

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

1. **DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA**, neste ato denominada Recorrente, pessoa jurídica de direito privado já qualificada nos autos do processo em epígrafe, vem, por meio de seu representante legal, interpor **RECURSO ADMINISTRATIVO** contra a decisão da digna Comissão de Licitação que julgou esta empresa inabilitada no Pregão Eletrônico nº. 02/2022, do processo administrativo nº 0951.110715/2022-06, apresentando no articulado as razões de sua irresignação:
2. Na data de 12 de janeiro de 2023, deu-se início a sessão referente ao Pregão Eletrônico nº. 02/2022, processo licitatório vinculado a Procuradoria-Geral da Fazenda Pública - PGFN.
3. Finda a sessão, em 16/01/2023 à DSS Serviços de Tecnologia da Informação LTDA foi declarada vencedora do certame, com registro de intenção de recorrer das empresas CENTRAL IT TECNOLOGIA DA INFORMACAO S/A, e GLOBALWEB OUTSOURCING DO BRASIL S.A.
4. Neste intervalo a CENTRAL IT encaminhou peça recursal, conforme preleciona o processo licitatório.
5. Disseca-se da peça, que essa RECORRENTE não apresentou documentação probatória demonstrando a qualificação econômico-financeira, o que em análise realizada pelo Pregoeiro, constatou-se por meio do Balanço Patrimonial, sua boa situação financeira.
6. Restando prejudicada o primeiro ponto levantado pela CENTRAL IT.
7. Seguindo o recurso, adentrou ao tópico “Habilitação técnica” e de forma arbitrária a CENTRAL IT afirmou que somente deveriam ser considerados para análise os atestados emitidos pelo TRE-MG, MDR e TJMT 74-2019, e os atestados TJMT 21 e Ministério do Trabalho Emprego deveriam ser desconsiderados por não terem sido executados concomitante por período mínimo de 24 (vinte e quatro) meses.
8. E que após análise a área técnica **denegou** o pedido de desconsideração dos atestados mencionados.
9. Adiante, a CENTRAL IT aduziu que atestado do MDR, em específico, não é capaz de comprovar o atendimento a todos os requisitos exigidos no Termo de Referência, em especial os itens 12.7.11.2, 12.7.11.4, 12.7.13.2, 12.7.13.3.
10. Entretanto, o Pregoeiro com muita cautela analisou item por item, seguindo com a presente análise:
11. Item 12.7.11.2 - Com base nas informações extraídas da documentação do processo licitatório do MDR, a área técnica demandante entendeu que a DSS atende ao critério do item 12.7.11.2 e **nega**, portanto, o pedido da CENTRAL IT quanto ao não atendimento do item 12.7.11.2.
12. Item 12.7.11.4 – resta comprovado no Atestado TJMT 21, em seu item 17 - Terabytes Storage, um volume de 1.2 PetaBytes de dados administrado pela empresa, superando o critério de habilitação solicitado no edital da Procuradoria, demonstrando, portanto, que a empresa cumpre o critério de habilitação do item 12.7.11.4, **negando**, novamente o afirmado pela CENTRAL IT.
13. Item 12.7.13.2 – a área técnica comprovou o atendimento por meio do atestado do MDR, **rejeitando** a hipótese encampada pela CENTRAL IT.
14. Item 12.7.13.3 – o Pregoeiro entendeu que não executamos atividades que comprovariam esta atividade realizada, visto que esta é realizada por equipe do SERPRO, dando procedência ao item para a CENTRAL IT.

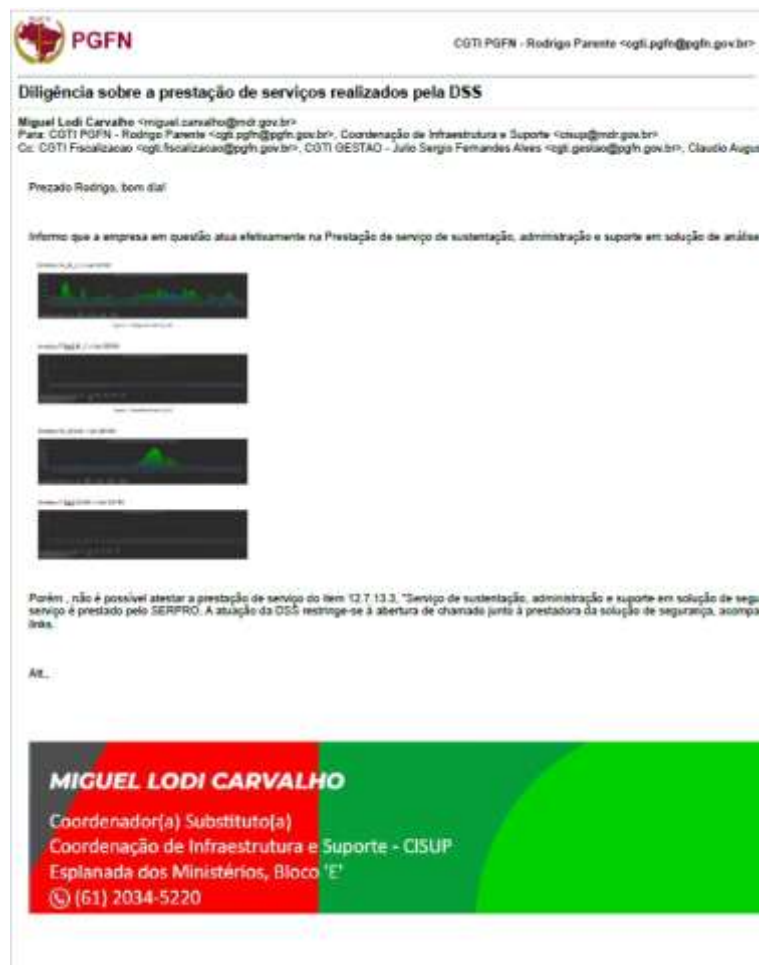
**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

