INCIDENTE CIBERNÉTICO NA AGÊNCIA NACIONAL DE ÁGUAS E SANEAMENTO BÁSICO (ANA) EM 2023: LIÇÕES E APRENDIZADOS

Marco Antonio Silva[1], Guilherme Simão da Costa[2]

Abstract: In September 2023, the Brazilian National Water and Sanitation Agency (ANA) was targeted by a high-severity cyberattack. The incident, caused by BlackSuit ransomware, affected the confidentiality, integrity, and availability of critical data and services. The agency promptly activated its Cyber Crisis Management Plan, implementing emergency containment measures, clear communication with stakeholders, and coordination with specialized government entities. The technical investigation revealed security flaws such as lack of multi-factor authentication, excessive permissions, and poor network segmentation. As a result, ANA adopted structural corrective actions, including full infrastructure reconfiguration, deployment of advanced security solutions, and access policy review. This paper describes the incident, analyzes its root causes and impacts, and highlights key lessons learned, contributing to the improvement of cybersecurity resilience in water resources management entity.

Resumo: Em setembro de 2023, a Agência Nacional de Águas e Saneamento Básico (ANA) foi alvo de um ataque cibernético classificado como de alta severidade. O incidente, provocado por um *ransomware* do tipo *BlackSuit,* comprometeu a confidencialidade, integridade e disponibilidade de dados e serviços críticos da instituição. A resposta envolveu a rápida ativação do Plano de Gerenciamento de Crise Cibernética da ANA, com adoção de medidas emergenciais de contenção, comunicação transparente com os públicos interno e externo e articulação com órgãos governamentais especializados. A investigação técnica apontou fragilidades como ausência de autenticação multifator na VPN, permissões excessivas e falhas na segmentação da rede. Como resultado, a Agência adotou um conjunto de medidas corretivas estruturantes, como a reconfiguração completa da infraestrutura, implementação de soluções de segurança avançadas e revisão de políticas de acesso. Este artigo descreve o incidente, analisa suas causas e impactos e compartilha as principais lições aprendidas com a experiência, visando contribuir para o fortalecimento da resiliência cibernética nos órgãos gestores de recursos hídricos.

Palavras-Chave: incidente cibernético; segurança da informação; ciberataque

1 - INTRODUÇÃO

Em setembro de 2023, a Agência Nacional de Águas e Saneamento Básico (ANA) enfrentou um incidente cibernético de alta gravidade. Tratou-se de um ataque do tipo *ransomware*, identificado como *BlackSuit*, que afetou a disponibilidade, confidencialidade e integridade de seus dados e serviços essenciais. A crescente complexidade dos ataques cibernéticos exige das instituições públicas maior preparação, planejamento e capacidade de resposta (CIS).

Os ataques cibernéticos estão se tornando cada vez mais frequentes e sofisticados em todo o mundo. Grupos criminosos estão realizando ataques visando desde infraestruturas críticas até informações sensíveis de empresas e governos. A crescente dependência da tecnologia aumenta a vulnerabilidade a esses ataques, tornando a segurança cibernética uma preocupação global. Esses ataques têm impactos em diferentes níveis, podendo causar enormes danos financeiros a empresas e indivíduos, levar à perda de dados confidenciais, interrupção de serviços essenciais e até a extorsão financeira.

A segurança da informação tornou-se uma prioridade estratégica para as instituições públicas na era digital. O volume crescente de dados sensíveis administrados por esses órgãos, incluindo informações pessoais de cidadãos, processos administrativos e operações críticas do Estado, evidencia a necessidade

[1] Agência Nacional de Águas e Saneamento Básico (ANA), 61-2109-5379, marcosilva@ana.gov.br
[2] Agência Nacional de Águas e Saneamento Básico (ANA), 61-2109-5122, guilherme.costa@ana.gov.br

de proteger esses ativos contra acessos não autorizados, perda ou modificação indevida. Um incidente de segurança pode comprometer não só o funcionamento institucional, mas também a confiança da sociedade na capacidade do setor público de zelar por informações fundamentais ao exercício da cidadania.

Além disso, o aumento de ameaças cibernéticas, como *ransomwares*, *phishing* e ataques de negação de serviço, coloca em risco a continuidade dos serviços públicos. Como esses serviços muitas vezes atendem demandas essenciais da população, interrupções podem gerar impactos sociais, econômicos e até mesmo políticos. Proteger os sistemas contra esses riscos é garantir o pleno funcionamento da Administração Pública, a continuidade de políticas públicas e a integridade das informações sob tutela do Estado.

Outro aspecto relevante é que a transformação digital, acelerada pela necessidade de modernização e eficiência no setor público, amplia a superfície de ataque por meio de novos sistemas, integrações e serviços digitais. Dessa forma, a gestão eficiente da segurança da informação deve ser dinâmica e adaptável, acompanhando a evolução das ameaças e incorporando inovações tecnológicas para prevenção, detecção e resposta a incidentes.

