5° Webinário de segurança da informação

Relatório geral do evento

ABIN TCU GABINETE DE SEGURANÇA INSTITUCIONAL GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO

Contextualização do 5º Webinário de Segurança da Informação

O 5º Webinário de Segurança da Informação foi realizado com o objetivo de promover reflexões qualificadas sobre o tema "Segurança da Informação: cenário atual e perspectivas para o setor público", em um momento particularmente relevante para a Administração Pública Federal. O evento ocorre em um contexto recente de publicação de documentos nacionais estruturantes, fundamentais para o fortalecimento da segurança da informação e da segurança cibernética no país.

O evento contou com a participação de:

Secretário de Segurança da Informação e Cibernética
André Luiz Bandeira Molina

Diretora do Departamento de Segurança da Informação
Danielle Jacon Ayres Pinto

Diretor do Departamento de Segurança Cibernética
Luiz Fernando Moraes da Silva

Coordenador-Geral do Núcleo de Segurança e Credenciamento
Guilherme Portella

Auditor Federal de Controle Externo do Tribunal de Contas da União
André Torres Breves Gonçalves

Diretor do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
Vanderson Rocha

Sumário

Publicação de Marcos Normativos Estruturantes

Em agosto, foram publicados dois instrumentos normativos de grande relevância: a Política Nacional de Segurança da Informação e a Estratégia Nacional de Cibersegurança. Tais documentos são considerados estruturantes por estabelecerem diretrizes estratégicas e orientações claras quanto ao direcionamento dos esforços institucionais no campo da segurança da informação e da cibersegurança.

A Estratégia Nacional de Cibersegurança foi formalizada por meio de decreto e constitui o resultado dos trabalhos desenvolvidos por um grupo de trabalho no âmbito do Comitê Nacional de Cibersegurança. Seu conteúdo fornece balizamentos estratégicos que orientam ações, prioridades e investimentos voltados ao fortalecimento da cibersegurança em nível nacional.

A Política Nacional de Segurança da Informação, por sua vez, aborda de forma específica os aspectos de governança e segurança da informação no âmbito da Administração Pública Federal. Atualmente em sua terceira versão, o documento apresenta uma evolução histórica significativa: a primeira edição foi elaborada no ano 2000, seguida por uma segunda versão publicada em 2018. A versão mais recente foi concebida com o propósito de evidenciar a necessidade de uma governança robusta em segurança da informação, com ênfase na gestão de riscos e na definição clara de papéis e responsabilidades dos atores envolvidos.

A política reafirma a importância da existência de um órgão central responsável pela formulação de diretrizes e políticas de segurança da informação, atribuição exercida pelo Gabinete de Segurança Institucional da Presidência da República (GSI). Além disso, observa-se a atuação colaborativa de outros órgãos com funções relevantes nesse ecossistema, como o sistema de controle interno do Poder Executivo Federal e o próprio Comitê Nacional de Cibersegurança, instituído a partir da Política Nacional de Cibersegurança.

Publicada em dezembro de 2023, a Política Nacional de Cibersegurança tem como finalidade propor, por meio do Comitê Nacional de Cibersegurança, medidas voltadas ao aprimoramento da segurança cibernética nacional. Um dos produtos decorrentes desse processo foi a elaboração e posterior publicação da nova Estratégia Nacional de Cibersegurança, em agosto, também na forma de decreto.

Abrangência da Segurança da Informação e Ênfase em Pessoas

No âmbito da Política Nacional de Segurança da Informação, são estabelecidas orientações sobre como a Administração Pública Federal, em especial o Poder Executivo Federal, deve atuar no campo da segurança da informação. Um dos pontos centrais destacados pelo normativo é a compreensão de que a segurança da informação não se limita à dimensão digital, apresentando um escopo significativamente mais amplo.

Nesse sentido, tem-se atribuído especial atenção à capacitação de pessoas, à gestão de servidores e colaboradores, bem como à realização de verificações de antecedentes. Observa-se que diversos incidentes cibernéticos possuem causas internas, associados a agentes internos, comumente denominados insiders. Diante desse cenário, a política busca contemplar aspectos que extrapolam a segurança cibernética estritamente técnica, incorporando elementos organizacionais, humanos e procedimentais.

A política estabelece, assim, uma governança sólida e reforça princípios orientados à gestão de riscos, evidenciando que a segurança da informação deve ser tratada de forma integrada, abrangente e colaborativa.

Objetivos do Webinário e Perspectivas de Aplicação

O propósito central do webinário consiste em fomentar o debate qualificado sobre o cenário atual da segurança da informação e as perspectivas futuras decorrentes da implementação dos novos instrumentos normativos. Considerando o caráter estruturante desses documentos, torna-se fundamental compreendê-los adequadamente e explorar suas possibilidades de aplicação prática.

Ressalta-se, ainda, que os direcionamentos estabelecidos pela Política Nacional de Segurança da Informação e pela Estratégia Nacional de Cibersegurança podem ser aproveitados não apenas por órgãos públicos submetidos aos regramentos federais, mas também por instituições que, embora não obrigadas formalmente a observá-los, podem utilizá-los como referência para o aprimoramento de suas práticas de segurança da informação e cibersegurança.

Outro objetivo importante a ser alcançado no webinário foi edificar a ideia de que o engajamento da alta gestão constitui elemento essencial para a concretização de iniciativas voltadas ao fortalecimento da segurança da informação no âmbito da Administração Pública Federal.

Questão Norteadora do Webinário

No início do evento, foi apresentada a questão orientadora do webinário, com o objetivo de subsidiar as intervenções dos participantes a partir das perspectivas institucionais de seus respectivos órgãos. A indagação central proposta foi:

De que forma as instituições representadas contribuem para o alcance dos objetivos da Política Nacional de Segurança da Informação e como essas contribuições podem apoiar os órgãos da Administração Pública Federal?

A partir dessa questão, foi definida a ordem das manifestações, iniciando-se pelo representante do Tribunal de Contas da União, seguido pelos representantes da Agência Brasileira de Inteligência, do Gabinete de Segurança Institucional e, por fim, do GSI, de modo a estruturar o debate e garantir a participação equilibrada dos diferentes atores institucionais.

