Comissão Mista de Reavaliação de Informações

139ª Reunião Ordinária

Decisão CMRI nº 492/2024/CMRI/CC/PR

NUP: 23546.041372-2024-18
Órgão: UFPA – Universidade Federal do Pará
Requerente: A.L.S.

Resumo do Pedido

Requerente fez um arrazoado referindo-se a falhas do SigEleição, ao longo do dia 17/04/2024, que comprometeram o processo de consulta para escolha dos novos dirigentes da Universidade Federal do Pará (UFPA), alegando que houve interrupção por várias horas e instabilidades ao longo do processo de votação. Assim sendo, solicitou a obtenção dos Logs completos do firewall CTIC/UFPA, no intervalo compreendido entre 8h30min e 21h15min, do dia 17/04/2024, segmentado a cada 30 minutos e por campus da UFPA, contendo:

1)Todas os acessos e tentativas de acesso ao servidor do SigEleição;
2) As respectivas localizações dos acessos e tentativas de acesso ao servidor do SigEleição;
3) Os respectivos horários dos acessos e tentativas de acesso ao servidor do SigEleição;
4) Eventuais acessos e tentativas de acesso ao servidor do SigEleição, que se caracterizem como padrão de "bots";
5) Eventuais acessos e tentativas de acesso ao servidor do SigEleição que tenham sido realizados a partir da rede da RNP, mas que não tenham sido de campi da UFPA.

Além das informações do firewall, solicitou também as seguintes informações:
6) Informações de todas as paradas e retornos do sistema, ao longo do período supracitado;
7) Informações de hardware e software dos servidores computacionais acrescentados à configuração inicial do sistema;
8) Registro de votos ao longo do dia;
9) Registro de votos ao longo do dia por campi.

Resposta do órgão requerido

O Centro de Tecnologia da Informação e Comunicação (CTIC) da UFPA informou que a Universidade é um Autonomous System (AS), ou um sistema autônomo identificado pelo nº ASN 262511, que é um grupo de um ou mais prefixos de endereçamento IP (Internet Protocol) e nome registro de domínios como ufpa.br e ufpa.edu.br. Assim, explicou que, tecnicamente a UFPA é responsável por gerenciar todo o seu bloco de endereços IPs, roteamento e publicar externamente seus domínios de Internet, sem a necessidade de um provedor externo, o que a coloca como um provedor de Internet para toda sua comunidade universitária. Dentre as diversas obrigações que um provedor de Internet possui, o registro de conexão de usuários está entre os principais e está descrito na Lei Nº 12.965/2014. Nesse contexto, afirmou que os arquivos de logs solicitados contêm informações técnicas e detalhes da infraestrutura do sistema, endereçamento IP da UFPA e redes externas, destacando que os dados solicitados irão identificar diretamente os usuários do sistema, endereços IPs de suas conexões com data e hora. Assim, negou o acesso com base no Art. 7º, inciso VII e Art. 10º, parágrafo 2º da Lei nº 12.965/2014.

Recurso em 1ª instância

Reiterou o pedido por meio de extenso arrazoado, argumentando em suma que houve falha no funcionamento do SigEleição no momento da consulta a comunidade e que o Parecer apresentado pelo setor destaca o impedimento/dificuldade de acesso de 1.914 eleitores (as) das três categorias que não entraram na sala de votação, não conseguiram votar e depois não retornaram, ou seja, não tentaram votar em outro momento, ao longo do dia, pela dificuldade de acesso. Apontou que esse número representaria um acréscimo de aproximadamente 13% no número de eleitores, se fossem levados em consideração os 15.032 eleitores que votaram no pleito, assim, ponderou que esses números não são desprezíveis, pois poderiam alterar significativamente a participação das categorias, mesmo que não alterasse o resultado final da eleição. Assim, entendeu que as informações solicitadas, os logs requisitados referentes ao SIGELEIÇÃO, não implicam qualquer exposição da infraestrutura da UFPA, nem representam um risco para a segurança dos usuários. Quanto à identificação direta do usuário, ressaltou que um endereço IP por si só não tem a capacidade de identificar diretamente um usuário específico. Isso é especialmente verdadeiro nas redes da UFPA, que utilizam sistemas de endereçamento dinâmico via DHCP em sua maioria. Prosseguiu afirmando que os logs não incluem dados pessoais dos usuários, como login, nome, número de telefone, RG, CPF, endereço físico do dispositivo ou informações sensíveis que possam violar a privacidade dos indivíduos. Portanto, concluiu que a disponibilização desses logs não representa qualquer ameaça à segurança da infraestrutura da UFPA ou à privacidade dos usuários.