Por fim, é fundamental destacar que a segurança da informação não é apenas uma preocupação tecnológica, mas um desafio organizacional e de gestão de pessoas. O desenvolvimento de políticas robustas, treinamentos regulares para servidores e colaboradores, sensibilização de todos os usuários e a integração entre diferentes áreas da instituição são pilares essenciais. Assim, fortalecer a segurança da informação no setor público é um requisito básico para garantir a prestação de serviços confiáveis, íntegros e eficientes para toda a sociedade.

Este artigo apresenta um relato do incidente cibernético ocorrido na ANA. Primeiro, traz uma contextualização da segurança da informação, descreve a detecção e resposta inicial ao incidente, analisa como o incidente aconteceu, enumera os impactos, descreve a estratégia de recuperação, as ações corretivas implementadas após o incidente, trata da comunicação e governança do incidente e das lições aprendidas.

2 - CONTEXTO DA SEGURANÇA DA INFORMAÇÃO NA ANA

No Plano Estratégico Institucional da ANA – PEI (ANA, 2023), consta o objetivo estratégico da segurança da informação da Agência, conforme descrito no Objetivo Estratégico 16:

- **OE 16**: Fomentar a cultura de gestão de riscos, de integridade, da segurança da informação e proteção de dados.

Descrição: Promover ações contínuas de conscientização e sensibilização voltadas ao desenvolvimento de habilidades em gestão de riscos, integridade, segurança da informação e proteção de dados.

A partir do objetivo estratégico disposto no plano estratégico da ANA, a Superintendência de Tecnologia da Informação (STI) definiu objetivo e iniciativas estratégicas de segurança da informação no Plano Estratégico de Tecnologia da Informação e Comunicações – PETIC (ANA, 2024), conforme abaixo.

- **OE TIC 06**: Aprimorar o ecossistema de Segurança da Informação e Comunicações.

IP6.1 – Implantar soluções tecnológicas de segurança cibernética integrada
IP6.2 – Fomentar a cultura de privacidade e segurança da informação
IP6.3 – Estabelecer e aprimorar os processos de gestão de segurança da informação

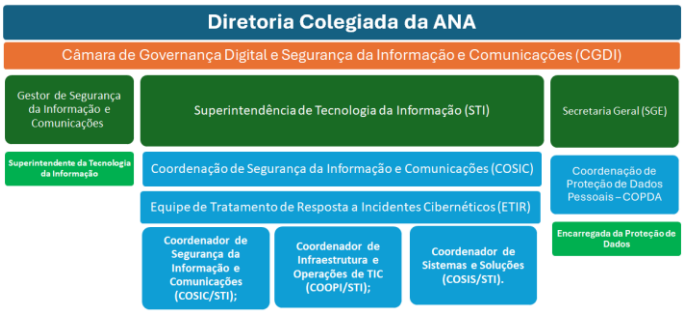
Anteriormente à ocorrência do incidente cibernético, a Agência já possuía uma estrutura de segurança a informação, com a definição de responsabilidades, processos e atividades. Essa estrutura é formada por unidades operacionais e estratégicas, conforme figura 1. A segurança da informação está sob a responsabilidade da STI. Dentro dessa unidade, o tema está sob gestão da Coordenação de Segurança da Informação e Comunicações (COSIC) e a implementação fica sob a responsabilidade da Coordenação de Operação de Infraestrutura de TIC (COOPI) e da Coordenação de Soluções e Sistemas (COSIS). A

Câmara de Governança Digital e Segurança da Informação (CGDI) e a Diretoria Colegiada (DIREC) são unidades estratégicas.

Destaca-se o papel da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), formada pelos coordenadores de segurança da informação, de operação de infraestrutura e de soluções e sistemas e do Gestor de Segurança da Informação e Comunicações, que tem a função precípua de executar o processo de gestão dos incidentes e definir as ações imediatas quando da ocorrência de um incidente de segurança. Completa a estrutura, a Coordenação de Proteção de Dados Pessoais (COPDA), ligado à Secretaria Geral (SGE) que tratar especificamente da proteção e o tratamento dos dados pessoais no âmbito dos processos da ANA.

Além da estrutura, a ANA conta com normativos, ferramentas e ações que operacionalizam a segurança da informação no ambiente tecnológico da Agência, conforme listados a seguir.