Observou-se a relevância da terceira geração da Política Nacional de Segurança da Informação (PNSI), seu vínculo com a Política Nacional de Cibersegurança, a Estratégia Nacional de Cibersegurança e as futuras ações previstas no âmbito da Secretaria de Segurança da Informação e Comunicação (SSIC), com o objetivo de fortalecer o ecossistema de proteção no Poder Executivo Federal. Ao reconhecer a contribuição dos representantes da ABIN, TCU, GSI e outros órgãos presentes, enfatizou a importância do debate para o aprimoramento da segurança cibernética nacional.

Contribuições do TCU para a PNSI

No que se refere à contribuição do TCU para os objetivos da Política Nacional de Segurança da Informação (PNSI), observou a atuação fiscalizatória e indutora do Tribunal. Embora o TCU possua uma área de TI com desafios comuns a outros órgãos, a contribuição do Tribunal se dá, principalmente, na auditoria e no controle externo. A função indutora do TCU envolve a promoção da melhoria na segurança da informação nos órgãos auditados, além da fiscalização rigorosa das práticas de governança e segurança implementadas por outros setores da Administração Pública Federal.

O TCU também tem um papel relevante na interação com os Órgãos Governantes Superiores (OGS), como o Gabinete de Segurança Institucional (GSI), que orienta e normatiza as práticas de segurança nos órgãos subordinados ao Executivo Federal. A cooperação com o GSI e a Secretaria de Gestão de Dados (SGD) é considerada

altamente produtiva, especialmente no que se refere à formulação de diretrizes que orientam a segurança da informação em nível federal.

Foram ressaltadas, ainda, duas auditorias relevantes conduzidas pelo TCU. A primeira, realizada em 2024, abordou a Política Nacional de Cibersegurança (PNCiber) e resultou no Acórdão 2430/2024, no qual foi observada a insuficiente priorização da segurança cibernética no Brasil. Uma das principais conclusões foi a limitação do alcance da PNCiber, que, sendo elaborada pelo Executivo, se aplica apenas aos órgãos deste poder, sem a abrangência necessária para toda a Administração Pública. O TCU recomendou, portanto, que a implementação dessas diretrizes se estenda para além do Executivo, alcançando toda a Administração Pública. A revisão da versão anterior da PNSI, de 2018, também trouxe à tona essas limitações, reforçando a necessidade de expandir as obrigações de segurança da informação a todos os níveis de governança pública.

Atuação do TCU na Avaliação de Controles e Governança de Segurança da Informação

Foi registrado que os acórdãos e trabalhos mencionados encontram-se disponíveis para consulta pública no portal institucional do Tribunal de Contas da União, especificamente na área da Diretoria de Avaliação da Segurança da Informação (DASI), em https://www.tcu.gov.br/dasi, o que reforça o compromisso com a transparência e a disseminação do conhecimento técnico produzido.

Ainda no ano de 2024, foi conduzido novo trabalho de auditoria que resultou no Acórdão nº 2387/2024, no qual foram avaliados os controles de segurança do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), com base na versão anterior da Política de Segurança da Informação (PPSI). Entre os achados iniciais, constatou-se a inexistência de previsão normativa clara quanto à responsabilidade da alta administração na gestão dos riscos de segurança da informação.

Observou-se que, em diversos órgãos, persiste o entendimento equivocado de que os riscos de segurança da informação são de responsabilidade exclusiva das áreas de tecnologia da informação. Tal percepção contrasta com a abordagem preconizada pelas boas práticas de governança, segundo as quais os riscos de segurança da informação devem ser tratados como riscos estratégicos da organização, inserindo-se, portanto, no âmbito de responsabilidade da alta gestão. Nesse sentido, buscou-se induzir uma mudança de entendimento institucional, enfatizando que risco de segurança constitui risco de negócio.

Essa mudança de perspectiva é considerada essencial para o fortalecimento das equipes operacionais, uma vez que o reconhecimento da responsabilidade pela alta administração tende a resultar em maior direcionamento de recursos financeiros, alocação adequada de pessoal e priorização orçamentária. No curso das auditorias, também foi identificada, em diversos órgãos, a ausência quase total de estrutura de tecnologia da informação. Em alguns casos, verificou-se a existência de equipes extremamente reduzidas, compostas por um ou dois profissionais; em outros, constatou-se a inexistência formal de equipe, sendo a função exercida de maneira informal por indivíduos sem estrutura adequada, situação particularmente crítica no contexto da segurança da informação.

Principais Dificuldades Identificadas nos Órgãos Auditados

No âmbito dos trabalhos realizados, os gestores relataram um conjunto recorrente de dificuldades, sistematizadas em cinco pontos principais:

1. elevada rotatividade de profissionais de tecnologia da informação;

2. escassez de profissionais qualificados, com migração frequente para oportunidades no exterior;

3. insuficiência de recursos financeiros;

4. complexidade crescente dos temas tecnológicos, incluindo computação em nuvem, virtualização, Internet das Coisas (IoT) e, de forma emergente, desafios associados à inteligência artificial;

5. elevado volume de demandas internas.

Com base nesses achados, foram emitidas recomendações específicas para cada órgão integrante do SISP, com vistas à implementação dos controles previstos na PPSI. Verificou-se que muitos órgãos sequer haviam implementado os controles correspondentes ao nível 1 da política — considerando-se a existência de níveis 1, 2 e 3 , sendo ainda mais restrito o número de instituições que alcançaram níveis mais avançados de maturidade.

Avanços Normativos e Alinhamento com Boas Práticas

Foi informado que a nova versão da Política de Segurança da Informação do Ministério da Gestão e da Inovação em Serviços Públicos, publicada pela Portaria MGI Nº 10.033, de 29 de dezembro de 2025 (https://www.in.gov.br/en/web/dou/-/portaria-mgi-n-10.033-de-29-de-dezembro-de-2025-678372512), incorporou avanço relevante ao estabelecer, em seu artigo 8º, a responsabilidade explícita da alta administração pela gestão dos riscos de segurança da informação. Tal direcionamento foi apontado como resultado de esforços conjuntos, incluindo contribuições oriundas das auditorias e recomendações emitidas pelo Tribunal de Contas da União.

No exercício de sua missão institucional, o TCU realiza a verificação do cumprimento das normas aplicáveis, avaliando a aderência dos órgãos auditados não apenas aos dispositivos normativos vigentes, mas também a boas práticas amplamente reconhecidas, tais como os CIS Controls e outros frameworks de referência. Ainda que tais modelos não possuam caráter vinculante, são considerados parâmetros técnicos mínimos para a avaliação da maturidade em segurança da informação.

