TERMO DE USO DO SERVIÇO SOC – PLANO INTERMEDIÁRIO CONECTA REDE DA RNP

Recomenda-se a leitura **atenta e completa** dos termos e condições a seguir, pois a adesão e o uso dos serviços estão sujeitos à aceitação integral das disposições estabelecidas, as quais regem o acesso e a utilização deste serviço de TIC.

A REDE NACIONAL DE ENSINO E PESQUISA – RNP, associação civil qualificada como Organização Social pelo Decreto no 4.077 de 09 de janeiro de 2002, inscrita no CNPJ/MF sob o no **03.508.097/0001-36**, portadora da Inscrição Municipal no **02.838.109**, com sede na **Rua Lauro Muller no 116, 11º andar, salas 1101 a 1104, Botafogo, Rio de Janeiro, RJ**, celebram o presente **Termo de Uso** ao serviço **Plano INTERMEDIÁRIO CONECTA REDE do SOC-RNP**, mediante as seguintes cláusulas e condições:

1. Objetivo e alcance do serviço

1.1. O SOC-RNP do **PLANO INTERMEDIÁRIO CONECTA REDE** é um serviço ofertado pela RNP às Organizações Usuárias do Sistema RNP, que consiste no monitoramento e fornecimento de informações referentes aos possíveis ataques proveniente de diversas camadas, tais como: - de negação de serviços distribuídos (DDoS) e a consequente mitigação dos ataques cibernéticos nos links do backbone da RNP, utilizados pelas Organizações Usuárias. Além disso, oferece ainda, o monitoramento e a mitigação de ataques as aplicações web, scan de vulnerabilidades externas, exposição de dados sensíveis na internet, dark e deep web, visibilidade de vulnerabilidades em IPs externos, a classificação de risco cibernético e a análise da evolução histórica da instituição.

1.2. O objetivo do serviço SOC-RNP - **PLANO INTERMEDIÁRIO CONECTA REDE** é elevar o nível de maturidade em cibersegurança, proporcionando monitoramento contínuo, 24 horas por dia e7 dias por semana, realizado pela equipe especializada do SOC-RNP, por meio das ações abaixo descritas:

- Monitoramento proativo e mitigação de Ataques de Negação de Serviço distribuído (DDoS) nos links fornecidos pela RNP;
- Monitoramento proativo e mitigação de ataques contra aplicações web, como ataques de injeção, *cross-site scripting* (XSS), OWASP TOP 10 e etc;
- Interação próxima entre o SOC-RNP e a instituição contratante, a fim de compreender a eficácia das possíveis medidas de mitigação implementadas;
- Monitoramento de credenciais vazadas das instituições usuárias na *deepweb* e *darkweb*;
- Reuniões mensais de alinhamento;
- Envio de relatório mensal detalhando contendo os principais ataques detectados e mitigados pelo SOC-RNP;
- Envio do relatório que aborda a classificação de risco da instituição, incluindo uma análise da evolução histórica;

- Gestão de vulnerabilidades, que inclui a varredura mensal de vulnerabilidades em IPs externos (IPs públicos), com o escopo limitado a uma quantidade máxima de 5 (cinco) IPs públicos ou 5 (cinco) URLs;

Fornecimento mensal de relatórios que detalham as vulnerabilidades identificadas, em conjunto com as sugestões de correção; e

Fornecimento de Indicadores semanais referente ao monitoramento do SOC-RNP.

2. Responsabilidades e Procedimentos da RNP e da Organização Usuária

2.1. As responsabilidades e procedimentos a serem seguidos por cada parte para a completa prestação do serviço do **SOC-RNP PLANO INTERMEDIÁRIO CONECTA REDE** estão detalhadas abaixo, de tal modo que, ao concordar com os Termos de Uso do serviço, a **Organização Usuária** se responsabilizará pelas seguintes ações:

- Atualização de Dados de Contato: A Organização Usuária se compromete a manter seus dados de contato sempre atualizados junto ao SOC-RNP. Qualquer alteração nos dados de contato deverá ser comunicada de forma imediata, a fim de garantir a comunicação eficaz em caso de incidentes ou necessidade de assistência.

- Realizar o preenchimento do formulário de onboarding: Cabe à Organização Usuária preencher o Formulário do Onboarding no qual, além de outras informações, deverá indicar os links que serão alcançados pelo serviço, os domínios de responsabilidade da Organização Usuária, as aplicações expostas a serem analisadas pelo o scan de vulnerabilidades, este item, com limitações de 5 (cinco) e IPs/Aplicações externas (IPs públicos), os links das páginas WEB à serem protegidas pela solução WAF.

- Colaboração com o SOC-RNP: A colaboração mútua será fundamental para garantir a efetividade na resposta a incidentes identificados, portanto, em caso de detecção de ataques, a Organização Usuária concorda em atuar em conjunto com o SOC-RNP para a mitigação dos ataques detectados conforme o plano utilizado.