Figura 1 – Estrutura de segurança da informação na ANA



- Política de Segurança da Informação e Comunicações (POSIC) publicada e implementada, que aborda gestão de senhas, controle de acesso e resposta a incidentes. É um documento que reúne um conjunto de ações, regras e boas práticas para utilização dos dados e informações institucionais;

- Plano de Continuidade em TI, Plano de Gerenciamento de Crise Cibernética, Plano de Contingência Operacional e o relatório de Análise de Impacto no Negócio (BIA) do inglês *Bussiness Impact Analyst*;

- Inventário e Controle de Ativos de hardware e Software por meio de tecnologias de monitoramento e processo de homologação de software;

- Gestão de vulnerabilidades: realização de avaliação de vulnerabilidades a fim de aplicar *patches* e atualizações de segurança;

- Política de *backup*[3] e recuperação de dados, que incluía *backup* regulares e automáticos dos dados e máquinas virtuais críticas. Os *backups* eram armazenados em locais seguros, incluindo armazenamento em nuvem, que garantia que os *backups* estejam em outro ambiente tecnológico, dificultando o acesso;

- Realização de Testes de Restauração de *backups* de forma regulares para garantir que os dados pudessem ser recuperados rapidamente e com integridade;

- Implementação de testes de penetração (PENTESTS[4]) para identificar vulnerabilidades e fortalecer defesas e campanha de simulação de ataque *phishing*[5], que direcionava os usuários para curso de segurança, caso fornecessem suas credenciais;

[3] *Backups* é o processo de criar cópias de dados digitais para proteger contra perdas, danos ou falhas. (Commvault)
[4] O teste de penetração (do inglês "*Penetration Test*" ou pentest"). O teste de penetração (ou pen test) é um exercício de segurança em que um especialista em segurança cibernética tenta encontrar e explorar vulnerabilidades em um sistema de computador. O objetivo deste ataque simulado é identificar quaisquer pontos fracos nas defesas de um sistema dos quais os invasores possam se aproveitar. (CLOUDFLARE)
[5] *Phishing* é um tipo de crime cibernético em que os golpistas enviam comunicações que parecem ser de fontes confiáveis, ou seja, uma falsa comunicação online que tenta enganar os usuários da internet para fornecer suas informações pessoais ou clicar em links que baixam malwares em seus dispositivos. (MCAFEE)

- Programas de conscientização com realização campanhas regulares de conscientização e curso sobre segurança cibernética para todos os servidores, colaboradores e estagiários;

- Capacitação em segurança da informação: os servidores da STI participaram de capacitações técnicas e de gestão como: Criação e gerenciamento de equipes de resposta a incidentes de segurança da informação (Cert.br) e capacitação para o gestor de segurança;

- Participação da ANA no Programa de Privacidade e Segurança da Informação (PPSI) da Diretoria de Privacidade e Segurança da Informação, da Secretaria de Governo Digital (SGD) do Ministério de Gestão e Inovação em Serviços Públicos (MGI). Este programa contém um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação;

- Participação da equipe da STI no Exercício do Guardião Cibernético (EGC), maior exercício de defesa cibernética do hemisfério sul, organizado pelo Comando de Defesa Cibernética (ComDCiber) e realizado na Escola Superior de Defesa (ESD). O exercício tem por objetivo treinar os setores das infraestruturas críticas do país em problemas cibernéticos simulados.

- Participação da equipe da COSIC no exercício cibernético *Locked Shield*, maior exercício cibernético do mundo, organizado pelo Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (*NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE*).

Além dessas ações, a Agência possuía os serviços básicos necessários para sua cibersegurança, como:

- Solução de antivírus de *endpoint,* para proteger dispositivos individuais contra ameaças cibernéticas, como vírus, *worms*[6], *trojans*[7] e outros tipos de *malware*[8]*;*

- Solução de *firewall* que é um sistema de segurança para proteger redes e dispositivos, atuando como um filtro que monitora o tráfego de rede e bloqueia acessos não autorizados;

- Solução de gestão de recursos em redes corporativas (*Active Directory* - AD): é um serviço que centraliza a gestão de recursos em redes corporativas. Ele armazena informações sobre usuários, computadores, grupos e outros recursos, permitindo que administradores e usuários os localizem e utilizem eficientemente. (MICROSOFT).

- Proteção *anti-DDoS* nos links de acesso à de internet: é um conjunto de tecnologias e práticas para proteger sistemas e redes, contra ataque de negação de serviço distribuídos (DDoS). Esses ataques visam sobrecarregar servidores e redes com tráfego malicioso, tornando-os inacessíveis para usuários legítimos. (AKAMAI);

- Acesso externo por meio de *Virtual Private Network* (VPN) ou Rede Virtual Privada: é um serviço que cria uma conexão segura e privada entre o seu dispositivo e a internet, criptografando seus dados e ocultando seu endereço IP. (KASPERSKY); e,

- Ferramenta para monitoramento e auditoria de logs e comportamento de usuários;

Devido a infraestrutura implementada anteriormente ao incidente cibernético de setembro de 2023, foi possível restabelecer parcialmente e de forma progressiva os ambientes em um curto espaço de tempo, sem que novos contra-ataques fossem bem-sucedidos, apesar de haver diversas tentativas nesse sentido durante o processo, todas devidamente identificadas e bloqueadas.