Programa Protege TI e Fortalecimento da Cultura de Segurança

Nos últimos três anos, foi desenvolvido o programa Protege TI, por meio do qual o Tribunal de Contas da União realizou diversas auditorias técnicas e promoveu ações de disseminação de conhecimento, incluindo transmissões ao vivo em plataforma digital, com o objetivo de apresentar boas práticas, referências técnicas e materiais de apoio. Entre os produtos desse programa, apresentam-se manuais técnicos elaborados a partir das auditorias realizadas, disponibilizados ao público por meio do canal institucional do TCU.

Por fim, reafirmou-se o compromisso do Tribunal de Contas da União com o fortalecimento da cultura de segurança da informação, a sensibilização da alta administração e a contribuição contínua para a melhoria da postura de segurança no Brasil.

Convergência entre Fiscalização, Indução e Cooperação Institucional

Foi destacada a relevância da atuação do Tribunal de Contas da União não apenas sob a perspectiva fiscalizatória, reconhecida como elemento central de qualquer processo institucional no setor público, mas, sobretudo, em sua função indutora de boas práticas e de políticas públicas. Ressaltou-se que, além da fiscalização, torna-se fundamental apoiar os órgãos da Administração Pública Federal no processo de elevação de sua maturidade em segurança da informação, o que demanda uma atuação baseada na cooperação institucional.

Nesse contexto, foi enfatizada a importância dos elementos apresentados acerca da relação entre o TCU e as

perspectivas da Política Nacional de Segurança da Informação, reconhecendo-se o valor dessas contribuições para o fortalecimento do ecossistema de governança e segurança da informação.

Atuação do Cepesc/ABIN no Âmbito da Política Nacional de Segurança da Informação

O Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc), unidade vinculada à Agência Brasileira de Inteligência, foi apresentado como um departamento que atua de forma integrada à área de tecnologia da informação da ABIN. Sua atuação institucional foi sintetizada em três frentes principais.

A primeira frente consiste na gestão da tecnologia da informação do próprio órgão, enfrentando desafios semelhantes aos vivenciados por outras instituições públicas. A segunda refere-se à produção de inteligência, atividade inerente à natureza institucional da Agência Brasileira de Inteligência. A terceira frente, considerada central e histórica para o Cepesc, corresponde à pesquisa e ao desenvolvimento de soluções voltadas à segurança das comunicações.

Essa vertente de pesquisa e desenvolvimento acompanha a trajetória do Cepesc desde sua criação, anterior inclusive à fundação da própria ABIN, e constitui o principal eixo de contribuição do órgão no contexto da Política Nacional de Segurança da Informação. Ao longo de aproximadamente quatro décadas de atuação, o Cepesc desenvolveu soluções voltadas tanto para comunicações fixas quanto móveis, acumulando expertise técnica relevante na área.

Atualmente, encontram-se em desenvolvimento dois projetos de grande porte, com previsão de divulgação futura, ambos concentrados no campo da pesquisa e do desenvolvimento de soluções tecnológicas para a segurança das comunicações.

O principal domínio de pesquisa do Cepesc é a criptografia, área diretamente alinhada aos princípios da Política Nacional de Segurança da Informação, especialmente no que se refere à proteção de dados, à garantia da privacidade e ao controle de acesso à informação. A atuação do centro concentra-se, portanto, no desenvolvimento e na aplicação de soluções criptográficas avançadas.

Observou-se, ainda, a existência de parcerias institucionais relevantes, com ênfase na cooperação com o Tribunal Superior Eleitoral. Nesse contexto, o Cepesc presta apoio à segurança das urnas eletrônicas, tendo desenvolvido e fornecido uma biblioteca criptográfica preparada para o uso de criptografia pós-quântica. Essa iniciativa foi apontada como uma das mais significativas aplicações de criptografia pós-quântica em ambiente produtivo em nível mundial, ao ser empregada no sistema eleitoral brasileiro.

Integração Institucional e Produção de Conhecimento Estratégico

Foi ressaltada a proximidade institucional entre os órgãos participantes do webinário e a relevância do trabalho conjunto para a consolidação da segurança da informação. Concluiu-se que a atuação em parceria é especialmente crítica nos domínios da pesquisa e da produção de inteligência, uma vez que esses elementos subsidiam a construção de cenários estratégicos, a identificação de demandas prioritárias e o reconhecimento de nichos de atuação necessários ao aprimoramento da segurança da informação.

Enfatizou-se que iniciativas como o webinário contribuem para a consolidação de convergências institucionais e para o reconhecimento de que a atuação isolada é insuficiente diante da complexidade do tema, sendo imprescindível uma abordagem integrada e colaborativa.

Contribuições do Departamento de Segurança Cibernética do GSI

A relação entre os departamentos e as respectivas áreas de atuação foi caracterizada como intrinsecamente interdependente, considerando-se que a segurança da informação, em seu sentido mais amplo, abrange pessoas, processos, instalações físicas e a própria informação em meio digital, enquanto a segurança cibernética constitui um dos principais elementos viabilizadores dessa proteção.

As contribuições institucionais do Departamento de Segurança Cibernética do GSI foram organizadas em quatro eixos principais.

O primeiro eixo refere-se à dimensão tecnológica, compreendendo a segurança cibernética em sua totalidade, incluindo aspectos como criptografia e outros mecanismos técnicos de proteção. O fortalecimento da segurança cibernética foi apontado como fator que, por consequência direta, contribui para o aprimoramento da segurança da informação de forma ampla.

O segundo eixo diz respeito à articulação institucional. Considerando as dimensões territoriais do país e a multiplicidade de órgãos que atuam nos campos da segurança da informação e da segurança cibernética, identificou-se a necessidade de uma governança mais robusta e de maior coordenação desse problema público. Ressaltou-se que tal coordenação somente pode ser efetivamente viabilizada por meio de articulação institucional, papel para o qual o GSI, em razão de sua vinculação à Presidência da República, ocupa posição estratégica. Nesse sentido, observaram-se esforços contínuos de participação em eventos, grupos de trabalho governamentais e processos de formulação de políticas públicas, inclusive nas áreas de serviços digitais e economia digital.