15. Após análise das razões da recorrente, em decisão proferida por esta Procuradoria-Geral da Fazenda Nacional, constatou-se o não atendimento pela DSS do item 12.7.13.3, qual seja: prestação de serviço de sustentação, administração e suporte em solução de segurança DDos (Distributed Denial of Service), sendo este exigido pelo instrumento convocatório.
16. Nesse compasso, o Pregoeiro procedeu com inabilitação da recorrente, retornando para fase de julgamento do certame em 01/02/2023, a posteriori, convocou a próxima na fila de classificação a empresa CENTRAL IT.
17. Em um primeiro momento, deve-se ater a análise minuciosa exarada por esta Procuradoria, contudo, equivocou-se em um único item, que culminou neste imbróglio.
18. Certo da busca pela verdade real, nos faz o presente recurso, o instrumento necessário para demonstrar a razões desta RECORRENTE ter ficado em 1º lugar e possuir a qualificação técnica exigida pelo instrumento editalício.
19. Segue-se ao mérito
20. Diante da análise apresentada pela área técnica, que deu ensejo a inabilitação da recorrente, com base nas razões recursais da Central IT, no qual considerou a análise dos atestados indicados na tabela ponto a ponto, e que nesta, a DSS indicou para o item 12.7.13.3 apenas o atestado "26 – MDR.
21. Dissertou que o Atestado do MDR não comprovou o exigido, ressaltando que a tabela (ponto a ponto) se trata de ferramenta obrigatória e exclusiva de apresentação dos atestados de capacidade técnica, e que a atuação da área técnica demandante restringiu a avaliar apenas o informado na tabela indicativa referenciada.
22. Desta feita, vimos esclarecer pontos relevantes e motivadores de provimento a manutenção da habilitação da DSS, vez que foram demonstrados pelos atestados anexados no sistema compras.gov o atendimento de todos os critérios de habilitação técnica exigido no edital.
23. Primeiramente, insta frisar que a DSS apresentou uma extensa relação de atestados de capacidade técnica e documentos complementares (contratos, editais, Termos de Referência) para aferição da qualificação exigida no certame e seguiu o previsto no item 12.7.19 que se referiu a exigência de apresentação de tabela de comprovação (ponto a ponto), norteia-se pelos próprios argumentos levantados pelo Ilustre Pregoeiro.
24. Todavia, dada a quantidade de informações técnicas juntadas ao processo via sistema, a comissão de licitação, ainda que com o apoio da tabela ponto a ponto encontrou dificuldades em visualizar requisitos nos atestados e documentos, motivo que ensejou diligências nas quais a DSS demonstrou pormenorizadamente em quais atestados constavam os requisitos não localizados.
25. Foram objeto de diligências os itens 12.7.12.2, 12.7.12.4, 12.7.9.1, 12.7.11.5, 12.7.11.6 para os quais a comissão técnica avaliadora informou não haver localizado atestados compatíveis de modo que solicitou que fossem enviados pela recorrente documentos aderentes que demonstrassem a prestação de tais serviços nos volumes e especificações definidas no Termo de Referência, a indicação dos requisitos foi realizada pela DSS com ressalva que estes constavam nos atestados já juntados ao processo via sistema.
26. Ante ao volume de informações houve apenas a necessidade de evidência tais requisitos de forma a deixá-los em melhor visibilidade a comissão técnica, assim, houve apontamento por atestado,

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

onde constava cada requisito não localizado (Registros no processo SEI nº 10951.110715/2022-06 / Pág. 1252 a 1254).

27. No que tange ao requisito previsto no item 12.7.13.3, do qual motivou a inabilitação da DSS, durante a avaliação dos atestados juntados ao processo de habilitação da recorrente, a comissão técnica não levantou questionamento sobre a inobservância ou dificuldade de localizar o item.
28. Outrossim, também não houve diligência junto a DSS na fase do recurso interposto pela Central IT no sentido de certificar se além do atestado "26 – MDR haveria outro que suprisse a exigência, por casualidade dado o volume de informações, eventualmente não identificado pela comissão ou não indicado pela DSS por equívoco na tabela ponto a ponto.
29. Frise-se que houve diligência junto ao Ministério do Desenvolvimento Regional - MDR como resta registrado nos autos do processo SEI 10951.110715/2022-06 / pg. 1288 e 1289.
30. Considerando o art. 43, § 3º, da Lei nº 8666/1993, o ilustríssimo pregoeiro deste órgão realizou diligência junto ao Ministério do Desenvolvimento Regional, e foi informado pelo agente público Miguel Lodi Carvalho que a DSS não realiza as atividades que comprovariam o atendimento ao item 12.7.13.3, (já que esta atividade é realizada, naquele Ministério, por equipe do SERPRO), empresa pública contratada pelo MDR, conforme print a seguir:



OBSERVAÇÃO – ENVIAMOS PARA O E-MAIL DO PREGOEIRO A IMAGEM ACIMA COM O NOME DE ANEXO 01 – DILIGÊNCIA MDR

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

31. Todavia, o agente público supratranscrito como faz parte do novo corpo técnico advindo da mudança governamental, provavelmente, não tem visão geral de toda pasta Ministerial em sua área tecnológica.
32. Cumulado com o fato de ser substituto, e os especialistas na área estarem de férias, seria importante ter-se cautela, visto termos informações do próprio órgão quanto a item em questão que gerou a inabilitação da DSS, serem realizados de forma plena por nossa equipe técnica.
33. É imperioso assegurar que o agente público prima pela transparência de informação, não é de bom tom negligenciar seu dever-ser como figura representativa do Estado.
34. Deve-se trazer à baila, o exposto pelo ordenamento jurídico em seu art. 11 da Lei 14.230/2021, que versa sobre improbidade administrativa, *in verbis*:

Art. 11. Constitui ato de improbidade administrativa que atenta contra os **princípios da administração pública a ação ou omissão dolosa que viole os deveres de honestidade, de imparcialidade e de legalidade**, caracterizada por uma das seguintes condutas:

V - **frustrar**, em ofensa à imparcialidade, o caráter concorrencial de concurso público, de chamamento ou de **procedimento licitatório**, com vistas à obtenção de benefício próprio, direto ou indireto, ou de terceiros; (Redação dada pela Lei nº 14.230, de 2021) (Grifo nosso)

35. Nota-se que houve uma frustração evidente, Sr. Pregoeiro, sem que houvesse de fato as informações corretas sobre o trabalho realizado por essa RECORRENTE.
36. Ilustre Pregoeiro, diante de vícios e falhas nos atos praticados ao longo do processo licitatório, seja pela Administração, seja pelos próprios licitantes, em consonância com o art. 55 da Lei nº 9.784/1999 e com a Súmula nº 473 do STF, evidencia a diretriz de busca do saneamento, impondo-se a anulação apenas diante da impossibilidade da convalidação – ou seja, quando se está diante de vício insanável.
37. O que não é o caso *in tela*.
38. O item 12.7.13.3 - O Distributed Denial of Service (DDoS), indicado como não identificado nos atestados da DSS, refere-se a um ataque distribuído de negação de serviço que tenta esgotar os recursos de rede, aplicação ou serviço para evitar que os usuários consigam acessar ambientes online.
39. Ele envia múltiplas solicitações para o recurso Web invadido para exceder a capacidade do site de lidar com diversas requisições ao mesmo tempo e, assim, prejudicar seu funcionamento.
40. Os principais alvos dos ataques DDoS são sites, porém, também podem atingir qualquer organização que dependa do fornecimento de serviços online. Estes ataques representam uma grande ameaça para as organizações, pois, ao causam a indisponibilidade nos serviços corporativos.
41. Além de ter os serviços paralisados e interromper as rotinas corporativas, a organização acaba perdendo a credibilidade, pois estes terão menos confiança na capacidade da organização fornecer serviços de qualidade.