É inerente ao negócio de TIC algum risco, pois nenhum ambiente pode ser considerado 100% livre de ataques, uma vez que os serviços de TIC estão cada vez mais conectados à internet e os criminosos

[6] *Worms* é um tipo de software malicioso que se replica e se propaga automaticamente por redes de computadores, explorando vulnerabilidades em sistemas operacionais e softwares. (McAfee)
[7] *Trojans* é um tipo de software malicioso que se disfarça de software legítimo para enganar os usuários e infectar seus dispositivos. (McAfee)
[8] *Malware,* é um termo genérico para qualquer tipo de software malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou redes de computadores ou dispositivos móveis. (McAfee)

estão a todo instante procurando formas, brechas e aperfeiçoando das táticas e técnicas para cometimento de crimes. Por esse motivo, a despeito de todas essas ações, atividades e ferramentas implementadas no ambiente tecnológico da ANA, não impediu que esse ambiente fosse atacado, pois conforme veremos a seguir na descrição do ataque, a segurança da informação é uma responsabilidade de todos os usuários dentro da organização e não somente da área de TIC.

3 - DETECÇÃO E RESPOSTA INICIAL

No 27 de setembro de 2023 pela manhã, a partir das 7:00 hs, a equipe técnica de operação de infraestrutura de TIC da ANA, por meio das ferramentas de monitoramento do ambiente, identificou indisponibilidades em diversos serviços e sistemas. Foi detectado comportamento inusuais na rede corporativa, caracterizado por tráfego de rede que diferia do fluxo considerado normal na infraestrutura da ANA. Desde o início do expediente às 8:00hs alguns usuários da rede, observavam dificuldades de acesso aos serviços e identificavam arquivos com a extensão *.blacksuit* em suas pastas de arquivos corporativos.

Por volta das 8:30 min, a equipe que tentava verificar o comportamento inusual e tentava reestabelecer as máquinas virtuais que estavam indisponíveis, percebeu que as senhas do usuário administrativo não autenticavam no ambiente virtualizado e acionou a equipe de segurança da informação. A equipe de segurança iniciou a análise e detectou de imediato a presença de arquivos criptografados, inclusive as máquinas virtuais. Os arquivos criptografados tinham a extensão *.blacksuit.* Rapidamente identificaram que se tratava de um grave incidente cibernético e um ataque do tipo *ransomware*[9] denominado "*BlackSuit*", que resultou na criptografia das máquinas virtuais, pastas de arquivos corporativos, além de pastas em estações de trabalho. Junto aos arquivos criptografados foi encontrado um arquivo texto que trazia a marca do grupo criminoso que realizou o ataque. Esse arquivo continha o endereço na *darkweb* para negociação do resgate dos arquivos criptografados.

Com essas evidências, foi convocada emergencialmente a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da Agência (ETIR/ANA), para definição de medidas de tratamento do incidente cibernético que estava em curso. Aproximadamente às 9:00h, todos os serviços e sistemas que funcionavam no ambiente virtualizado tornaram-se indisponíveis. Foi identificado que os criminosos ainda estavam com acesso à rede corporativa, usando credenciais válidas de usuários legítimos da rede. Os criminosos estavam conectadas à rede via VPN.

O Plano de Gerenciamento de Crise Cibernética (PGCC) foi acionado. Durante a análise dos registros de acesso à VPN, identificou-se que conexões foram iniciadas a partir do sistema operacional *Kali Linux,* que não é um sistema operacional usado por usuários da ANA. Analisando a ferramenta de *firewall*, verificou-se também um fluxo de dados e arquivos saindo pela conexão de internet, sugerindo que dados e arquivos estavam sendo exfiltrados da ANA.

As evidências foram coletadas e, em seguida, foram tomadas providências para interromper imediatamente o ataque. Então, todas as conexões por VPN e saída para internet foram interrompidas no *firewall* e com isso a atuação dos criminosos foi interrompida, uma vez que estavam conectados à rede da ANA por meio da VPN e pela internet. Após a interrupção do acesso, a equipe começou a investigar os ativos que foram acessados por IPs externos, em particular o IP 188.xxx.yyy, com localização geográfica na Letônia/UE.

Foi identificado que foram usadas para acessar a rede 4 (quatro) credenciais válidas de usuários legítimos, ou seja, 4 usuários e as respectivas senhas válidas foram usadas no ataque e consideradas comprometidas. Com a identificação de uso de credenciais interna, percebeu-se que foram usadas para explorar os sistemas internos, indicando uma estratégia de lateralização do ataque e escala de permissão.