O terceiro eixo corresponde à presença institucional. A participação em webinários, eventos técnicos, articulações internacionais e encontros profissionais foi apresentada como fundamental não apenas para facilitar a coordenação entre atores, mas também para conferir visibilidade às atividades desenvolvidas pelo GSI. Observou-se que parte significativa da atuação do órgão possui natureza normativa e, frequentemente, carece de adequada explicação pública, o que pode gerar interpretações imprecisas, inclusive em veículos de comunicação e análises especializadas. Dessa forma, ressaltou-se a importância da atuação do GSI em iniciativas de conscientização e esclarecimento.

O quarto eixo refere-se à atuação operacional do CTIR.Gov, bem como às parcerias nacionais e internacionais mantidas pelo órgão. No âmbito da Diretoria de Segurança Cibernética, o CTIR.Gov foi caracterizado como unidade operacional e de coordenação responsável por prover consciência situacional cibernética à Presidência da República e aos integrantes da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). Essa atuação envolve órgãos setoriais, agências reguladoras e demais participantes, todos integrados com o objetivo de compartilhar informações e agilizar a troca de dados em prol da segurança cibernética e, por extensão, da segurança da informação.

Por fim, foram destacadas as parcerias nacionais e internacionais como elemento relevante da atuação institucional. Foram mencionadas interações recentes com gestores públicos e representantes de outros países, em diálogos realizados no âmbito do Ministério das Relações Exteriores, incluindo encontros com delegações da Índia e da Eslováquia. Essas experiências foram apontadas como oportunidades de aprendizado, permitindo a compreensão de diferentes modelos de organização e abordagens adotadas por outros países no tratamento da segurança da informação.

Em síntese, as contribuições do Departamento de Segurança Cibernética do GSI foram consolidadas em quatro dimensões principais: a atuação técnica

em segurança cibernética; a articulação institucional; a presença ativa em espaços de debate e conscientização; e a atuação operacional do CTIR.Gov, sustentada por parcerias nacionais e internacionais.

Sinergia entre Segurança da Informação e Segurança Cibernética

Foi ressaltada a importância de evidenciar a forte sinergia existente entre as duas dimensões centrais de atuação da Secretaria: a segurança da informação e a segurança cibernética. Observou-se que, embora essas dimensões frequentemente operem de forma integrada no âmbito interno, é fundamental explicitar sua complementaridade e interdependência, especialmente no contexto da formulação e implementação de políticas públicas.

Salientou-se que o exemplo produzido no âmbito da Administração Pública Federal possui potencial de repercussão para além do Gabinete de Segurança Institucional, alcançando outros setores e instituições. Tal efeito multiplicador está diretamente relacionado aos documentos e diretrizes elaborados no âmbito do Departamento de Segurança Cibernética, cuja atuação contribui para consolidar padrões de proteção, ações de conscientização e iniciativas de capacitação.

Foi enfatizado que essas dimensões não se restringem aos impactos diretos junto à sociedade, mas também alcançam órgãos que não integram formalmente a Administração Pública Federal, os quais podem adotar as práticas nacionais como referência. Ademais, ressaltou-se a relevância dessas iniciativas no plano internacional, ao permitir que outros países conheçam as práticas brasileiras, aprendam com elas e, reciprocamente, contribuam com experiências e modelos distintos, especialmente no contexto de acordos e cooperação internacional.

Concluiu-se que tais elementos de sinergia são estruturantes e não devem ser negligenciados, sendo essencial a disseminação contínua dessas práticas no cotidiano institucional, como forma de fortalecer de maneira integrada a segurança da informação e a segurança cibernética.

Proteção de Informações Classificadas e Segurança dos Segredos de Estado

Foi observado que, embora esse campo represente um volume reduzido do conjunto informacional produzido pela Administração Pública, sua relevância é estratégica para a proteção dos interesses do Estado.

Ressaltou-se que essa área ainda é pouco conhecida por parte da Administração Pública Federal e por gestores de segurança da informação, o que reforça a importância de torná-la progressivamente mais compreensível, acessível e adequadamente protegida, como parte integrante da lógica de proteção do Estado.

Na sequência, foi apresentada a atuação do Núcleo de Segurança e Credenciamento, estrutura instituída pela Lei de Acesso à Informação, com a finalidade específica de assegurar a proteção dos segredos de Estado. Trata-se de um volume pequeno das informações produzidas pelo setor público, porém cujo eventual comprometimento tende a ocasionar danos significativos aos interesses do Estado e da sociedade.

O Núcleo foi concebido para exercer a coordenação das estruturas responsáveis pela proteção dessas informações sensíveis, desempenhando suas atribuições por meio da edição de normativos, do credenciamento de segurança de pessoas, da realização de ações de fiscalização e da habilitação de órgãos e entidades. Essas atividades encontram-se regulamentadas por decreto específico que disciplina a aplicação da Lei de Acesso à Informação no tocante às informações classificadas (Decreto nº 7.845/2012).

Relevância Geopolítica e Ameaças Contemporâneas

No contexto geopolítico contemporâneo, caracterizado por instabilidade e intensificação de disputas estratégicas, a proteção dos segredos de Estado assume importância ainda mais acentuada. Tal cenário é marcado pelo aumento da complexidade das ameaças, que se manifestam tanto no ambiente digital quanto por meio de técnicas tradicionais de inteligência adversa e espionagem. Diante desse quadro, o Núcleo de Segurança e Credenciamento atua para enfrentar esses desafios, buscando aproximar a maturidade brasileira das práticas adotadas por grandes economias e Estados com elevado grau de maturidade institucional em segurança da informação sigilosa.

Considerando a posição do Brasil entre as maiores economias do mundo, ficou evidente o esforço nacional para alcançar níveis de maturidade compatíveis com os padrões adotados por países de porte equivalente, no que se refere à proteção de informações sensíveis e classificadas.

Contribuições do Núcleo no Âmbito da Política Nacional de Segurança da Informação

No processo de elaboração da Política Nacional de Segurança da Informação, o Núcleo de Segurança e Credenciamento participou das fases iniciais de discussão e da construção das primeiras minutas do decreto que instituiu a política. No que se refere aos objetivos da PNSI, foram identificadas três dimensões nas quais a atuação do Núcleo se apresenta de forma particularmente relevante.