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

42. É importante ressaltar, que o Ministério do Desenvolvimento Regional, não possui uma solução de tecnologia contratada, dedicada a prevenção de ataques DDoS, desta forma, a equipe da DSS realiza este trabalho, em conjunto com as operadoras de Telecom, que neste caso é o SERPRO.
43. Para um melhor entendimento, segue-se os Métodos de Administração do Ambiente:
- **Sustentação:** O time de especialistas alocados no Ministério do Desenvolvimento Regional, é responsável pela sustentação de todos os ativos de infraestrutura que compõem o ambiente, no caso de ataques cibernéticos, existem atuações da equipe no balanceador (F5) e nas caixas de Firewall, onde poderá ser identificado o ataque, através de anormalidades identificadas.
 - **Administração:** O time de especialistas é responsável por desenvolver, aplicar, modificar e atualizar as caixas de firewall, aplicando atualizações de firmware e de regras, que podem mitigar estes ataques, quando necessário.
 - **Suporte:** Quando um ataque DDoS é percebido, o time de especialistas realiza duas ações em paralelo. A primeira ação consiste em uma atuação conjunto com o SERPRO (que faz o fornecimento de um link de internet ao MDR), onde são realizadas atividades de bloqueio do ataque. A segunda ação é realizada no balanceador de carga (F5), e no próprio Firewall, com o objetivo de mitigar o incidente (ataque).
44. Contudo, ao realizar averiguação junto a equipe DSS no âmbito do MDR, resta demonstrado que estas atividades são desempenhadas, **inclusive é de ciência do órgão**, que a equipe possui um time de especialistas capacitados, que não somente possui expertise, como também possui capacidade técnica para desenvolver estudos especializados, acerca de ataques cibernéticos, conforme demonstra e-mail enviado pelo MDR no dia 14/12/2022, solicitando uma nota técnica sobre um incidente de ataque cibernético DDoS, ao preposto da DSS tecnologia Hamilton Junior, conforme imagem à seguir.

De: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Enviada em: quarta-feira, 14 de dezembro de 2022 09:35

Para: Hamilton Leite Cavalcante Junior <hamilton.junior@dssnet.com.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>

Assunto: Incidente de segurança

Hamilton. Bom dia.

Destarte estarmos monitorando o ambiente após contramedidas ao incidente de segurança que indisponibilizou ou degradou os serviços de rede do MDR nesta semana, solicito iniciarmos as Análises após ações - APA.

Nesse sentido, solicitamos Nota Técnica contemplando o relato de todo incidente (ataque), evidências e ações de tratamento.

A Nota Técnica deverá ser entregue até o dia 21/12/2022, porém solicitamos registros preliminares para enviarmos ao CTIR Gov (logs e evidências) até amanhã.

Informe que foi solicitado ao Serpro a apresentação de relatório com as medidas realizadas.

Atenciosamente,

OBSERVAÇÃO – ENVIAMOS PARA O E-MAIL DO PREGOEIRO A IMAGEM ACIMA COM O NOME DE ANEXO 02 – DILIGÊNCIA DDoS MDR

45. Conforme imagem abaixo, a nota técnica foi entregue, inclusive houve o aceite por parte do Coordenador Geral de Tecnologia da Informação do MDR, conforme imagem abaixo:

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

RE: Incidente de segurança



Claudio Augusto Novais Ferraz <claudio.fr

Para: Hamilton Júnior

Cc: Diego Menegazzi; ETIR; Sistemas Seguranca; Silvio Guido Alves da Silva;

Herick Gervasio de Melo Souza; Willian Crisanto; georgia.dssnet@outlook.com; +2 outros



sex 03/02/2023 10:31

Boa tarde.

Atendeu sim. Recebido.

Atenciosamente,



De: Hamilton Júnior <hamiltonjr.dssnet@outlook.com>

Enviado: sexta-feira, 3 de fevereiro de 2023 10:23

Para: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>; "Silvio Guido Alves da Silva" <silvio.silva@dssnet.com.br>; Herick Gervasio de Melo Souza <herick.souza@dssnet.com.br>; Willian Crisanto - DSS <willian.crisanto@dssnet.com.br>; georgia.dssnet@outlook.com <georgia.dssnet@outlook.com>; Elmiro Barbosa <elmiro.barbosa@dssnet.com.br>; Valter Brito Dourado Araújo <valter.araujo@dssnet.com.br>

Assunto: RES: Incidente de segurança

Bom dia, Claudio!

A nota técnica enviada, atendeu a necessidade?

Pode confirmar o recebimento sobre o documento produzido pela equipe, acerca do tratamento do incidente de ataque cibernético ao MDR, em dezembro passado?

Desde já, agradeço por sua atenção!!

OBSERVAÇÃO – ENVIAMOS PARA O E-MAIL DO PREGOEIRO A IMAGEM ACIMA COM O NOME DE ANEXO 03 – DILIGÊNCIA DDoS MDR

46. Nesse sentido, conforme e-mails acima (anexos remetidos via e-mail por não serem suportados no campo de recursos do site compras.gov) fica evidenciado que houve tratamento ao ataque DDoS.
47. A Nota técnica em questão solicitada a DSS pelo MDR informa todas as atividades que foram realizadas, (anexo remetido via e-mail por não serem suportados no campo de recursos do site compras.gov), que comprova a expertise da equipe e a ciência do órgão acerca do tratamento de incidentes de envolvendo ataques cibernéticos.
48. Além da equipe possuir expertise, também fornece ao MDR informações importantes, quanto a ataques cibernéticos DDoS, contribuindo assim para a disponibilidade do ambiente e continuidade, mensalmente entrega ao órgão, relatórios de metas aferidas, que informam necessidades e melhorias aplicadas ao ambiente.
49. Destaca-se que no relatório do mês de janeiro de 2023 (anexo remetido via e-mail por não serem suportados no campo de recursos do site compras.gov), a equipe de especialistas da DSS, informa a seguinte melhoria aplicada:

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

“Foram realizadas todas as tratativas possíveis com os ativos presentes no MDR para impedir que o ataque sofrido obtivesse sucesso, no qual foi fundamental o apoio da equipe de segurança do SERPRO mitigando os acessos dentro da própria operadora, bem como o apoio do fabricante do *appliance* F5 Big-IP, no qual um Especialista realizou todo procedimento possível para descartar os acessos indevidos. Durante este processo foi identificado a necessidade de atualização dos ativos do MDR, no qual, já se encontra processo licitatório em andamento, este que deve garantir maior segurança e respostas mais rápidas a futuros incidentes”

50. Não obstante as evidências demonstradas acerca da realização das atividades DDoS no MDR, a DSS também possui a experiência exigida prevista no Atestado TJMT 21/2014, que está vinculado a matriz ponto a ponto e consta nos autos do processo de habilitação da DSS tendo sido encaminhado via sistema junto aos demais documentos no prazo previsto no instrumento convocatório, tratando-se de documento válido para efetiva comprovação do item 12.7.13.3, na página 07 do Atestado TJMT 14- CT 21/20214:

- Solução de Segurança de TI;
- Firewall de rede e de aplicações (perimetral e WAF);
- Analisador de conteúdo HTTP;
- IPS e IDS de rede;
- Concentrador VPN;
- Filtro de Conteúdo, Anti-vírus e anti-spam;

51. Conforme evidenciado no item “Firewall de rede e de aplicações (perimetral e WAF)” é importante ressaltar que o WAF, ou firewall de aplicativos web, ajuda a proteger os aplicativos web ao filtrar e o monitorar o tráfego HTTP entre o aplicativo web e a internet.