- Manutenção do Ambiente: A Organização Usuária se compromete a manter seu ambiente de TI atualizado e a tratar as vulnerabilidades identificadas de forma proativa tanto pelos apontamentos efetuados pelo serviço do SOC como por advento próprio. Isso inclui a aplicação de patches de segurança e a implementação de medidas preventivas para evitar ataques não monitorados neste plano INTERMEDIÁRIO CONECTA REDE do SOC-RNP.

- Reuniões Mensais: A Organização Usuária se compromete a participar ativamente das reuniões mensais, a fim de ajustar e melhorar o serviço prestado pelo SOC-RNP.

- Gestão de Vulnerabilidades: A Organização Usuária assume total responsabilidade pela correção das vulnerabilidades identificadas pelo SOC-RNP. Nesse contexto, a RNP fica isenta de qualquer responsabilidade por eventuais ataques resultantes dessas vulnerabilidades.

- Comunicação Eficiente: A Organização Usuária deverá manter a comunicação eficiente com o SOC-RNP, a fim de garantir a agilidade da resposta aos incidentes, além de aprimorar a postura da segurança geral.
- Configurações DNS para Monitoramento de Aplicações Web: a Organização Usuária deverá efetuar as configurações necessárias em seu registo DNS, a fim de desviar o tráfego da aplicação monitorada para o ambiente cloud-based da plataforma de WAF.
- Configurações de Certificados SSL/TLS para Monitoramento de Aplicações Web: a Organização Usuária deverá fornecer um certificado SSL/TLS válido, com sua respectiva chave privada, para que a plataforma WAF seja capaz de descriptografar e inspecionar o tráfego HTTPS.
- Monitoramento de credenciais vazadas na deepweb e darkweb: A Organização Usuária ficará responsável pela investigação e validação das credencias vazadas.
- O Responsável Técnico indicado no formulário de onboarding responderá pelo recebimento de registros relacionados ao monitoramento do SOC-RNP, pelo recebimento dos Indicares semanais e relatórios mensais de Segurança e comunicação sobre incidentes relacionados ao escopo deste termo;

2.2. É de responsabilidade da Organização Usuária a atualização de quaisquer dados que divergem do formulário de onboarding como nome e contatos dos responsáveis, janela da varredura de vulnerabilidade, alteração de blocos de IP e afins, devendo comunicar quaisquer alterações imediatamente à RNP, para fins de atualização do formulário de onboarding, por meio dos seguintes canais: atendimento@rnp.br ou telefone 0800 722 0216.

2.3. O SOC-RNP se responsabilizará pelas seguintes ações:

- **Monitoramento e Mitigação de DDoS:** O SOC-RNP tem como responsabilidade o monitoramento proativo e a mitigação de ataques de Negação de Serviço Distribuído nos links fornecidos pela RNP.
- **Segurança de Aplicações Web:** o SOC-RNP deverá efetuar o monitoramento proativo e mitigação de ataques contra aplicações web.
- **Reuniões Mensais:** É de responsabilidade do SOC-RNP agendar mensalmente as reuniões de alinhamento, sendo essencial que esses encontros tenham uma duração máxima de 30 minutos e ocorram até o 10º dia útil do mês subsequente.
- **Relatórios Mensais**: O SOC-RNP é responsável por fornecer, até o 5º dia útil do mês subsequente, um relatório que inclua os principais ataques detectados, a classificação de risco da instituição, a análise da evolução histórica e os resultados obtidos da varredura de vulnerabilidades dos IPs externos, conforme escopo definido na gestão de vulnerabilidade.
- **Gestão de Vulnerabilidades:** O SOC-RNP assume a responsabilidade de realizar mensalmente a varredura de vulnerabilidades em IPs externos (IPs públicos) ou URLs, dentro de um escopo máximo de 5(cinco) IPs públicos ou URLs, conforme estabelecido na janela de atuação e escopo definido no formulário de *onboarding*.
- **Relatórios de Vulnerabilidades:** As vulnerabilidades identificadas serão apresentadas mensalmente no relatório mensal, conforme estipulado no item 13 da cláusula segunda.

- **Indicadores Semanais:** O SOC-RNP fornecerá indicadores semanais referentes ao monitoramento.

2.4. Não estão incluídas as seguintes ações de monitoramento e mitigação no serviço SOC-RNP – PLANO INTERMEDIÁRIO CONECTA REDE:

- O monitoramento, detecção e mitigação de ataques de negação de serviços distribuídos para links que não forem fornecidos pela RNP ou que não estão informados no formulário de *onboarding.*
- O SOC-RNP não será responsável por ataques que ocorram em camadas diferentes das camadas 3, 4 e 7 do modelo OSI.
- O SOC-RNP não realizará investigação de ataques DDoS passados, ou seja, ocorridos antes da data do início do monitoramento.
- O SOC não manterá mitigações ativas durante períodos indefinidos. A mitigação possui o objetivo de interromper o ataque apenas durante a janela de sua ocorrência.
- O SOC-RNP não cobrirá a visibilidade de segurança de sistemas e dispositivos não incluídos no escopo deste termo.
- O SOC-RNP não se responsabilizará pelo uso de credenciais vazadas em ataques cibernéticos.
- O SOC-RNP não garantirá a detecção de todas as credenciais vazadas, em razão da variedade de métodos de vazamentos que poderão estar fora de seu escopo de atuação.
- O SOC-RNP não incluirá a realização de varreduras de vulnerabilidades em ambientes internos ou sistemas que não são publicamente acessíveis.
- O SOC-RNP não cobrirá a varredura de vulnerabilidades além dos 5 (cinco) IP´s/ URLs especificados.
- O SOC-RNP não abrangerá a elaboração de planos de ação para as recomendações de ações corretivas.
- O SOC-RNP não se responsabilizará por incidentes resultantes de ambientes e aplicações desatualizados na **Organização Usuária**. A responsabilidade de manter o ambiente atualizado recai sobre a **Organização Usuária**.
- O SOC-RNP isenta-se de qualquer responsabilidade pela correção de vulnerabilidades de qualquer natureza, cabendo exclusivamente à organização usuária a responsabilidade por sua correção.
- O SOC-RNP não abrangerá a geração de históricos anteriores ao início deste termo de serviço ou integração de dados históricos de outras soluções ou fornecedores externos de segurança.
- O SOC-RNP não assegurará a detecção de 100% dos eventos relacionados a **Organização Usuária**. Portanto, não será aplicada penalidade por falhas na monitoração, na eventualidade de o cliente identificar qualquer tipo de ameaça por

  meio de informações privilegiadas, contato direto de um possível ator de ameaças ou demais fontes de informação.
- O SOC-RNP não será responsável por ataques de zero-day, que envolvam vulnerabilidades ainda desconhecidas.

- A execução do trabalho feito pelo SOC-RNP não garantirá que novas vulnerabilidades não afetarão os ambientes da **Organização Usuária**, haja vista que estas surgem frequentemente com a evolução tecnológica.
- O SOC-RNP não poderá ser responsabilizado por quaisquer tipos de paradas, indisponibilidades, perdas, acessos indevidos, crises ou incidentes na Organização Usuária. Tais situações são de total responsabilidade da Organização Usuária, devendo esta adotar as devidas tratativas para o retorno do seu ambiente tecnológico.

3. Suspensão ou encerramento dos Serviços

3.1. A RNP poderá suspender ou rescindir seu acesso aos serviços se uma destas situações acontecer:

- A Organização Usuária violar estes termos ou políticas de forma relevante ou recorrente.
- Se a RNP necessitar suspender ou encerrar os serviços para obedecer a um requisito legal ou uma ordem judicial.
- Se tivermos razões concretas para acreditar que sua conduta na utilização do serviço causa danos ou responsabilidade à RNP ou a terceiros.
- Se o Programa Conecta Rede, do Governo Federal, deixar de custear os serviços e outro meio de custeio, pela RNP ou pela própria Organização Usuária, caso tenha interesse, não o substituir.

4. Vigência e Rescisão

4.1. Estes Termos de Uso entram em vigor na data de sua publicação e permanecerão válidos por tempo indeterminado, enquanto o serviço for disponibilizado. Reservamo-nos o direito de modificar ou atualizar estes termos a qualquer momento, sem aviso prévio. As alterações serão efetivas a partir da data de sua publicação via e-mail. Recomendamos que as Organizações Usuárias acessem periodicamente os Termos de Uso para manter-se informados sobre eventuais modificações. O uso contínuo do serviço após a publicação de alterações constitui aceitação dos novos termos.

4.2. O usuário pode encerrar o uso do serviço a qualquer momento, com a necessidade de notificação prévia com antecedência mínima de 60 (sessenta) dias.

4.3. A RNP reserva-se o direito de suspender ou encerrar o acesso ao serviço, total ou parcialmente mediante aviso prévio de 30 (trinta) dias, com exceção da suspensão ou encerramento motivado por violação destes Termos de Uso ou de uso indevido do serviço. A rescisão do acesso ao serviço não implica em qualquer obrigação de indenização ou compensação por parte do provedor.

5. Aceite Eletrônico

5.1. Aceite: Ao utilizar o Serviço SOC Plano Intermediário – Conecta Rede, o usuário concorda expressamente com os Termos de Uso e demais políticas aplicáveis. O aceite é formalizado por meio da assinatura eletrônica e representa sua concordância com todos os termos aqui estabelecidos.

5.2. Autenticidade e Validade: O usuário reconhece que o aceite eletrônico tem a mesma validade que uma assinatura física, constituindo prova suficiente de sua concordância com o conteúdo dos Termos de Uso.

6. Foro

6.1. Fica eleito o foro da cidade do Rio de Janeiro - RJ , para dirimir quaisquer dúvidas oriundas do presente TERMO.

_____ Documento assinado digitalmente
FABIO CARLOS MACEDO
Data: 19/02/2025 17:01:20-0300
Verifique em https://validar.iti.gov.br _____x

Assinatura do responsável legal para instituição