A primeira dimensão corresponde à proteção das informações estatais sensíveis, objetivo que se alinha diretamente à missão institucional do Núcleo.

A segunda dimensão refere-se ao papel normativo. Como exemplo recente, mencionou-se a publicação de instrução normativa específica sobre o uso de computação em nuvem para o tratamento de informações classificadas.

A terceira dimensão diz respeito à atuação internacional. Uma das competências do Núcleo consiste na negociação de acordos internacionais entre Estados, com o objetivo de estabelecer equivalências jurídicas para o tratamento de informações sigilosas. Esses instrumentos jurídicos viabilizam tanto a troca segura de informações entre países quanto a cooperação industrial em setores estratégicos, como o setor de defesa.

Em síntese, a contribuição do Núcleo de Segurança e Credenciamento se estrutura nessas três dimensões principais — proteção de informações sensíveis, normatização e atuação internacional, configurando-se como elemento decisivo para o fortalecimento da Política Nacional de Segurança da Informação.

Centralidade da Proteção de Informações Classificadas no Ecossistema de Segurança do Estado

Foi enfatizada a relevância estratégica do trabalho desenvolvido pelo Núcleo de Segurança e Credenciamento, ressaltando-se que, embora as informações classificadas representem parcela reduzida do volume total de informações produzidas pelo Estado, sua fragilidade e eventual comprometimento podem gerar consequências de grande magnitude, frequentemente superiores à capacidade de mitigação ou de resposta tempestiva por parte das instituições públicas.

Evidenciou-se o compromisso institucional de alinhar, de forma cada vez mais consistente, a dimensão da informação classificada às capacidades de ação previstas no âmbito da Política Nacional de Segurança da Informação e à futura Estratégia Nacional de Segurança da Informação. Enfatizou-se que essa estratégia deverá contemplar não apenas diretrizes conceituais, mas também ações

práticas, orientações estratégicas e, posteriormente, um plano estruturado de implementação.

Esse esforço envolve a necessidade de refletir sobre mecanismos de proteção, ações de conscientização e fortalecimento das capacidades institucionais da Administração Pública Federal como um todo para o adequado tratamento das informações classificadas. Ressaltou-se que essa dimensão é central não apenas para a proteção de conteúdos sensíveis, mas também por seu papel como vetor econômico para indústrias estratégicas nacionais. Por meio do fortalecimento das capacidades institucionais dos órgãos envolvidos, bem como da celebração de acordos adequados e da adoção de boas práticas, torna-se possível viabilizar processos vantajosos para o país, especialmente em setores sensíveis, ao mesmo tempo em que se assegura a proteção de recursos estratégicos e de propriedades industriais relevantes para o Estado.

Nesse sentido, reforçou-se a importância de ampliar o conhecimento sobre a atuação do Núcleo de Segurança e Credenciamento também sob essa perspectiva estratégica e econômica.

Desafios Atuais, Perspectivas Futuras e Soberania Digital

Na sequência, foi introduzido novo eixo de debate do webinário, voltado à compreensão do cenário atual da segurança da informação e, a partir dessa análise, à construção de perspectivas futuras. Informou-se que o evento contemplaria, posteriormente, uma etapa específica dedicada à discussão de visões de futuro.

Foi apresentada, então, a questão norteadora desse novo bloco de discussões, estruturada em duas partes. A primeira parte buscou abordar os desafios impostos à Administração Pública pelo acelerado processo de evolução tecnológica, frequentemente em ritmo superior à capacidade de resposta das instituições estatais, bem como pelo crescimento expressivo das ameaças associadas a esse contexto. Nesse âmbito, questionou-se quais seriam os principais desafios percebidos para a Administração Pública e de que forma os órgãos representados poderiam atuar, dentro do ecossistema de proteção da segurança da informação, para enfrentá-los.

A segunda parte da questão propôs a reflexão sobre a relação entre esses desafios e a construção da soberania digital do Estado. Informou-se que o tema da soberania digital vem sendo debatido em diferentes grupos de trabalho no âmbito da Presidência da República e em outros espaços de diálogo com especialistas e acadêmicos. Observou-se que a soberania digital compreende múltiplas dimensões, incluindo dados, equipamentos, operações, processos de fiscalização e capacidades institucionais associadas à supervisão e ao controle. Ressaltou-se que todo esse conjunto de elementos integra um ecossistema diretamente relacionado à noção de soberania digital do Estado.

Por fim, foi anunciada a formulação de uma questão específica dirigida ao representante do Núcleo de Segurança e Credenciamento, a ser apresentada após as manifestações iniciais dos demais participantes. Essa questão buscaria explorar o papel do Núcleo no equilíbrio entre as exigências de transparência previstas na Lei de Acesso à Informação e a necessidade de proteção das informações classificadas. Foi solicitado o aprofundamento acerca das principais medidas de classificação que distinguem as informações classificadas das informações ostensivas tratadas cotidianamente no âmbito da Presidência da República e da Administração Pública Federal.

Fragilidades Estruturais Persistentes

Foram apontadas fragilidades estruturais recorrentes nos órgãos públicos, entre as quais se observa a insuficiência de

governança em segurança da informação. Observou-se que, frequentemente, a alta administração não assume de forma efetiva sua responsabilidade pela gestão dos riscos de segurança, deixando de reconhecer a segurança da informação como risco estratégico organizacional.

Do ponto de vista técnico-operacional, foi percebida a dificuldade dos órgãos em manter uma gestão adequada de vulnerabilidades, com ativos devidamente atualizados e corrigidos. Somam-se a isso os desafios relacionados à gestão de identidades e acessos, com a necessidade de adoção de mecanismos modernos de autenticação multifator, cuja implementação ainda se mostra incipiente em diversos contextos da Administração Pública.

Outro desafio estrutural relevante refere-se à escassez de profissionais qualificados. Observou-se que muitos especialistas altamente capacitados buscam oportunidades mais atrativas, inclusive no exterior, ou migram entre órgãos em função de diferenças estruturais e remuneratórias. Esse cenário gera a percepção de baixo retorno sobre investimentos em capacitação, embora se tenha ressaltado que a ausência de pessoal qualificado inviabiliza o uso efetivo de ferramentas e soluções tecnológicas. Foi enfatizado que a aquisição de tecnologias, por si só, não é suficiente para garantir níveis adequados de segurança, sendo imprescindível a existência de equipes capacitadas para sua operação e gestão.