52. De modo geral, o WAF protege os aplicativos web contra ataques como falsificação de solicitação entre sites, cross-site-scripting (XSS), inclusão de arquivo e injeção de SQL, entre outros. O WAF é uma defesa de protocolo da camada 7 (no modelo OSI) e não foi desenvolvido para fins de defesa contra todos os tipos de ataques. Esse método de mitigação de ataques costuma fazer parte de um conjunto de ferramentas que, juntas, criam uma defesa holística contra diversos vetores de ataque. Com a implantação de um WAF à frente da aplicação web, é colocado um escudo entre a aplicação e a internet. Enquanto um servidor proxy protege a identidade da máquina cliente com o uso de um intermediário, o WAF é um tipo de proxy reverso que protege o servidor contra a exposição, já que seus clientes passam pelo WAF antes de chegar ao servidor. O WAF funciona por meio de um conjunto de regras normalmente chamadas de “políticas”. As políticas têm como objetivo proteger o aplicativo contra vulnerabilidades filtrando o tráfego malicioso.

53. O valor de um WAF deve-se, em parte, à velocidade e à facilidade com que a modificação das políticas pode ser implantada, permitindo uma resposta mais rápida a variados vetores de ataque. Durante um ataque DDoS, o rate limiting pode ser implantado rapidamente modificando-se as políticas do WAF, atividade esta, que é realizada todas as vezes em que é percebido um ataque cibernético (DDoS), no ambiente do TJMT.

54. Os itens elencados estão ligados diretamente a soluções de segurança de Tecnologia de Informação com o propósito de mitigar ataques DDos, evidenciando a qualificação técnica desta RECORRENTE.

55. Consubstanciado ao citado, no Termo de Referência do Edital Pregão Eletrônico n. 1/2013 – CIA 0117352-45.2013.8.11.0000 TJMT que vincula o contrato e atestado de capacidade técnica n.

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

21/2014, consta detalhamento de Experiência com Firewall - Mikrotik, ISA, IPTABLES ou Checkpoint, todos dispositivos de proteção DDoS conforme pág. 51, item 15.1.1, subitem 8:

“8. Experiência com Firewall - Mikrotik, ISA, IPTABLES ou Checkpoint;”

56. Quando um ataque DDoS é percebido no ambiente do TJMT, a equipe de especialistas, conta com o apoio do fabricante dos *appliances* Mikrotik, ISA, IPTABLES ou Checkpoint, onde um especialista realiza todos os procedimentos, para descartar os acessos considerados DDoS. Inclusive, neste momento, pode ser identificado junto ao fabricante a necessidade de atualização dos ativos de segurança, com o objetivo de mitigar o ataque e garantir que novos ataques sejam identificados e tratados com a brevidade necessária.
57. Diante disso, é inequívoca a comprovação que a DSS atende ao requisito 12.7.13.3, conforme atestado de capacidade técnica TJMT Contrato 21/2014 e edital e TJ que os vincula e o do MDR, que pode ser comprovada pelos anexos:
- ANEXO 01 – DILIGÊNCIA_MDR
 - ANEXO 02 – DILIGÊNCIA_DDoS MDR
 - ANEXO 03 – DILIGÊNCIA_DDoS_MDR
 - ANEXO 04 - Declaração_CT_21.2014_TJMT
 - ANEXO 05 - Evidencia_MDR_Nota_Técnica_DDoS
 - ANEXO 06 – Nota Técnica Ataque de Segurança
58. Posto isso, ressalta-se que a DSS cumpriu com todos os requisitos técnicos de habilitação, uma vez que todos se encontraram devidamente registrados no sistema comprasnet conforme prazos previstos nos critérios de habilitação.
59. Assim, fica claro que não há qualquer motivo que enseje a não habilitação da DSS, pois resta demonstrado o pleno cumprimento do disposto no Edital e seus anexos incluindo o devido cumprimento do item 12.7.13.3, restando atendidas as exigências técnicas em características, quantidades e prazos do objeto da licitação, bem como, a finalidade primordial de ter ofertado o melhor preço para execução do objeto.
60. Logo, *in casu*, não se há o que falar em não preenchimento dos requisitos de qualificação técnica.
61. Pelo presente é que se faz razoável esse Recurso Administrativo.

II - DOS PEDIDOS

62. Diante do exposto, requer que o presente Contrarrazão seja julgado totalmente procedente para a devida e justificada Habilitação da empresa **DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA**, que demonstrou atender todos os quesitos de habilitação exigidas pelo Edital, HABILITANDO a empresa para ser declarada vencedora, optando assim pelo serviço de menor valor, no qual tal empresa foi declarada vencedora em tal certame, como rege tal Lei nº 8.666/93, não havendo assim nenhum prejuízo ao erário, tanto por qualificação quanto por preços, sendo assim legal, pois atende todos os requisitos do edital e está de acordo com objetivo de toda e qualquer licitação, que é a busca pelo MENOR PREÇO ofertado pelas licitantes Habilitadas, atingindo os princípios da legalidade, impessoalidade, moralidade, igualdade, publicidade e probidade administrativa, da vinculação do instrumento convocatório, do julgamento objetivo e dos que lhe são correlatos, sempre buscará a proposta mais vantajosa para a Administração.
63. Em assim não entendendo, que se faça subir para a autoridade superior.

**PREGÃO ELETRÔNICO Nº. 02/2022, DO PROCESSO ADMINISTRATIVO Nº 0951.110715/2022-06,
PROCURADORIA-GERAL DA FAZENDA NACIONAL**

64. Com protestos de máximo respeito e ânimo de justiça.

OBSERVAÇÃO IMPORTANTE: Considerando que o sistema de registro de recurso da plataforma <https://www.gov.br/compras/pt-br/> não suporta anexos em formato PDF ou Imagens, estando aberto apenas para registro de texto, além registro no campo específico do site comprasgov. encaminhamos o presente recurso em formato PDF com o demonstrativo das imagens citadas, bem como os anexos 01, 02, 03, 04, 05 e 06 que representam evidências que fundamentam a peça recursal, no e-mail de comunicação oficial indicado no edital (licitacoes.pgfn@pgfn.gov.br).

Neste sentido, dada a necessidade de apresentação dos documentos junto a peça recursal e indisponibilidade do sistema para inserção dos anexos, mui respeitosamente, pedimos a comissão de licitação que seja dada a publicidade do recurso PDF e anexos remetidos via e-mail aos demais licitantes e interessados do certame.

FERNANDO
ANTONIO
BELLEZZIA:3926
7598600

Assinado de forma
digital por FERNANDO
ANTONIO
BELLEZZIA:39267598600
Dados: 2023.02.08
17:42:12 -04'00'

Fenando Antonio Bellezzia
Diretor de Serviços

Valter Brito Dourado Araújo

De: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>
Enviado em: sexta-feira, 3 de fevereiro de 2023 10:31
Para: Hamilton Júnior
Cc: Diego Menegazzi; ETIR; Sistemas Seguranca; Silvio Guido Alves da Silva; Herick Gervasio de Melo Souza; Willian Crisanto; georgia.dssnet@outlook.com; Elmiro Barbosa; Valter Brito Dourado Araújo
Assunto: RE: Incidente de segurança

Boa tarde.

Atendeu sim. Recebido.