Resposta do órgão ao recurso em 1ª instância

Ratificou a resposta inicial, ademais ponderou que o sistema SigEleição faz parte de um conjunto de sistemas que formam o sistema integrado de gestão da Universidade, o SIG-UFPA. Por mais que a solicitação seja direcionada ao SigEleição, as informações solicitadas possuem dados da rede da UFPA, rede dos usuários externos, dados sobre o servidor do SigEleição, dados dos dispositivos utilizados pelos usuários, etc, o que compromete os demais sistemas e serviços por utilizarem a mesma rede e endereçamento IP do data center institucional. Considerou que, um ataque cibernético pode ser realizado através da exploração de vulnerabilidades, engenharia social, desatualização de sistemas operacionais etc. Toda a informação obtida sobre o ambiente alvo do atacante é utilizada para explorar qualquer falha na rede ou arquitetura dos sistemas, levando ao êxito do atacante. Ressaltou que não houve invasão do SigEleição, mas apenas possivelmente tentativa de sobrecarregar os canais de acesso, dificultando a votação para o eleitor regular. No caso dessa hipótese informou que isto ainda está em avaliação. De outro lado, afirmou que todos os usuários que persistiram conseguiram exercer o direito de voto.

Recurso em 2ª instância

Reiterou o recurso por meio de extenso arrazoado que em suma replica os argumentos do recurso anterior, bem como contrapôs a base legal da negativa, o Art. 7º, inciso VII e Art. 10, § 2º da Leiº 12.965/2014, que trata de não fornecimento de dados pessoais, de conexões, conteúdos de comunicações privadas, da vida privada, da honra e da imagem direta ou indiretamente envolvidas, a não ser por força de lei ou mediante ordem judicial. Nesse sentido, argumentou que os Logs não trazem informações da infraestrutura da UFPA e o endereço de IP não tem a capacidade de identificar o usuário, portanto a disponibilidade das informações não compromete a segurança da infraestrutura da UFPA, nem o sigilo de dados pessoais, mesmo assim, se algum técnico em informática insistir nessa versão, o CTIC teria como anomizá-los e fornecer as demais informações. Um conhecedor de TI externo poderá confirmar que a infraestrutura da UFPA está salvaguardada, bem como os dados das pessoas não estão expostos pelos endereços dos IPs. Sobre a estrutura do firewall da UFPA e acerca do IP, alegou que o próprio CTIC já divulgou informações sobre a estrutura de firewall da UFPA publicamente na Internet. Durante o evento denominado WorkShop CTIC, realizado em dezembro de 2023, os slides apresentados incluíam detalhes sobre a estrutura de firewall (até mesmo os endereços IP utilizados). Especificamente, o décimo slide do Workshop CTIC disponibilizado em https://www.ctic.ufpa.br/publicacoes/documentos/workshop2023/CSIC.pdf mostrou essas informações de forma transparente. Ainda de acordo com o décimo slide citado anteriormente do workshop, A UFPA utiliza o equipamento Fortinet Fortigate 300D como parte de sua infraestrutura de firewall. O material informativo do “WORKSHOP CTIC 2023” elaborado pela Coordenadoria de Segurança da Informação e Comunicação da UFPA, está disponível publicamente na internet, apresenta a infraestrutura da UFPA, além da situação de vulnerabilidade do próprio sistema, deixando claro a dificuldade de gerenciamento de riscos e de respostas aos incidentes.