Repensando Modelos de Infraestrutura e Serviços Compartilhados

Introduziu-se, ainda, a reflexão sobre a fragmentação das estruturas de tecnologia da informação na Administração Pública. Observou-se que, atualmente, praticamente todos os órgãos mantêm infraestruturas próprias de TI, incluindo data centers, equipes e recursos dedicados, independentemente do nível de maturidade ou capacidade institucional. Esse modelo resulta em duplicação de esforços e consumo elevado de recursos financeiros e humanos.

Diante das limitações recorrentes de orçamento, pessoal e capacidade operacional, foi sugerida a necessidade de discutir, em nível estratégico, a adoção de modelos de serviços de tecnologia da informação compartilhados entre órgãos, seja no âmbito do Poder Executivo, do Legislativo ou do Judiciário. Tal abordagem poderia representar alternativa viável para otimizar recursos, ampliar a resiliência e elevar o nível de segurança, especialmente para instituições com menor capacidade instalada.

Por fim, ressaltou-se que a expectativa pela ampliação de recursos financeiros e humanos, embora legítima, nem sempre se concretiza, o que impõe à Administração Pública o desafio de repensar modelos organizacionais e operacionais, buscando soluções estruturais mais sustentáveis diante do cenário tecnológico e de ameaças em constante evolução.

Evolução Tecnológica e Desafios Estruturais de Capacidade no Setor Público

A intervenção iniciou-se com uma contextualização histórica da área de tecnologia da informação no governo federal, especialmente a partir do início da década de 2010, período marcado pela realização do primeiro concurso público para Analistas de Tecnologia da Informação, no âmbito da Administração Pública Federal. Observou-se que, naquele momento, havia forte preocupação institucional, inclusive por parte do então órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), com os processos de contratação de soluções de TI.

Esse período foi caracterizado por transformações relevantes, como a padronização do uso do pregão eletrônico e a introdução das tecnologias de virtualização, que demandaram processos

de adaptação para sua incorporação ao ambiente governamental. Na sequência, ampliaram-se as discussões relativas aos Centros de Processamento de Dados (CPDs), com a adoção de modelos de colocation, virtualização e contratação de serviços junto a outros órgãos e empresas especializadas.

Posteriormente, emergiram novas ondas tecnológicas, como o uso de soluções de big data e, mais recentemente, a inteligência artificial. Observou-se que, diferentemente dos ciclos tecnológicos anteriores, essas inovações passaram a surgir em ritmo significativamente mais acelerado, dificultando a capacidade das instituições públicas de assimilar, processar e internalizar adequadamente essas mudanças em suas estruturas organizacionais e operacionais. Nesse cenário, ficou evidente que o avanço da inteligência artificial tem sido particularmente disruptivo, frequentemente superando a capacidade de resposta institucional.

Retomando aspectos mencionados anteriormente por outros participantes, enfatizou-se que a questão relacionada à força de trabalho constitui elemento central desse desafio. Ao longo dos anos, verificou-se dificuldade persistente em estruturar equipes de tecnologia da informação suficientemente robustas e dedicadas para acompanhar as sucessivas evoluções tecnológicas. Essa limitação não se restringe a uma única instituição, configurando-se como desafio transversal à Administração Pública Federal.

Apesar dos esforços empreendidos pelo Ministério da Gestão e da Inovação em Serviços Públicos, incluindo iniciativas de fortalecimento do SISP, realização de concursos públicos e implementação de mecanismos remuneratórios, persiste a dificuldade de constituir estruturas de TI com capacidade técnica e atratividade comparáveis às oferecidas pelo mercado privado.

Essa defasagem impacta diretamente a capacidade institucional de acompanhar a evolução tecnológica, resultando em lacunas relacionadas a pessoal, infraestrutura e atualização técnica. Tais limitações tornam-se particularmente críticas no campo da segurança cibernética, afetando a capacidade de resposta a vulnerabilidades e o enfrentamento de ameaças crescentes.

Por fim, observou-se que o acúmulo simultâneo de demandas técnicas, operacionais e estratégicas gera sobrecarga nas equipes existentes, configurando-se como um dos principais desafios contemporâneos enfrentados pela Administração Pública no contexto da segurança da informação e da segurança cibernética.

Centralidade do Capital Humano no Enfrentamento das Ameaças Emergentes

Foi enfatizada a relevância estratégica do recurso humano para a estruturação das atividades institucionais e para o enfrentamento das novas ameaças no campo da segurança da informação e da segurança cibernética. Foi informado que essa temática constitui um dos pontos centrais das discussões conduzidas no âmbito do Gabinete de Segurança Institucional.

A primeira questão ressaltada refere-se à dificuldade de competição com o mercado privado na atração e retenção de profissionais especializados. Em um contexto de escassez de mão de obra qualificada, observa-se que os profissionais disponíveis tendem a optar por ambientes que oferecem condições remuneratórias mais atrativas, o que impacta diretamente a capacidade do setor público de compor e manter equipes adequadas. Esse desafio se agrava em áreas que demandam grande contingente de especialistas, ao mesmo tempo em que a evolução tecnológica ocorre em ritmo acelerado.

Tal limitação repercute em todo o ecossistema de segurança da informação.

Em interações com diferentes órgãos, especialmente no debate sobre a formulação de políticas de segurança da informação ou sobre a operacionalização de diretrizes da Estratégia Nacional de Cibersegurança, é recorrente a manifestação de que as equipes disponíveis são reduzidas frente à relevância estratégica das atribuições sob sua responsabilidade.

Nesse contexto, apontou-se como perspectiva necessária o reconhecimento de que as áreas de segurança da informação e de segurança cibernética não devem ser tratadas como atividades paralelas ou periféricas, mas como funções transversais às estruturas organizacionais. Tal entendimento implica a necessidade de políticas públicas específicas, planejamento orçamentário adequado e integração da temática aos processos de planejamento institucional, de modo a fortalecer a capacidade do Estado de mitigar e responder às ameaças emergentes.