Atenciosamente,

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador(a)-Geral

Coordenação-Geral de Tecnologia da Informação - CGTI

SGAN Q.906, Módulo 'F' Bloco 'A' Ed.Celso Furtado

 (61) 2034-5713

De: Hamilton Júnior <hamiltonjr.dssnet@outlook.com>
Enviado: sexta-feira, 3 de fevereiro de 2023 10:23
Para: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>
Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>; "Silvio Guido Alves da Silva" <silvio.silva@dssnet.com.br>; Herick Gervasio de Melo Souza <herick.souza@dssnet.com.br>; Willian Crisanto - DSS <willian.crisanto@dssnet.com.br>; georgia.dssnet@outlook.com <georgia.dssnet@outlook.com>; Elmiro Barbosa <elmiro.barbosa@dssnet.com.br>; Valter Brito Dourado Araújo <valter.araujo@dssnet.com.br>
Assunto: RES: Incidente de segurança

Bom dia, Claudio!

A nota técnica enviada, atendeu a necessidade?

Pode confirmar o recebimento sobre o documento produzido pela equipe, acerca do tratamento do incidente de ataque cibernético ao MDR, em dezembro passado?

Desde já, agradeço por sua atenção!!

Cordialmente,



Hamilton Leite Cavalcante Júnior

Gerente de Serviços - Preposto

+55 61 99548-484

hamiltonjr@outlook.com

www.dssnet.com.br

De: Hamilton Júnior

Enviada em: quarta-feira, 21 de dezembro de 2022 19:16

Para: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>; "Silvio Guido Alves da Silva" <silvio.silva@dssnet.com.br>; Herick Gervasio de Melo Souza <herick.souza@dssnet.com.br>; Willian Crisanto - DSS <willian.crisanto@dssnet.com.br>; georgia.dssnet@outlook.com

Assunto: ENC: Incidente de segurança

Boa noite, Claudio.

Conforme solicitado, segue a nota técnica do incidente de segurança.

Para demais esclarecimentos, estou à disposição.

Atenciosamente,



Hamilton Leite Cavalcante Júnior

Gerente de Serviços - Preposto

+55 61 99548-484

hamiltonjr@outlook.com

www.dssnet.com.br

De: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Enviada em: quarta-feira, 14 de dezembro de 2022 09:35

Para: Hamilton Leite Cavalcante Junior <hamilton.junior@dssnet.com.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>

Assunto: Incidente de segurança

Hamilton. Bom dia.

Destarte estarmos monitorando o ambiente após contramedidas ao incidente de segurança que indisponibilizou ou degradou os serviços de rede do MDR nesta semana, solicito iniciarmos as Análises após ações - APA.

Nesse sentido, solicitamos Nota Técnica contemplando o relato de todo incidente (ataque), evidências e ações de tratamento.

A Nota Técnica deverá ser entregue até o dia 21/12/2022, porém solicitamos registros preliminares para enviarmos ao CTIR Gov (logs e evidências) até amanhã.

Informo que foi solicitado ao Serpro a apresentação de relatório com as medidas realizadas.


Atenciosamente,


CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador(a)-Geral

Coordenação-Geral de Tecnologia da Informação - CGTI

SGAN Q.906, Módulo 'F' Bloco 'A' Ed.Celso Furtado

 (61) 2034-5713



Cuiabá, 7 de fevereiro de 2023.

DECLARAÇÃO

Declaramos para os devidos fins, que a empresa **DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA.**, sediada na Av. Arquimedes Pereira Lima, 3.483, Bairro Santa Cruz, Cuiabá/MT, inscrita no CNPJ nº 03.627.226/0001-05, prestou serviços de *"conectividade em tecnologia da informação referente à administração de sistemas operacionais, à administração de servidores de e-mail, à administração de servidores de aplicação, à infraestrutura de redes, à segurança e à administração de usuários, seus perfis de acesso, credenciais e demais aplicações relacionadas, mediante solicitação de execução pelo departamento de conectividade, da Coordenadoria de Informática do Tribunal de Justiça de Mato Grosso"* para o **TRIBUNAL DE JUSTIÇA DO MATO GROSSO**, sediado na Rua C, s/n - Centro Político Administrativo, Cuiabá - MT, CEP: 78049-926, inscrito no CNPJ nº 03.535606/0001-10, mediante o Contrato n. 21/2014, no período de 16/04/2014 a 15/04/2020, ou seja, por 72 (setenta e dois) meses.

A execução do Contrato n. 21/2014 abarcava também as seguintes tarefas:

- Instalação, configuração, administração, sustentação, monitoramento e operação de soluções de segurança de Perímetro, em alta disponibilidade, com funcionalidades de IDS/IPS e Filtro de conteúdo Web;
- Prestação de serviço de sustentação, administração e suporte em solução de análise de tráfego de rede;
- Administração e suporte em solução de segurança DDoS (Distributed Denial of Service), incluindo atividades conjuntas de ataques cibernéticos, junto as operadoras de Telecom.

(assinado digitalmente)

HELVIDIO CESAR MEDEIROS TERRA
Fiscal Técnico Substituto do Contrato n. 21/2014

Valter Brito Dourado Araújo

De: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>
Enviado em: sexta-feira, 3 de fevereiro de 2023 10:31
Para: Hamilton Júnior
Cc: Diego Menegazzi; ETIR; Sistemas Seguranca; Silvio Guido Alves da Silva; Herick Gervasio de Melo Souza; Willian Crisanto; georgia.dssnet@outlook.com; Elmiro Barbosa; Valter Brito Dourado Araújo
Assunto: RE: Incidente de segurança

Boa tarde.

Atendeu sim. Recebido.


Atenciosamente,

CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador(a)-Geral

Coordenação-Geral de Tecnologia da Informação - CGTI

SGAN Q.906, Módulo 'F' Bloco 'A' Ed.Celso Furtado

 (61) 2034-5713

De: Hamilton Júnior <hamiltonjr.dssnet@outlook.com>
Enviado: sexta-feira, 3 de fevereiro de 2023 10:23
Para: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>
Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>; "Silvio Guido Alves da Silva" <silvio.silva@dssnet.com.br>; Herick Gervasio de Melo Souza <herick.souza@dssnet.com.br>; Willian Crisanto - DSS <willian.crisanto@dssnet.com.br>; georgia.dssnet@outlook.com <georgia.dssnet@outlook.com>; Elmiro Barbosa <elmiro.barbosa@dssnet.com.br>; Valter Brito Dourado Araújo <valter.araujo@dssnet.com.br>
Assunto: RES: Incidente de segurança

Bom dia, Claudio!

A nota técnica enviada, atendeu a necessidade?

Pode confirmar o recebimento sobre o documento produzido pela equipe, acerca do tratamento do incidente de ataque cibernético ao MDR, em dezembro passado?

Desde já, agradeço por sua atenção!!

Cordialmente,



Hamilton Leite Cavalcante Júnior

Gerente de Serviços - Preposto

+55 61 99548-484

hamiltonjr@outlook.com

www.dssnet.com.br

De: Hamilton Júnior

Enviada em: quarta-feira, 21 de dezembro de 2022 19:16

Para: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>; "Silvio Guido Alves da Silva" <silvio.silva@dssnet.com.br>; Herick Gervasio de Melo Souza <herick.souza@dssnet.com.br>; Willian Crisanto - DSS <willian.crisanto@dssnet.com.br>; georgia.dssnet@outlook.com

Assunto: ENC: Incidente de segurança

Boa noite, Claudio.