[9] *Ransomware* é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. Na maioria dos casos, a infecção por *ransomware* ocorre da seguinte maneira. O malware primeiro ganha acesso ao dispositivo. Dependendo do tipo de *ransomware*, todo o sistema operacional ou apenas arquivos individuais são criptografados. Um resgate é, então, exigido das vítimas em questão

Por medida de segurança as credenciais de acesso ao *backup* e ao ambiente de nuvem usado pela ANA foram revogadas, bem como, as políticas de acesso, mantendo apenas uma credencial segura. Ou seja, a conexão entre o ambiente interno da ANA e o ambiente de nuvem computacional, onde parte dos sistemas da ANA estão hospedados e armazenado o *backup*, foi interrompida, garantindo que o ambiente de nuvem não seja comprometido pelo ataque cibernético.

Após o isolamento vertical com a interrupção do acesso à internet e para evitar que algum agente deixado pelos criminosos pudesse continuar agindo na rede, numa comunicação entre as máquinas, conhecido como movimento horizontal, foi realizado o desligamento dos *switches* que conectam os computadores da rede. A partir desse momento o ataque estava completamente interrompido e passou a analisar a extensão do comprometimento.

Com a interrupção total do ataque, uma Sala de Crise foi estabelecida no início da tarde do mesmo dia e os procedimentos protocolares de comunicação de incidente cibernético em órgão público foram seguidos. Além disso, iniciou-se o processo de investigação para identificar a causa raiz do incidente, coleta e análise de evidências digitais e tentativa de identificação do grupo responsável pelo ataque. Se iniciou também uma pesquisa na *darkweb* para ver o que poderia estar sendo falado sobre o ataque da ANA.

No final da manhã foi feita a primeira comunicação sobre o incidente à Diretoria Colegiada da Agência. No início da tarde foram feitos os comunicados aos órgãos da estrutura de segurança da informação: Secretaria de Governo Digital (SGD) do Ministério de Gestão e Inovação em Serviços Públicos (MGI), Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CTIR.Gov), Agência Brasileira de Inteligência (ABIN), Polícia Federal (PF), Encarregada de Dados Pessoais da ANA e Agência Nacional de Proteção de Dados Pessoais (ANPD). Ao final do dia foi feita uma descrição detalhada sobre o incidente à DIREC e feito o primeiro comunicado interno para os servidores e colaboradores e externo no portal institucional da ANA na internet.

4 - ANÁLISE DO INCIDENTE

A análise técnica do incidente indicou que o ataque sofrido pela ANA foi possível devido ao comprometimento de credenciais de usuários legítimos da rede da ANA e ao acesso à rede corporativa por meio da VPN. Dentro da rede corporativa, os criminosos usaram de técnicas elevar o nível de privilégio da credencial ou mesmo para descobrir credenciais com maiores privilégios na rede. Como tiveram sucesso em descobrir credencial com maiores permissões, conseguiram acessar a solução gerenciadora das máquinas virtuais e criptografaram todos os arquivos das máquinas virtuais o que fez com que todos os serviços e sistemas hospedados nessas máquinas virtuais ficassem indisponíveis.

A propagação do *ransomware* foi realizada por meio de movimento lateral em uma rede mal segmentada, o que permitiu o rápido comprometimento de servidores e estações de trabalho. Uma conta de serviço foi identificada como uma das contas usadas para execução do *malware*. Essa cadeia de ataque segue padrões já documentados em *frameworks* como MITRE ATT&CK (MITRE, 2023).

Como todo ataque do tipo *ransomware,* além de criptografar os arquivos, os criminosos extraem os dados e arquivos do órgão vítima do ataque para tentar extorquir recursos financeiros nas 2 vertentes: uma por meio da “venda” da senha para descriptografar os arquivos e outra com a ameaça de divulgação dos dados explotados.

Podemos identificar algumas vulnerabilidades exploradas nesse ataque cibernético. A primeira, que foi verificada o uso de credenciais legitimas de usuários da ANA com senhas comprometidas. Essa prática é uma das mais recorrentes em ataques cibernéticos, pois permite que os invasores evitem a detecção imediata, atuando como se fossem usuários internos. Não se tem nenhuma informação, nem mesmo suspeita, de como os atacantes descobriram as credenciais válidas de usuários da ANA. Existem diversas formas conhecidas para obter credenciais válidas ou disponibilizadas na internet, para pessoas e grupos mal-intencionados. Existem diversas técnicas utilizadas para obtenção dessas credenciais (NIST, 2012)

como: p*hishing, malware, engenharia social*, ataque de força bruta e ataques de dicionário, exploração de serviços expostos e captura de credenciais na memória com uso de ferramentas como *Mimikatz* que permitem a extração de senhas armazenadas temporariamente na memória RAM de sistemas Windows. Portanto, existem inúmeras técnicas para se obter credenciais legitimas de redes corporativas e com as evidências que foram coletadas no ataque não permite identificar como o atacante teve acesso a essas credenciais.