Resposta do órgão ao recurso em 2ª instância

A recorrida, por meio de extenso arrazoado, prestou diversos esclarecimentos e informações, que serão resumidamente pontuadas. Precipuamente comunicou que a publicação de informação técnica da infraestrutura da rede da UFPA na internet foi imediatamente retirada, por se entender que são informações que não deveriam estar expostas. Ademais, prosseguiu considerando que as referidas informações que foram expostas na internet não apresentaram nenhuma relação com o problema ocorrido no dia da consulta à comunidade para escolha de reitor (a) e vice-reitor(a), pois, conforme já mencionado em respostas anteriores, o problema técnico ocorreu na comunicação da aplicação com o banco de dados para resgatar os dados sobre a eleição. Ato contínuo, esclareceu que o número informado na resposta da petição nº 4, de 1.941 eleitores, é o resultado da subtração do número total de eleitores diferentes e o número de votos computados. De modo que, em nenhum momento foi taxado que esse número é de eleitores das três categorias, que não conseguiram entrar novamente no sistema para votar e muito menos em qual chapa seria o seu voto, branco, nulo ou simplesmente que não desejaram participar do pleito. Seguiu afirmando que o código fonte do sistema SigEleição sempre esteve disponível para qualquer usuário poder realizar auditoria, conforme respondido a COC na petição nº 6. Informou que ao todo foram realizados 35.932 acessos, ou seja, os logins realizados com sucesso pelos eleitores. Quanto às tentativas de acesso explicou que não é possível registrar se não houver login com sucesso. Sobre as respectivas localizações dos acessos e tentativas de acesso ao servidor do SigEleição declarou que é uma atividade inviável de realizar, devido ao número de endereços IPs que foram registrados, pois afirmou não possuir ferramenta computacional baseada em software livre que faça a localização geográfica de endereços IPs em massa. Somou a isso o endereçamento via Network Address Translation (NAT) realizados por provedores externos ao qual não possui nenhuma gerência. Informou que os horários de acesso estão descritos no link https://drive.google.com/file/d/1WBmuK_iKUqBNLQeEFrbRVQgRq9ZeyyLX/view?usp=sharing. Quanto às tentativas de acesso declarou que não é possível registrar se o usuário não realizou o login com sucesso. Assim, declarou expressamente que não podem identificar de forma taxativa a quantidade total de acessos à página web do SigEleição efetuadas por robôs. Nesse sentido, explicou que durante o processo de login é necessário responder uma pergunta gerada aleatoriamente, que é uma ferramenta justamente para evitar que o acesso seja feito por robôs no tipo de ataque de força bruta. Com relação à Rede Nacional de Pesquisa (RNP) explicou que é uma operadora de Internet independente e que possui autonomia no gerenciamento de seu endereçamento IP, portanto, somente o RNP possui autoridade para responder, caso julgue procedente, de forma precisa sobre a solicitação de seus endereços Ips. Ainda, informou que o sistema SigEleição ficou paralisado em 4 (quatro) períodos, e todas as vezes em que ficou inoperante, a presidente da comissão necessitou entrar com a chave de segurança para poder liberar a cabine de votação aos eleitores. Os períodos foram aproximadamente de: 09:09h até 11:09h; 11:40h até 11:50; 12:30 até 12:35; 15:25 até 15:31. Informou que foi apresentado gráfico representando a quantidade de votos registrados a cada hora da eleição, compreendendo o intervalo de 9:00h até as 21:00h, gráfico este que fez parte da tela de acompanhamento da eleição e que estava disponível a todos os presentes no auditório. Nesse particular, destacou-se que no intervalo de 10:00h às 11:00h não houve registro de votos porque o sistema estava inoperante, portanto, o módulo de registro de votos não poderia computar e registrar nenhum voto no banco de dados. Ademais, esclareceu que a configuração da eleição foi feita para o eleitor poder realizar o seu voto de qualquer localidade, por intermédio de um computador ou dispositivo móvel com acesso à Internet. Para esse formato torna-se imprescindível existir uma única "cabine virtual", que registre os eleitores como aptos cadastrados a votar, divididos por categoria: docentes, técnicos e discentes. Portanto, não é possível o registro de votação por campi, pois não há distribuição de cabines de votação por unidades. Por fim, quanto ao pedido logs completos do firewall CTIC/UFPA e do Sistema SigEleição reforçou os motivos da negativa de acesso, ponderando que tais logs contêm informações sensíveis e estratégicas relacionadas à segurança da informação e ao funcionamento dos sistemas da Universidade, que por mais que seja um sistema específico, todos compartilham o mesmo ambiente do data center institucional. Nesse contexto, pontuou diversas razões para a referida negativa, tendo em vista que a disponibilização pretendida.