Conforme solicitado, segue a nota técnica do incidente de segurança.

Para demais esclarecimentos, estou à disposição.

Atenciosamente,



Hamilton Leite Cavalcante Júnior

Gerente de Serviços - Preposto

+55 61 99548-484

hamiltonjr@outlook.com

www.dssnet.com.br

De: Claudio Augusto Novais Ferraz <claudio.ferraz@mdr.gov.br>

Enviada em: quarta-feira, 14 de dezembro de 2022 09:35

Para: Hamilton Leite Cavalcante Junior <hamilton.junior@dssnet.com.br>

Cc: Diego Menegazzi <diego.menegazzi@mdr.gov.br>; ETIR <etir@mdr.gov.br>; Sistemas Seguranca <sistemas.seguranca@mdr.gov.br>

Assunto: Incidente de segurança

Hamilton. Bom dia.

Destarte estarmos monitorando o ambiente após contramedidas ao incidente de segurança que indisponibilizou ou degradou os serviços de rede do MDR nesta semana, solicito iniciarmos as Análises após ações - APA.

Nesse sentido, solicitamos Nota Técnica contemplando o relato de todo incidente (ataque), evidências e ações de tratamento.

A Nota Técnica deverá ser entregue até o dia 21/12/2022, porém solicitamos registros preliminares para enviarmos ao CTIR Gov (logs e evidências) até amanhã.

Informo que foi solicitado ao Serpro a apresentação de relatório com as medidas realizadas.


Atenciosamente,


CLAUDIO AUGUSTO NOVAIS FERRAZ

Coordenador(a)-Geral

Coordenação-Geral de Tecnologia da Informação - CGTI



SGAN Q.906, Módulo 'F' Bloco 'A' Ed.Celso Furtado

 (61) 2034-5713

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA				 DSS Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	
Nome do arquivo:					Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior	



NOTA TÉCNICA

ATAQUE DE SEGURANÇA

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 2/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto			Aprovador: Hamilton Junior	

Ficha de Identificação

Título	Nota Técnica
Assunto	Ataque de Segurança
Cliente	DSS
Data de Publicação	15/12/2022
Gerente	Hamilton Leite Cavalcante Júnior
Autor	Herick Gervasio
Analista Responsável	Herick Gervasio
Revisor	Silvio Silva e Willian Crisanto
Palavras-chave	Segurança, Ataque, Appliance, DDoS
Resumo	Atividades relacionadas ao ataque realizado contra as aplicações do MDR.
Acesso	Restrito
Distribuição	N/A
Total de Páginas	10

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 3/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto			Aprovador: Hamilton Junior	

Introdução:



Este documento tem por objetivo apresentar todas as atividades executadas para interromper o ataque em direção ao Ministério do Desenvolvimento Regional - MDR, impactando suas aplicações e serviços disponibilizados para os usuários externos e internos.

Objeto:

Apresentar toda evidência, com base em logs, acessos e ações com a finalidade de impedir que o ataque de negação de serviços obtivesse sucesso, neste processo foi realizado contato com a prestadora de serviços de internet contratada pelo MDR, provedor SERPRO, que disponibiliza link de Internet e INFOVIA para as unidades Bloco E da Esplanada, 906 Norte e CENAD no Setor Policial Sul.

Evidências:

1. Relato dos usuários: Na **segunda-feira 12/12/2022 por volta das 8h30** foi identificado lentidão na rede do BLOCO E e diversas aplicações indisponíveis;
2. Partindo da premissa do ambiente saudável do MDR foi identificado que o Firewall do BLOCO E estava com excesso de conexões concorrentes e CPU em 100% de utilização conforme imagem abaixo: figura 1;
3. Devido ao excesso de conexões no Firewall não foi possível realizar acesso a caixa para coleta de logs e desta forma identificar a origem do tráfego, bem como verificar os LOGS na gerência do appliance Check Point devido os logs não estarem sendo enviados.
4. Durante a investigação foi identificado uma grande quantidade de conexões recebidas no appliance F5 Big-IP, conforme imagem abaixo: figura 2;
5. Analisando os logs do F5 foi possível identificar que alguns nodes dos pools estavam se tornando indisponíveis devido ao excesso de conexões ICMP e SSL conforme imagem abaixo: figura 3;

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 DSS Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 4/10	
Nome do arquivo:					Área Eminente: CGTI	
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior		

```

FW_906N_02  FW_FWMIA  FW_FWCENAD02

CPVIEW.Overview
-----
Overview SysInfo Network CPU I/O Software-blades Advanced
-----
CPU:
Num of CPUs:      4

  CPU  Used
  ---  ---
  1    100%
  2    100%
  3    100%
-----
Memory:
Total MB  Used MB  Free MB
-----
Physical  7,815   6,491   1,324
FW Kernel  5,688   2,821   2,867
Swap      18,457    0     18,456
-----
Network:
Bits/sec          54,368K
Packets/sec       14,200
Connections/sec   1,735
Concurrent connections 72,612
-----
Disk space (top 3 used partitions):
Partition  Total MB  Used MB  Free MB
-----
/          31,741  30,222    0
/var/log   99,193  67,872  26,200
/boot      288      50      223
-----
Events:
# of monitored daemons crashes since last cpstart  0

```

Figura 1 - Firewall CheckPoint Bloco E

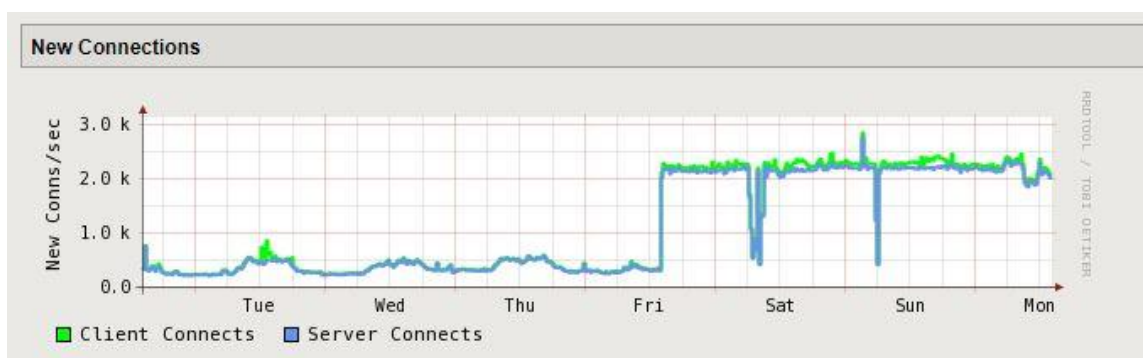




Figura 2 – Novas Conexões F5 Big-IP Bloco E

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 5/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior		