Outra vulnerabilidade explorada nesse ataque foi a falta do múltiplo fator de autenticação no acesso por meio da VPN (MFA do inglês *Multiple Factor Authentication*). O MFA ou Autenticação Multi-Fator, é um método de segurança que exige que os usuários forneçam dois ou mais fatores de autenticação para acessar um sistema ou conta e não somente uma senha. Esses fatores podem ser algo que o usuário sabe (como uma senha, PINs, perguntas secretas), algo que ele possui (como um token físico, código enviado por SMS ou aplicativo autenticadores de *smartphone*, como o *Google Authenticator* por exemplo, chaves de segurança) ou algo que ele é (como uma impressão digital, reconhecimento facial, outros dados biométricos). A MFA adiciona uma camada extra de segurança, tornando mais difícil para pessoas não autorizadas acessarem informações confidenciais, mesmo que uma senha seja comprometida. Na ocasião do ataque o acesso VPN da ANA não estava com o MFA ativado, ou seja, os usuários acessavam a VPN somente com uma senha.

As vulnerabilidades descritas acima são as principais que foram exploradas pelos atacantes nesse incidente. Podemos ainda citar num segundo nível de vulnerabilidades, o baixo controle de credenciais de serviço, a falta de segmentação da rede interna, assim com a falta de ferramentas de monitoramento de comportamento dos usuários da rede.

5 - IMPACTOS DO INCIDENTE

O ataque cibernético na ANA causou impactos em pelo menos 4 dimensões:

- Impacto operacional: interrupção de serviços e sistemas computacionais, tanto internos quanto externos, sistemas de uso externo ficaram fora do ar, muito tempo de inatividade na rede corporativa e falta de acesso aos arquivos criptografados;

- Impacto reputacional: perda de confiança dos usuários quando à indisponibilidade dos sistemas e dados da ANA;

- Impacto financeiro: necessidade de aumento nos investimentos em segurança, contratações, etc;

- Impacto legal**:** conformidade com normativos da ANA, vários prazos estabelecidos nos regulamentos da ANA tiveram que ser estendidos, além da possibilidade de vazamento de dados pessoais armazenados na ANA, em confronto com a Lei Geral de Proteção de Dados Pessoais (LGPD).

O ataque cibernético comprometeu mais de 100 estações de trabalho, HDs externos e diversos serviços e sistemas internos e externos. Todos os serviços da ANA foram temporariamente desativados, resultando em significativa perda de produtividade. Embora não tenha sido identificada exfiltração de dados sensíveis, o impacto reputacional e operacional foi significativo, exigindo atuação conjunta das áreas de segurança, tecnologia e comunicação da Agência. Diversos meios de comunicação, como jornais e revistas noticiaram o ataque e informaram da paralização dos sistemas da Agência.

6 - ESTRATÉGIA DE RECUPERAÇÃO DO AMBIENTE TECNOLÓGICO

Segundo o estudo *EY 2023 Global Cybersecurity Leadership Insights* (ERNST & YOUNG, 2023), o tempo médio de resposta e recuperação a um incidente cibernético pode chegar a 11 (onze) meses para empresas com baixo desempenho em cibersegurança. Já aquelas mais eficazes, que possuem programas de prevenção bem instituídos e maduros, conseguem reduzir esse tempo pela metade, chegando a cerca de 5 (cinco) meses em média. A maioria das organizações que sofreram com ataques cibernéticos, aproximadamente 76%, precisaram de seis meses ou mais para responder a um incidente.

Próximo a completar 3 (três) meses do ataque cibernético sofrido pela ANA, em dezembro de 2023, cerca de 85% dos serviços e sistemas da Agência foram reestabelecidos, e os demais 15% foram restabelecidos até os 5 (seis) meses, identificados como referência de tempo médio de restabelecimento pós-incidente, para empresas com alta performance em cibersegurança.

Antes de iniciar os procedimentos de recuperação do ambiente, foram realizadas reuniões com outros órgãos da administração pública que passaram por incidentes semelhantes. Essas reuniões tinham o objetivo de compartilhar a experiências desses órgãos em situações semelhantes com vistas a estabelecer um conjunto de boas práticas que pudessem ser adotadas pela ANA no reestabelecimento do ambiente. Além das boas práticas foram identificadas as ferramentas de segurança da informação que foram adotadas com sucesso nessas instituições. Além dos órgãos da administração pública, foram consultadas empresas especializadas em segurança da informação para verificar como poderiam apoiar a Agência nesse momento, seja com conhecimentos ou disponibilizando temporariamente ferramentas.

Foi definida uma estratégia de restabelecimento seguro da infraestrutura de rede e das aplicações, cujas definições de prioridades foram alinhadas e acordadas com a Diretoria Colegiada da Agência. A STI dispôs as equipes para atuações em frentes de trabalho, em especial: infraestrutura de rede, estações trabalho, bancos de dados, aplicações estruturantes, aplicações prioritárias e demais aplicações.

