento jurídico, programa da ICANN ou artigo revisado por pares. As faixas orçamentárias identificadas como “modelos” são premissas de planejamento. As afirmações baseadas em fontes primárias estão vinculadas abaixo. Correções podem ser enviadas pelos canais de contato e de divulgação responsável do site.

PERSPECTIVA EM PRIMEIRA PESSOA · A RESPONSABILIDADE DEVE COIBIR TANTO A INÉRCIA QUANTO O EXCESSO

Um limite pessoal ao poder de fiscalização

Não estou pedindo — nem quero — acesso direto a uma ferramenta de bloqueio de domínios. Esse poder exige uma análise independente, registros públicos de auditoria, um recurso rápido e a possibilidade de reversão.

Acredito que existam muitas empresas competentes e responsáveis às quais se poderia confiar partes desse trabalho. Com base na minha experiência e no histórico que publiquei, não incluo a NameSilo nesse grupo.

Eu não aconselharia empresas americanas legítimas a confiar funções delicadas relacionadas a abusos ou segurança a prestadores de serviços específicos cujos conflitos de interesse, competência ou conduta não resistam a um escrutínio independente. Trata-se de ações documentadas, não de nacionalidade: a origem russa, por si só, não prova nada, assim como o endereço de uma empresa americana também não prova nada.

Quero justiça e responsabilização efetiva para registradores que obtiveram receita com o registro e a renovação de domínios documentados como parte de campanhas repetidas de golpes. Quando as evidências apontam, além da negligência, para uma possível facilitação consciente — seja por envolvimento operacional direto, seja atuando como intermediário informado cuja função era manter um domínio prejudicial registrado e online, apesar de repetidos avisos —, tal conduta deve ser investigada de forma independente e, se comprovada, acarretar consequências. Não apresento suspeitas como fatos comprovados; mas a condição de intermediário não deve conferir imunidade ao escrutínio.

Analisar a investigação subjacente ↗

A

Referências e notas de fonte

[1] **ICANN: Orçamento aprovado para o ano fiscal de 27 (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Fonte dos US$ 165,1 milhões destinados ao financiamento das operações do ano fiscal de 27 e composição das fontes de financiamento.

[2] **ICANN: Alteração Global de 2024 ao Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Fonte contratual principal das obrigações dos registradores relativas ao DNS Abuse.

[3] **ICANN: Alteração Global de 2024 ao Base Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Fonte contratual principal para as obrigações de mitigação do operador de registro.

[4] **Conformidade Contratual da ICANN: orientação sobre obrigações relativas ao DNS Abuse (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

Interpretação operacional, requisitos de denúncia e exemplos de mitigação adequada.

[5] **ICANN: implementação dos requisitos de mitigação do DNS Abuse (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf

Relatório semestral de implementação e contagem de investigações e medidas de mitigação.

[6] **ICANN SSAC, SAC115: Relatório sobre uma abordagem interoperável ao tratamento de denúncias de abuso (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf

Contexto sobre a interoperabilidade na notificação de casos de abuso e a qualidade das evidências.

[7] **Hollenbeck, RFC 5731: Mapeamento de nomes de domínio no EPP (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

Definição técnica dos valores de status do domínio EPP, incluindo o status definido pelo servidor.

[8] **Laurie et al., RFC 9162: Certificate Transparency, versão 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html

Especificação de referência do protocolo e limites de CT como sensor.

[9] **ICANN, Serviço Centralizado de Dados de Zona** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

Escopo e modelo de acesso para os arquivos de zona dos gTLDs participantes.

[10] **Centro de Denúncias de Crimes na Internet do FBI, Relatório Anual do IC3 de 2025** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Números relativos a reclamações e perdas relatadas, incluindo o número de casos de phishing/spoofing.

[11] **Bijmans et al., "Catching Phishers By Their Bait" (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf

Medições específicas do conjunto de dados sobre a infraestrutura de phishing e os tempos de vida observados.

[12] **Domínios recém-registrados e tempo de vida das tentativas de phishing, Revista de Segurança Cibernética (2026)** · https://doi.org/10.1093/cybsec/tyag020

Evidências empíricas recentes sobre domínios de phishing recém-registrados e a distribuição de sua vida útil.

[13] **Análise inferencial de domínios registrados com intenção maliciosa — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

Análise financiada pela ICANN sobre registros maliciosos e fatores do ecossistema; limitações relevantes das alegações causais.

[14] **Chainalysis: Tendências de golpes com criptomoedas em 2026** · https://www.chainalysis.com/blog/crypto-scams-2026/

Estimativa do fornecedor sobre os influxos de golpes na cadeia de blocos em 2025; não considerados como parte do total de phishing de domínios.

[15] **APWG, Relatório sobre as Tendências das Atividades de Phishing, 1º trimestre de 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Ataques de phishing/URLs observados; as métricas não correspondem ao número de domínios registrados únicos.

[16] **Centro de Informações sobre Crimes Cibernéticos / Interisle, Panorama do Phishing em 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Distingue entre ataques observados, domínios únicos e domínios registrados com fins maliciosos.

[17] **Verisign, Relatório sobre o Setor de Nomes de Domínio, 2º trimestre de 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Fonte dos 401,6 milhões de registros relatados em todos os TLDs.