Mon Dec 12 03:47:37 BRT 2022	warning	f5blea	tmm1[12778]	011e0001	Limiting icmp unreachable response from 501 to 500 packets/sec for traffic-group /Common/traffi
Mon Dec 12 03:47:50 BRT 2022	warning	f5blea	tmm1[12778]	011e0001	Limiting icmp unreachable response from 501 to 500 packets/sec for traffic-group /Common/traffi
Mon Dec 12 04:01:08 BRT 2022	notice	f5blea	mcpd[6391]	01070638	Pool /Common/pool_webapp_inst1 member /Common/jbossh01:8080 monitor status down. [21hrs:50mins:11sec]
Mon Dec 12 04:01:08 BRT 2022	err	f5blea	tmm1[12778]	01010028	No members available for pool /Common/pool_webapp_inst1
Mon Dec 12 04:01:08 BRT 2022	err	f5blea	tmm1[12778]	01010028	No members available for pool /Common/pool_webapp_inst1
Mon Dec 12 04:01:31 BRT 2022	notice	f5blea	mcpd[6391]	01070727	Pool /Common/pool_webapp_inst1 member /Common/jbossh01:8080 monitor status up. [21hrs:50mins:11sec]
Mon Dec 12 04:01:31 BRT 2022	err	f5blea	tmm1[12778]	01010221	Pool /Common/pool_webapp_inst1 now has available members
Mon Dec 12 04:01:31 BRT 2022	err	f5blea	tmm1[12778]	01010221	Pool /Common/pool_webapp_inst1 now has available members
Mon Dec 12 04:03:52 BRT 2022	warning	f5blea	tmm1[12778]	01260013	SSL Handshake failed for TCP 185.7.214.218:55924 -> 200.168.208.237:443
Mon Dec 12 04:07:22 BRT 2022	warning	f5blea	tmm1[12778]	01260013	SSL Handshake failed for TCP 164.92.135.200:57072 -> 200.168.208.237:443

Figura 3 - Logs F5 Big-IP Bloco E

6. Através dos logs do F5 Big-IP do BLOCO E coletamos alguns IPs externos que mais se repetiam e construímos uma black-list para aplicar no Firewall, porém devido à alta carga de processamento só foi possível aplicar as configurações após várias tentativas, essa medida não surtiu o efeito esperado, mantendo a caixa com alto processamento.
7. Realizando uma análise minuciosa dos logs no F5 Big-IP, foi identificado que se tratava de um ataque coordenado de DDoS que apresentavam origens de diversos países.
8. É importante ressaltar que não possuímos licença para WAF nos appliances F5 Big-IP para mitigação e proteção contra-ataques cibernéticos, desta forma com o apoio de uma revendedora decidimos como medida de contenção criar uma regra do tipo iRule no appliance, de forma a bloquear outros países, permitindo assim somente sessões originadas por endereços do Brasil (BR).
9. Como os links de internet do MDR são providos pelo SERPRO, acionamos o suporte da fornecedora para mitigar em conjunto o ataque de DDoS, após o fornecimento dos IPs publicados no MDR recebemos a imagem abaixo informando o resultado das tratativas realizadas no qual pode ser observado em vermelho o tráfego bloqueado;



 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 DSS Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 6/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior		



Figura 4 - Tráfego SERPRO

10. Após realizar todas as alternativas possíveis, em atividades de atuação de bloqueio para países externos e bloqueios por parte da Serpro percebemos uma queda substancial nas novas conexões ao MDR, perdendo força no ataque, resultado obtido por **volta das 22h15 de 12/12/2022** conforme imagem abaixo: figura 5;

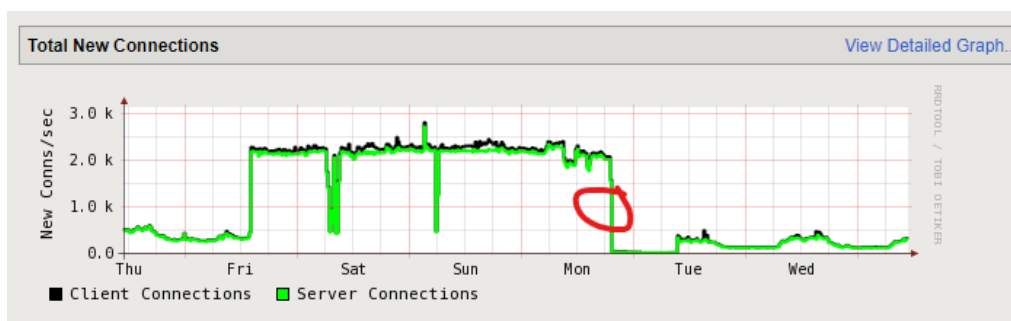




Figura 5 - Novas Conexões F5 Big-IP Bloco E

11. Com todos os procedimentos adotados passamos a receber somente requisições originadas no Brasil conforme imagem abaixo: figura 6;
12. Após controle dos ataques de DDoS no appliance F5 Big-IP e encerramento do expediente dos usuários, **por volta das 22h30 do dia 12/12/2022** conseguimos ter acesso aos logs do Firewall e mesmo assim persistia uma quantidade alta de conexões correntes.

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 7/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior		



```

f5cenada
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 40.69.174.70/US
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.17.128.73/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.35.4/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.222.53.7/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.37.3/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 164.163.84.74/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 164.163.84.74/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 187.45.125.202/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 143.244.35.66/US
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.253.230.4/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.253.230.3/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 189.6.0.182/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.82.0.66/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 45.231.140.198/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 177.184.106.82/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 152.255.15.162/BR
Dec 12 20:05:56 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 187.64.0.112/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 170.82.124.50/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 168.205.243.146/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 131.161.24.98/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 54.214.180.4/US
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.37.3/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.35.129/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 143.244.35.66/US
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 143.244.35.66/US
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 177.36.54.3/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 187.19.144.18/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.37.2/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.35.3/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.253.230.4/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.253.234.4/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.37.1/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 186.223.128.17/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 189.6.0.173/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 189.6.0.177/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 172.217.37.5/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 168.90.146.202/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.169.116.229/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 45.6.229.107/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 199.122.126.146/US
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.82.0.71/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.169.116.228/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 186.223.128.92/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 186.223.128.92/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.17.128.73/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.17.128.73/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.17.128.73/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 189.4.0.191/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 201.76.1.212/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.19.135.135/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 191.254.30.216/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.19.135.135/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.19.135.135/BR
Dec 12 20:05:57 f5cenada info tmm1[13216]: Rule /Common/Irule_Geolocation <FLOW_INIT>: IP Address/Counry 200.19.135.135/BR

```

Figura 6 - Log F5 Big-IP Bloco E

13. Desta forma iniciamos uma nova investigação, no qual foi possível verificar que essas conexões eram originadas de um servidor interno do Bloco E, referente a publicação dos serviços do S2ID conforme imagem abaixo: figura 7;

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 DSS Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 8/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto			Aprovador: Hamilton Junior	