Natureza do Problema da Cibersegurança e Desafios de Governança

Foram apresentados pontos complementares aos já discutidos, com destaque para a especificidade da cibersegurança enquanto política pública. Ressaltou-se que, diferentemente de áreas como saúde, educação ou saneamento — caracterizadas por políticas estruturantes de natureza predominantemente incremental, ainda que variem em prioridade, escopo territorial ou volume de investimento, a cibersegurança se distingue por envolver a atuação direta contra um adversário ativo.

Nesse contexto, a cibersegurança, assim como a defesa, configura-se como um campo no qual há agentes que buscam deliberadamente comprometer ou destruir as estruturas e capacidades construídas pelo Estado. Essa característica torna a cibersegurança um problema público particularmente complexo, exigindo atuação contínua baseada em conhecimento especializado e inteligência. Salientou-se que o enfrentamento eficaz dessas ameaças pressupõe a compreensão aprofundada do adversário, o que confere centralidade às atividades de inteligência, não apenas no âmbito da segurança, mas de forma transversal em diversas áreas da Administração Pública.

Coordenação Institucional e Limitações dos Modelos Tradicionais

Outro desafio relevante apontado refere-se à coordenação institucional. Reiterou-se que o Brasil ainda carece de uma governança mais robusta em segurança cibernética, desafio ampliado pelas dimensões territoriais do país e pelo elevado grau de digitalização de seus serviços e processos. Observou-se que, em determinados contextos nacionais ou em problemas públicos menos complexos, a coordenação exclusivamente ministerial pode ser suficiente para alcançar resultados satisfatórios.

Entretanto, no caso da segurança cibernética, tal abordagem mostra-se insuficiente. Trata-se de um problema multidimensional e integralmente transversal, que envolve múltiplos atores públicos e privados. Avaliou-se que a coordenação baseada apenas em instâncias interministeriais, grupos de trabalho ou programas isolados não é capaz de responder de forma eficaz à complexidade do fenômeno. Defendeu-se, assim, a necessidade de uma instância de coordenação externa, dedicada exclusivamente a essa finalidade, capaz de potencializar recursos escassos e promover maior coerência sistêmica nas ações de segurança cibernética.

Regulação, Fiscalização e Internalização do Risco

Por fim, ficou evidente o papel da regulação e da fiscalização como instrumentos fundamentais de governança. Observou-se que essas ferramentas

auxiliam gestores que já possuem consciência da relevância do risco, ao mesmo tempo em que obrigam entes públicos e privados a internalizarem a segurança como elemento estratégico de suas decisões.

Foi citado, como exemplo, o Comitê de Segurança de Infraestruturas Críticas, no qual participam diversos entes privados. Nesse contexto, a regulação desempenha papel decisivo ao induzir investimentos em segurança por parte de atores que, de outra forma, poderiam subestimar os riscos ou postergar ações de proteção. Esse mecanismo contribui para a elevação do nível geral de maturidade do ecossistema de segurança cibernética.

Concluiu-se que a regulação e a fiscalização não devem ser compreendidas como fins em si mesmas, mas como instrumentos que promovem a internalização do risco, incentivando a adoção de sistemas de proteção, boas práticas, capacitação de pessoal e políticas adequadas de contratação e remuneração. Esses elementos foram apresentados como desafios centrais ainda a serem enfrentados no fortalecimento da segurança cibernética e da segurança da informação.

Transparência, Informação Classificada e Sensibilidade Institucional

Introduziu-se o debate sobre o equilíbrio entre a transparência pública, conforme estabelecido pela Lei de Acesso à Informação, e a necessidade de proteção das informações classificadas. Ressaltou-se que esse equilíbrio assume relevância ainda maior diante do ecossistema complexo de segurança da informação e das diversas dimensões anteriormente discutidas pelos participantes.

Foi enfatizado que a sensibilidade associada às informações classificadas não se manifesta apenas em cenários de crise ou de ameaça direta, mas também decorre, em grande medida, do desconhecimento institucional acerca das formas adequadas de tratamento desse tipo de informação e de suas características específicas. Nesse contexto, foi observada a importância de esclarecer essas questões para promover maior compreensão, segurança jurídica e efetividade na proteção das informações sensíveis.

Conceito Jurídico de Informação Classificada e Governança Institucional

A discussão sobre transparência e proteção da informação classificada está diretamente relacionada à correta compreensão do conceito jurídico de informação classificada. Embora o termo “classificação” possua acepção própria no campo arquivístico, no âmbito jurídico — especialmente à luz da Lei de Acesso à Informação, a informação classificada corresponde àquela à qual se atribui grau de sigilo em razão do potencial impacto negativo sobre a segurança do Estado ou da sociedade fruto da sua divulgação não autorizada.

Esse entendimento decorre do disposto no artigo 5º, inciso XXXIII, da Constituição Federal, que assegura o direito de acesso à informação, ressalvadas aquelas cujo acesso possa comprometer a segurança do Estado e da sociedade. A Lei de Acesso à Informação regulamenta esse comando constitucional, estabelecendo os limites e as restrições necessárias em função da proteção desses interesses superiores.

No tratamento da informação classificada, foi observada a existência de uma governança tripartite, estruturada a partir da atuação coordenada de três instâncias institucionais, cada qual com atribuições específicas. O Núcleo de Segurança e Credenciamento exerce o papel de proteção da informação, sendo responsável por prover mecanismos técnicos e organizacionais, coordenar as estruturas competentes e editar normativos aplicáveis, inclusive para entidades privadas que manejam informações classificadas. A

Controladoria-Geral da União atua como autoridade de monitoramento da Lei de Acesso à Informação, fiscalizando a correta aplicação dos processos de classificação e de proteção, não apenas sob a ótica da transparência. A Comissão Mista de Reavaliação de Informações, sediada na Casa Civil, por sua vez, desempenha a função de instância recursal e de reavaliação das informações classificadas.

Classificação, Sigilo e Segurança da Informação

Ressaltou-se a recorrente confusão conceitual entre segurança da informação e restrição de acesso. Observou-se que, muitas vezes, as iniciativas voltadas à segurança são equivocadamente associadas à intenção de limitar a transparência pública. Entretanto, o papel do Núcleo consiste em assegurar que as informações definidas pelo Estado como sensíveis sejam efetivamente protegidas, por meio da adoção de medidas proporcionais ao seu grau de sensibilidade ou sigilo.