Recurso à Controladoria-Geral da União (CGU)

Reiterou o pedido nos mesmos termos apresentados anteriormente.

Análise da CGU

A CGU considerou que matéria semelhante já foi objeto de avaliação pela Casa em diversos precedentes, dentre os quais destacou o NUP 21210.011394/2022-40, no qual foi relatado que, em uma pesquisa em sites especializados na matéria, alguns dos ataques cibernéticos utilizam de técnicas de engenharia social visando manipular as pessoas para que revelem dados pessoais ou corporativos, utilizando-se de métodos psicológicos de persuasão e convencimento, para obter informações e inserir vírus de forma ilícita. No âmbito da segurança cibernética, os ataques virtuais por meio da engenharia social atingem pessoas desatentas que podem ter seus computadores infectados por vírus e podem permitir, de forma não intencional, que senhas, dados e informações corporativas sejam roubadas. Assim, vislumbrou que a divulgação de informações sobre o sistema tem o potencial de fragilizar as estratégias de controle da segurança de rede de computadores e, por consequência, pode gerar danos relacionados com o vazamento de informações que seriam de acesso restrito; pode propiciar diversos tipos de ataques cibernéticos e pode violar sigilos e frustrar as garantias e os direitos de usuários previstos na Lei nº 12.965/2014. Assim, entendeu que o atendimento desse tipo de pedido poderia ultrapassar o limite do razoável para o Estado e a sociedade e, assim, ferir o interesse público. Adicionalmente, ressaltou o Marco Civil da Internet (art. 7º e art. 10º da Lei12.965/2014) que reconhece a importância da privacidade, da segurança e da proteção dos dados dos usuários e registro de conexões.

Decisão da CGU

A CGU opinou pelo conhecimento e, no mérito, pelo desprovimento do recurso, devido ao pedido ser desarrazoado por não atender ao interesse público, nos termos do inciso II do art. 13 do Decreto nº 7.724/2012.

Recurso à Comissão Mista de Reavaliação de Informações (CMRI)

Argumentou que o acesso ao log da eleição será fundamental para esclarecer as tentativas de ataque ao sistema eleitoral da UFPA, o que demonstra as fragilidades do sistema e a dificuldade em garantir idoneidade ao processo de escolha de Reitor (a) da UFPA.

Admissibilidade do recurso à CMRI

Recurso conhecido. Conforme o art. 24 do Decreto nº 7.724, de 2012, e os arts. 19 e 20 da Resolução CMRI nº 6, de 2022, o recurso cumpre os requisitos de legitimidade, tempestividade, cabimento e regularidade formal.