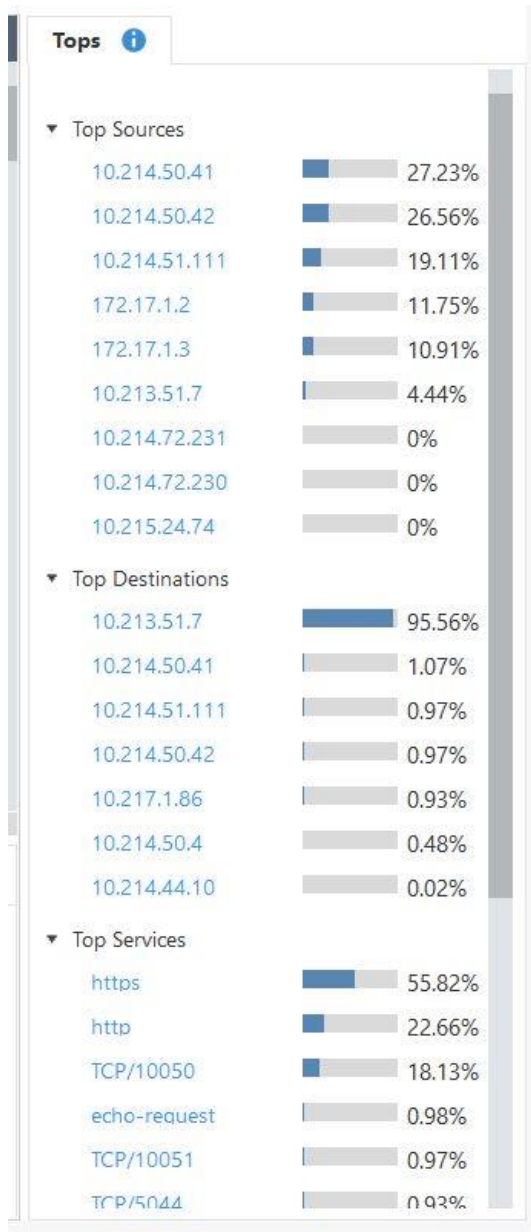


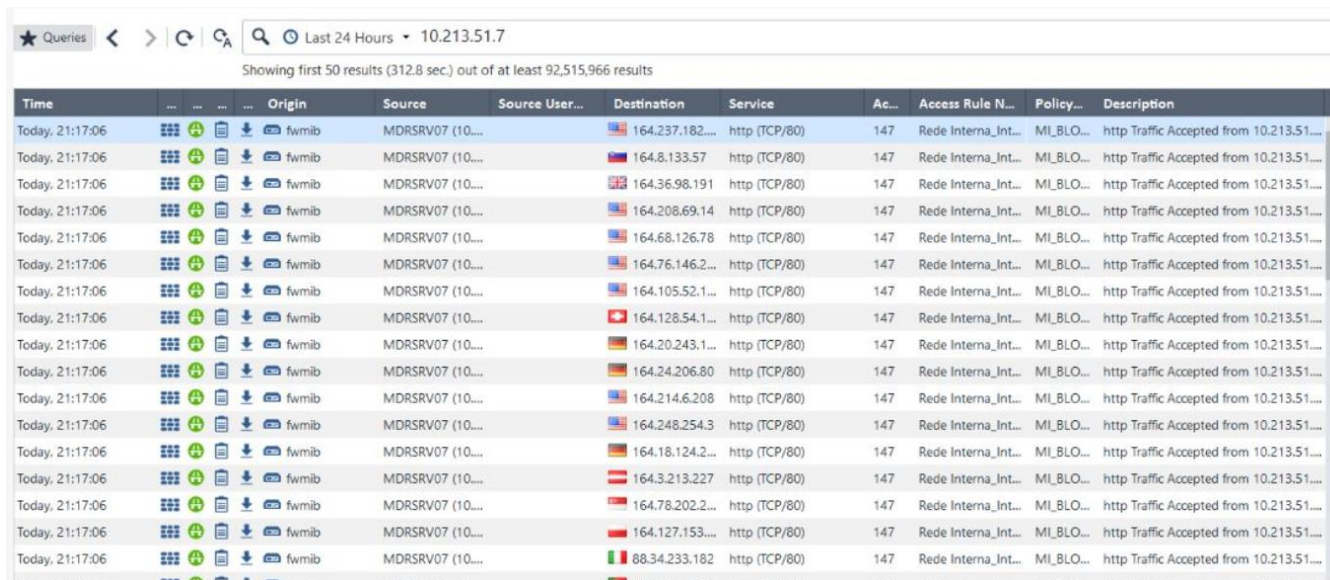


Figura 7 - Sessões CheckPoint Bloco E

14. Verificamos que esse servidor estava realizando diversas solicitações de acessos na porta 80 a diversos países conforme imagem abaixo: figura 8;



 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 9/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto		Aprovador: Hamilton Junior		



Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.237.182...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.8.133.57	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.36.98.191	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.208.69.14	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.68.126.78	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.76.146.2...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.105.52.1...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.128.54.1...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.20.243.1...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.24.206.80	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.214.6.208	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.248.254.3	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.18.124.2...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.3.213.227	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.78.202.2...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		164.127.153...	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...
Today, 21:17:06	fwmib	MDRSRV07 (10...		88.34.233.182	http (TCP/80)		147	Rede Interna_Int...	ML_BLO... http Traffic Accepted from 10.213.51...

Figura 8 - Logs CleckPoint Bloco E

15. Devido ao comportamento suspeito a equipe de aplicação identificou alguns processos no servidor Linux não pertencentes a aplicação do S2ID, demonstrando vulnerabilidade do mesmo.
16. Devido a circunstância o servidor foi desligado, e com isso o excesso de novas conexões concorrentes no Firewall normalizaram, **sendo registrado na terça-feira, 13/12/2022 por volta de 1h00 da manhã.**
17. Por se tratar de uma aplicação fundamental ao MDR, foi restaurado o backup do servidor para uma data anterior ao ataque e realizado diversas medidas de proteção para o mesmo, como troca das credenciais administrativas e mudança IP interno.
18. Após a realização de todas as medidas informadas não detectamos mais ataques externos ao appliance F5 Big-IP como no Firewall.
19. É importante ressaltar que após os ataques, e aplicado as regras para contorno ao mesmo, tivemos como falhas o não recebimentos de e-mails externos ao domínio MDR e acessos negados a VPN, aos quais se encontravam em países externos.
20. Para sanar as falhas de comunicação de e-mail foram desabilitados as regras de proteção Geográfica por meio das iRules, **atividade realizada no dia 14/12/2022 por volta das 13h.**

 Ministério do Desenvolvimento Regional	NOTA TÉCNICA					 Serviços de Tecnologia da Informação
	Data de criação 15/12/2022	Data de revisão Nota Técnica	Validade	Versão 1.0	Folha: 10/10	
Nome do arquivo:						Área Eminente: CGTI
Elaborador: Herick Souza		Revisor: Silvio Silva e Willian Crisanto			Aprovador: Hamilton Junior	

Conclusão:

Foram realizadas todas as tratativas possíveis com os ativos presentes no MDR para impedir que o ataque sofrido obtivesse sucesso, no qual foi fundamental o apoio da equipe de segurança do SERPRO mitigando os acessos dentro da própria operadora, bem como o apoio do fabricante do appliance F5 Big-IP, no qual um Especialista realizou todo procedimento possível para descartar os acessos indevidos.

Durante este processo foi identificado a necessidade de atualização dos ativos do MDR, no qual, já se encontra processo licitatório em andamento, este que deve garantir maior segurança e respostas mais rápidas a futuros incidentes.