Foram fatores críticos de sucesso para o rápido restabelecimento a infraestrutura de TIC: - acionamento rápido das instâncias especializadas e regulamentares, bem como a identificação de boas práticas com órgãos da Administração Pública Federal que sofreram ataques semelhantes; - apoio da alta administração da Agência na garantia de recursos financeiros e apoio na realização de ações que possibilitassem um ambiente seguro, mesmo que em detrimento de um retorno mais rápido; - equipe técnica com dedicação integral à resolução da crise; - processo de comunicação contínua, objetiva e tempestiva aos públicos interno e externo à Agência; - aplicação de procedimentos contingenciais pré-definidos e organizados, facilitando a atuação das diversas equipes acionadas.

Com essa recuperação, a ANA mantém-se no mesmo patamar de tempo de resposta pós-incidente reconhecido internacionalmente para instituições de alta performance em cibersegurança.

7 - AÇÕES CORRETIVAS E PREVENTIVAS

Na etapa de recuperação do ambiente, foram adotadas diversas medidas estruturais para tornar o ambiente de TIC da ANA mais seguro e visando prevenir futuros incidentes do mesmo tipo. A STI realizou reuniões com diversos órgão públicos e o Serviço de Processamento de Dados do Governo Federal (SERPRO), além das empresas especializadas em segurança da informação e comunicações, para identificar as melhores práticas no ambiente renovado. Também houve encontros para definir quais ferramentas de segurança seriam incorporadas à infraestrutura nesse novo cenário. As boas práticas identificadas foram: - reconfiguração da rede com segmentação lógica; - possuir antivírus de *endpoint* gerenciável com licença válida; - segregar a rede de usuários da rede de servidores por meio de um *firewall*; - adotar a diretiva de negar todo o acesso e dar permissão apenas ao que seja expressamente necessário a realização das atividades; - aplicar política de senhas complexas com alteração periódica da senha; - redefinição de perfis de usuários com base no princípio do menor privilégio; - sanitização periódica mensal de contas dos usuários e revisão de credenciais administrativas de rede; - ativar o múltiplo fator de autenticação (MFA) para acesso por meio da VPN; - reintegração gradual das estações de trabalho dos usuários, após rigorosa verificação e formatação completa; - reestabelecimento de serviços a partir de *backups* seguros e implementar ferramentas de monitoramento do comportamento de usuários, auxiliar na compreensão e construção de um padrão de tráfego de rede.

Após definidas as prioridades, iniciou-se o processo de restauração do *backup* de máquinas e arquivos, sendo meticulosamente verificada a integridade de cada conjunto de dados. Juntamente com a recuperação dos sistemas, as estações de trabalho passaram por um rigoroso processo de sanitização e formatação, a fim de garantir que nenhum resquício malicioso permanecesse na rede. Esse processo colaborativo e organizado contribuiu para a recuperação eficaz da infraestrutura da ANA, e, embora o

trabalho de restabelecimento fosse demorado no início, avanços significativos foram alcançados na direção de retomar a total normalidade das atividades da Agência.

Concluindo, a infraestrutura de TIC da ANA foi restaurada com foco na mitigação de riscos de segurança. Essas práticas seguem diretrizes do NIST SP 800-61 e ISO/IEC 27001 para resposta a incidentes (NIST, 2012; ISO, 2022).

8 - COMUNICAÇÃO E GOVERNANÇA

Durante o gerenciamento do incidente, equipe da STI, juntamente com a equipe da Assessoria de Comunicação (ASCOM) realizou comunicados diários aos servidores e colaboradores internos. Além disso, a ANA publicou informações em seu portal institucional na internet onde manteve os usuários externos informados da situação dos sistemas. Cada sistema que era restabelecido, a página que continha informações do incidente era atualizada. A comunicação foi orientada com foco em transparência, controle de danos e prevenção de desinformação. A mobilização de múltiplas partes interessadas demonstrou a importância da governança integrada em contextos de crise.

A Diretoria Colegiada recebia informações diárias sobre o andamento das ações de restabelecimento, bem com definia a priorização dos serviços e sistemas que deveriam ser restabelecidos. Além disso, mantinha comunicação com outras autoridades do Governo Federal informando o andamento das ações de restabelecimento.

Para facilitar a comunicação e a tornar mais rápido a tomada de decisão, uma Sala de Crise foi estabelecida e um grupo de WhatsApp específico foi criado. Participavam da Sala de Crise e do grupo os gestores da STI, diretores, chefes das unidades e superintendentes. Todas as informações relevantes eram compartilhadas nesses espaços, o que tornava a tomada de decisão mais tempestiva.

9 - LIÇÕES APRENDIDAS

O incidente evidenciou a necessidade de aprimorar continuamente os controles de segurança da informação, revisar políticas internas, qualificar usuários e manter um ambiente tecnológico resiliente. Entre as lições aprendidas destacam-se: o papel central da autenticação multifator (MFA), a importância de *backups* segregados da infraestrutura interna, a necessidade de treinamentos periódicos em segurança da informação e a atuação conjunta entre áreas técnicas, jurídicas e administrativas.