Análise da CMRI

Em análise ao presente recurso, precipuamente, observou-se que o recorrente de maneira pontual reiterou o log da eleição, sendo assim, para fim de avaliação desta comissão, destaca-se que a análise será direcionada apenas a esta parte do pedido, pois entendeu-se que sobre os demais itens o requerente aceitou os esclarecimentos e informações prestadas pela UFPA. Particularmente, sobre a resposta do órgão na 2ª instância recursal, apesar da análise da CGU não ter relatado em seu parecer, importa resumir o que ali foi informado para cada item da solicitação. Naquele contexto, constatou-se que os itens 1 e 3 do pedido foram atendidos parcialmente, conforme o disposto no art. 7º da LAI, e para parte não atendida, a UFPA declarou a respectiva inexistência de dados, apresentando as razões pertinentes. Verificou-se ainda que a inexistência também foi conferida aos itens 2, 4, 5 e 9 com a apresentação das devidas justificativas. Logo, nesses casos, destaca-se que não há negativa de acesso, pois com base na Súmula CMRI nº 06/2015, a declaração de inexistência de informação objeto de solicitação constitui resposta de natureza satisfativa. Ademais, quanto aos itens 6 e 8 o pedido foi atendido integralmente, em cumprimento à Lei nº 12.527/2011. Posto isto, com relação aos logs completos do firewall CTIC/UFPA e do Sistema SigEleição, a UFPA negou o acesso argumentando que tais logs contêm informações sensíveis e estratégicas relacionadas à segurança da informação e ao funcionamento dos sistemas da Universidade, que por mais que seja um sistema específico, todos compartilham o mesmo ambiente do data center institucional. Nesse contexto, pontuou que a divulgação de logs pode expor vulnerabilidades, endereços IPs, padrões de tráfego de rede, acessos, regras aplicadas, e outras informações que podem ser exploradas por atacantes; podendo causar o aumento do risco de invasões, ataques cibernéticos e comprometimento da infraestrutura tecnológica da UFPA. Ademais, ponderou que os logs no caso do sistema SigEleição contêm os logins, nomes e endereços IPs de sua autenticação, assim, a disponibilização pública de logs poderia violar regulamentações de privacidade, conforme a Lei Geral de Proteção de Dados (LGPD). Considerou ainda que os arquivos de logs devem ser acessados apenas por pessoas autorizadas, como administradores de sistemas, equipes de segurança e desenvolvedores de sistemas do CTIC, pois o controle de acesso é essencial para garantir a integridade e a confidencialidade desses registros com fim a evitar o vazamento de informações sensíveis. Portanto, com base no explicado pela UFPA, esta Comissão observou que todas as informações públicas existentes referentes ao pedido foram disponibilizadas ao recorrente, com exceção dos logs completos do firewall CTIC/UFPA e do Sistema SigEleição, pois a recorrida demonstrou a impossibilidade do respectivo atendimento, explicando que a ostensividade pretendida conferiria perigo à segurança da informação e aos sistemas da Instituição. Logo, em que pese a não aceitação do recorrente ante à negativa, pondera-se que a disponibilização fere o interesse público, nesse âmbito, importa destacar que o Decreto nº 7.724/2012 foi expresso em resguardá-lo, quando dispôs em seu art. 13 que não serão atendidos pedidos desarrazoados. Assim, tratando-se o presente recurso de pedido que se caracteriza desarrazoado, haja vista que está em desconformidade com os interesses públicos do Estado em prol da sociedade, deve-se acolher a negativa de acesso nos termos ora expostos.

Decisão da CMRI

A Comissão Mista de Reavaliação de Informações, por unanimidade, decide pelo conhecimento do recurso, e no mérito, pelo indeferimento, devido ao pedido ser desarrazoado, nos termos do inciso II do art. 13 do Decreto nº 7.724/2012.

Documento assinado eletronicamente por **Pedro Helena Pontual Machado**, **Secretário(a)-Executivo(a) Adjunto(a)**, em 12/12/2024, às 18:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **CARLOS AUGUSTO MOREIRA ARAUJO**, **Usuário Externo**, em 13/12/2024, às 17:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Jorge Luiz Mendes de Assis**, **Usuário Externo**, em 13/12/2024, às 22:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **LEILA DE MORAIS**, **Usuário Externo**, em 16/12/2024, às 09:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marco Aurélio de Andrade Lima**, **Chefe de Gabinete**, em 16/12/2024, às 09:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Eveline Martins Brito**, **Usuário Externo**, em 16/12/2024, às 14:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **PAULO ROCHA CYPRIANO**, **Usuário Externo**, em 23/12/2024, às 10:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade do documento pode ser conferida informando o código verificador **6280264** e o código CRC **D5CA6D25** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00131.000031/2024-51 SEI nº 6280264