Política de Divulgação Responsável – OmniSec

Essa é uma versão reduzida e pública da nossa **Política de Divulgação Responsável**, cobrindo apenas os principais macro assuntos de forma sucinta. Caso tenha necessidade de acessar mais informações, pedimos que entre em contato pelos canais oficiais deste site que responderemos sua solicitação.

1. Objetivo

Estabelecer diretrizes formais para o reporte responsável de vulnerabilidades, promovendo um canal seguro, ético e colaborativo entre a sociedade, pesquisadores, profissionais de segurança e nossa organização.

2. Abrangência

Aplica-se a todos os usuários (internos e externos) que consumam ou interajam com nossos produtos, serviços, aplicações, APIs, ambientes corporativos, recursos digitais e quaisquer outros ativos tecnológicos mantidos, operados ou controlados pela **OmniSec**.

3. Diretrizes Gerais

3.1 Divulgação Responsável de Vulnerabilidades

A **OmniSec** valoriza a privacidade, a proteção de dados e a segurança da informação, sendo prioridades em todos os nossos serviços e produtos. Estudamos, pesquisamos e investimos continuamente nas pessoas, em nossos processos e contamos com tecnologia diferenciada alinhada as melhores práticas do mercado, sendo sua contribuição muito bem-vinda para a manutenção e a segurança de nosso ecossistema.

Se você é pesquisador de segurança ou profissional da área, contamos e prezamos pela sua colaboração para manter nossos clientes e usuários cada vez mais protegidos. Caso tenha identificado uma melhoria ou tenha encontrado uma possível vulnerabilidade em nossos sistemas, considere as recomendações deste documento durante nossa comunicação.

Pesquisadores, profissionais e entusiastas podem reportar vulnerabilidades seguindo nossas diretrizes, construídas e baseadas nas recomendações da **ISO/IEC 29147 - Information Technology — Security Techniques — Vulnerability Disclosure**.

Esta referência, descreve recomendações para um processo adequado de divulgação de vulnerabilidade entre as “partes interessadas” para que estes recebam seus relatórios, corrijam, publiquem informações relevantes abastecendo a “inteligência comunitária” quando aplicável e tomem decisões de risco proporcionais e acertadas.

Testar todo esse processo e sua capacidade de divulgação são boas práticas interessantes para um bom suporte, manutenção e operação segura de qualquer produto ou serviço exposto as ameaças, sejam estas novas, antigas, desconhecidas e/ou que estejam submetidas a escrutínio contínuo interno ou externo.

3.2 Canais e Meios de Comunicação

Nossos principais canais, baseado nas recomendações da “**RFC 2142 – Mailbox Names for Common Services, Roles and Functions**” são:

- csirt@ - Contato padrão via caixa do Centro de Resposta de Incidentes de Segurança, normalmente utilizado por Centros de Inteligência, instituições de segurança, CERTs regionais e globais para comunicação entre os times especializados.

- security@ - Caixa utilizada para quaisquer assuntos que envolvam segurança da informação, sejam spams, incidentes, phishings, engenharia social e suas variantes. Atualmente, herdou responsabilidades específicas que no passado eram do contato “abuse”.

- abuse@ - Para reclamações diversas sobre anormalidades, violações de uso inaceitável, abusos aos recursos tecnológicos, da rede, dos domínios e/ou da respectiva organização, do texto original da RPC sobre “inappropriate public behavior”.

Uma vez recebido a comunicação, nossas equipes farão os testes e validações necessárias e entrará em contato em tempo adequado e proporcional com o remetente/informante original. Relatórios e informações parciais podem atrasar, interferir no tempo ou inviabilizar nossa validação.

Caso o assunto seja sensível ou necessite de nível de proteção adicional, considere utilizar nossa chave-pública para envio criptografado do conteúdo.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: ID do usuário: CSIRT <csirt@omniseccorp.com>
Comment: Válido a partir de: 12/12/2025 13:21
Comment: Válido até: 12/12/2028 12:00
Comment: Tipo: EdDSA de 255 bits (chave privada disponível)
Comment: Uso: Assinatura, Criptografia, Certifying User IDs
Comment: Impressão digital: 3473927A0EB93F7342C87EDB12A878046D79A0C7