Após o incidente foi possível identificar algumas oportunidades de melhorias no tema segurança da informação na ANA, tais como: melhoria da infraestrutura física de TIC com aquisição de novos equipamentos, necessária devido à termino da garantia de equipamentos, acesso remoto seguro, fundamental para o desenvolvimento pleno da atividades de TI, destinação insuficiente de recursos financeiros previstos para o orçamento da área de TI podendo inviabilizar contratações de serviços e aquisição de equipamentos essenciais para a evolução na segurança do parque tecnológico da Agência, implementação de novas tecnologias e práticas, melhoria na comunicação e coordenação das atividades de segurança, necessidade de treinamento e conscientização dos servidores e colaboradores no tema segurança da informação, atualização das políticas de segurança da informação, realização de simulação e testes de intrusão, simulações de *phishing* e outros ataques e por fim promover a criação de uma cultura de segurança da informação na organização.

10 - CONSIDERAÇÕES FINAIS

Apesar da gravidade do incidente, a resposta ágil e coordenada permitiu à ANA recuperar seus serviços com segurança. O caso reforça a importância da preparação institucional e serve como referência para outras entidades públicas e órgãos gestores de recursos hídricos, que buscam fortalecer sua resiliência cibernética frente a ameaças digitais cada vez mais sofisticadas. O evento cibernético trouxe reflexões sobre oportunidades de melhorias nos processos, ferramentas e cultura da Agência, reafirmação da importância da segurança cibernética, da conscientização dos usuários da rede e importância de investimentos em segurança da informação.

REFERÊNCIAS

AGÊNCIA NACIONAL DE ÁGUAS. *Plano Estratégico 2023-2026.* Agência Nacional de Águas. Brasília: ANA, 2023. Disponível em < https://www.gov.br/ana/pt-br/acesso-a-informacao/acoes-e-programas/planejamentoestrategico/pei-2023-2026.pdf>. Acesso em 13/06/2025.

AGÊNCIA NACIONAL DE ÁGUAS. *Plano Estratégico de Tecnologia da Informação 2023-2026*. Agência Nacional de Águas. Brasília: ANA, 2024. Disponível em <https://www.gov.br/ana/pt-br/acesso-a-informacao/tecnologia-da-informacao/petic-2023-2026.pdf>. Acesso em 13/06/2025.

AKAMAI. O que é um ataque de DDoS? Página: O que é um ataque de DDoS? Disponível em: <https://www.akamai.com/pt/glossary/what-is-ddos>. Acesso em: 19 de jun. de 2025.

CIS. Center for Internet Security. Página Principal. Disponível em: <https://www.cisecurity.org/>. Acesso em: 19 de jun. de 2025.

CLOUDFLARE. O que é teste de penetração? Página: O que é teste de penetração? Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-penetration-testing/>. Acesso em: 19 de jun. de 2025.

COMMVAULT. Commvault: Recursos. Página: Recursos. Disponível em: <https://www.commvault.com/resources>. Acesso em: 19 de jun. de 2025.

ERNST & YOUNG. EY 2023 Global Cybersecurity Leadership Insights. EY 2023 Global Cybersecurity Leadership Insights, 2023. Disponível em: < https://www.ey.com/en_gl/insights/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy>. Acesso em: 19 de jun. de 2025.

ISO. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Information security management systems.

ISO. ISO 22361:2022 - Security and resilience. Crisis management. Guidelines.

KASPERSKY. O que é uma VPN? Como funciona, tipos e benefícios. Página: O que é uma VPN? Como funciona, tipos e benefícios. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn>. Acesso em: 19 de jun. de 2025.

MCAFEE. McAfee: *O que é malware?* Página Recursos. Disponível em: <https://www.mcafee.com/pt-br/antivirus/malware.html>. Acesso em: 19 de jun. de 2025.

MICROSOFT. Visão geral do Active Directory Domain Services. Página: Visão geral do Active Directory Domain Services. Disponível em: <https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. Acesso em: 19 de jun. de 2025.

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS. *Guia do Framework de Privacidade e Segurança da Informação*. Ministério da Gestão e Inovação em Serviços Públicos: MGI, 2024. Disponível em < https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf >. Acesso em 13/06/2025.

MITRE. MITRE ATT&CK Framework. MITRE ATT&CK Framework, 2023. Disponível em: < https://attack.mitre.org>. Acesso em: 19 de jun. de 2025.

NIST. Computer Security Incident Handling Guide. Special Publication 800-61 Revision 2. National Institute of Standards and Technology, 2012. Disponível em: < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Acesso em: 19 de jun. de 2025.

TRIBUNAL DE CONTAS DA UNIÃO. *Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética 2020-2023*. Tribunal de Contas da União. Brasília: TCU, 2021. Disponível em < https://portal.tcu.gov.br/publicacoes-institucionais/sumarios-executivos/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023>. Acesso em 13/06/2025.