mDMEaTxBIBYJKwYBBAHaRw8BAQdAQi5PVOP7os6aix7OM2vx26U9aUHTAEhA7vHr
qJjDxUm0HUNTSVJUIDxjc2lydEBvbW5pc2VjY29ycC5jb20+iJkEExYKAEEWIQQ0
c5J6Drk/c0LIftsSqHgEbXmgxwUCaTxBIAIbAwUJBaTY0AULCQgHAgIiAgYVCgkI
CwIEFgIDAQIeBwIXgAAKCRASqHgEbXmgxwdkAQD42FpDj2R010TzJHymy+OYH2eO
OP3sEWBBBYpGOfOwhAD9FJln38C567MHKRJiTZM+F5ynmkIj1VFk/7IOD6C8wgK4
OARpPEEgEgorBgEEAZdVAQUBAQdATMTk6dWyqGxsmNfJBW0+6QA7GsnPIwul0qUn
W6470jcDAQgHiH4EGBYKACYWIQQ0c5J6Drk/c0LIftsSqHgEbXmgxwUCaTxBIAIb
DAUJBaTY0AAKCRASqHgEbXmgx9fJAQChLPBqUdzcIEcAfEQyqtsgeNpmq919rzeT
n5SNpZJLawD9H0nMvtFKLqABqa3gVUnFhCVWNqhHYEusyGQobsHOqwg=
=v4nm
-----END PGP PUBLIC KEY BLOCK-----
```

3.3 Recomendações e Boas-Práticas

Regras e exceções são importantes para jogar o bom jogo. Algumas orientações essenciais para garantir que testes de segurança e relatos de vulnerabilidades sejam conduzidos de forma ética, responsável e segura.

- Atenção extra para não violar leis, regulamentos ou diretrizes de autoridades legais em vigência
- Não causar dano, interrupção, stress ou impacto em nossos serviços, sistemas ou dados
- Não agir de má-fé, promover extorsão, exploração indevida frente as condições e descobertas
- Não executar força bruta, exploração de contas ou transações indevidas a menos que exista um motivo justificável para a extensão destes testes
- Não armazenar, compartilhar ou destruir dados nossos, de clientes e/ou usuários
- Dentro do possível e se disponíveis, enviar relatórios e/ou PoV (Provas de Conceito) com explicações suficientes e reproduzíveis de forma a avaliar os cenários indicados

- Caso encontre dados sensíveis durante os testes, retire uma amostra mínima, interrompa imediatamente o teste, apague os registros além da amostra e comunique nossos canais
- Caso seja necessário envolver terceiros ou haja implicação legal, priorizaremos onde possível a confidencialidade das informações de todas as partes envolvidas e comprometidas.

3.4 Cultura de Privacidade

Promovemos treinamentos regulares, campanhas de sensibilização e revisões periódicas de nossos processos, reforçando a importância da privacidade e da segurança da informação para todos. Seus dados serão usados apenas para contato durante as análises em linha as diretrizes e leis de proteção de dados pessoais. Não compartilharemos nenhuma informação sem comunicação prévia e sua permissão, exceto quando exigido por lei ou para continuidade de investigação (quando e se aplicável).

3.5 Sobre Incidentes, Segurança e Resposta

A OmniSec possui plano de **Resposta a Incidentes**, com base em metodologias reconhecidas, baseadas no NIST e utilizadas por Centros de Respostas (CERTs) globais**.** Em caso de incidente, garantimos análise, mitigação, recuperação e comunicação aos titulares e autoridades competentes em tempo legal**.** Considere sempre os canais de contato oficiais em caso de suspeita de violação, necessidade de comunicação ou informações.

4. Referências

Esta política, em constante revisão, tem como referência:

- **NIST CSF 2.0 e Incident Handling**
- **ISO/IEC 27701**
- **RFC-2142**

5. Atualizações e Revisões

Esta política será revisada periodicamente, sempre que houver alterações legais, regulatórias ou operacionais relevantes. O histórico de versões é mantido em nossos documentos e padrões para garantir a rastreabilidade e transparência em sua versão original e completa. Modificações com aplicabilidade imediata podem ocorrer sem prévio aviso e/ou pelo menos uma (1) vez ao ano conforme nossas políticas internas.

6. Contatos

Dúvidas, sugestões, recomendações e solicitações podem ser feitas diretamente por nossos canais oficiais, parcialmente mascarados para evitar coleta de emails por bots, cadastramentos indevidos e ferramentas de rastreamento web (web crawling). Além dos canais previamente indicados, estão disponíveis:

- **dpo** [arroba] omnisecorp [ponto] com
- **denuncia** [arroba] omnisecorp [ponto] com