O ato de classificação de informações, conforme previsto no artigo 24 da Lei de Acesso à Informação, baseia-se em dois critérios fundamentais. O primeiro e principal critério refere-se ao risco potencial à segurança do Estado e da sociedade decorrente da divulgação da informação. O segundo critério diz respeito ao tempo de restrição de acesso, determinado de acordo com o grau de sigilo atribuído.

A legislação brasileira prevê três graus de sigilo, cada qual associado a prazos máximos de restrição de acesso: informações classificadas como reservadas possuem prazo de até cinco anos; informações classificadas como secretas possuem prazo de até quinze anos; e informações classificadas como ultrassecretas possuem prazo de até vinte e cinco anos, admitida prorrogação nos termos legais.

Observa-se, contudo, que a prática administrativa frequentemente se limita à observância da temporalidade, desconsiderando o critério do risco potencial, o qual é fundamental para a correta classificação da informação. A classificação de uma informação como secreta, por exemplo, exige a adoção de parâmetros criptográficos específicos, definidos em normas técnicas, além da limitação de acesso exclusivamente a pessoas devidamente credenciadas no grau correspondente. Portanto, o ato de classificação transcende a mera definição de prazo, implicando um conjunto de obrigações técnicas, organizacionais e procedimentais.

Instrumentos Normativos e Desafios Operacionais

O papel do Núcleo de Segurança e Credenciamento inclui a orientação das autoridades classificadoras e dos órgãos públicos quanto ao correto ato de classificação, às medidas de proteção aplicáveis e ao tratamento adequado das informações após a atribuição do grau de sigilo. Para tanto, foi estruturado um conjunto de normas e instrumentos que organizam essas medidas em quatro pilares principais.

O primeiro pilar corresponde ao Decreto nº 7.845, que regulamenta a proteção das informações classificadas no âmbito da Lei de Acesso à Informação, complementado por normativos infralegais específicos. O segundo pilar abrange as normas de credenciamento de segurança, voltadas à realização de investigações de vida pregressa, com o objetivo de mitigar riscos associados ao fator humano. O terceiro pilar refere-se às normas de criptografia de Estado, desenvolvidas em cooperação com o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, atualmente em processo de revisão. O quarto pilar consiste na norma recentemente editada sobre o tratamento de informações classificadas em ambientes de computação em nuvem, a qual estabelece requisitos

relacionados à soberania de dados e às condições operacionais necessárias para autorizar o uso de nuvem nesse contexto.

Por fim, ficou evidente que a atuação do Núcleo se desenvolve em um ambiente marcado por constrangimentos administrativos, como a escassez de pessoal e de recursos orçamentários. Considerando que essas limitações já afetam de maneira significativa as áreas de segurança da informação em geral, a proteção de informações classificadas impõe desafios adicionais, em razão de seu elevado nível de sensibilidade. Ainda assim, reafirmou-se o compromisso institucional com a garantia dessa proteção especial, reconhecida como indispensável à salvaguarda dos interesses do Estado e da sociedade.

Diferenciação entre Informação Ostensiva e Informação Classificada

Ressaltou-se que, como regra geral, as informações produzidas pelo setor público possuem natureza pública e são de acesso irrestrito. Esse princípio encontra-se consagrado na Lei de Acesso à Informação, que estabelece a publicidade como regra e a restrição como exceção.

A própria Lei de Acesso à Informação define, de forma taxativa, as hipóteses em que a divulgação de informações pode ser legalmente restringida. Entre essas exceções encontram-se as informações classificadas, cuja divulgação possa representar risco à segurança do Estado ou da sociedade, sendo essa a categoria de informação que demanda a atribuição formal de grau de sigilo.

Além das informações classificadas, foram mencionadas outras categorias de informações cujo acesso é legalmente restrito, tais como: informações pessoais, que, como regra, não são públicas, ressalvadas as hipóteses previstas na legislação de proteção de dados pessoais; informações protegidas por sigilo de propriedade intelectual, incluindo aquelas relacionadas a atividades de pesquisa e desenvolvimento; segredos industriais; informações submetidas a sigilo judicial; bem como outros tipos de sigilo expressamente previstos em legislação específica.

Reiterou-se, entretanto, que essas hipóteses constituem exceções ao regime geral de publicidade, de modo que as informações públicas são, em sua maioria, ostensivas e de acesso irrestrito. O Núcleo de Segurança e Credenciamento atua de forma específica sobre o subconjunto das informações classificadas em grau de sigilo, cuja restrição de acesso decorre do potencial impacto de sua divulgação sobre a segurança do Estado e da sociedade.

Consciência Institucional sobre Regimes de Informação

Foi reafirmada a centralidade da distinção entre informação ostensiva e informação classificada, apresentando-se a necessidade de ampliar a compreensão institucional não apenas sobre o regime geral de publicidade das informações, mas também sobre a possibilidade de produção de informações classificadas pelos órgãos públicos e sobre a consequente obrigação de estruturar mecanismos adequados para seu tratamento e proteção.

Nesse sentido, enfatizou-se a importância de promover maior conscientização junto aos órgãos da Administração Pública Federal, de modo a assegurar que a gestão da informação classificada seja realizada de forma consistente com os marcos normativos e com as capacidades institucionais disponíveis.

Soberania Digital na Perspectiva do Controle Externo

Dando continuidade ao debate, foi introduzido o tema sobre soberania digital, a partir da perspectiva do controle externo exercido pelo Tribunal de Contas da União,

com base nos trabalhos em curso e nos diálogos institucionais mantidos no âmbito do Estado brasileiro.

A soberania digital, conforme prevista no artigo 3º da Política Nacional de Segurança da Informação, foi associada à capacidade do país de controlar e proteger seus dados e sistemas críticos, assegurando que as decisões estratégicas relacionadas a esses ativos sejam tomadas em consonância com o interesse nacional. Ressaltou-se tratar-se de um tema complexo, multifacetado e permeado por variáveis históricas, tecnológicas, econômicas e geopolíticas.

Observou-se que, historicamente, o Brasil ocupou majoritariamente a posição de consumidor de tecnologias, e não de produtor, o que gera fragilidades estruturais quando se discute soberania digital. Essa dependência tecnológica impõe desafios adicionais à construção de autonomia decisória e operacional no tratamento de dados e na operação de sistemas críticos.

Foi observada, nesse contexto, a relevância da Instrução Normativa nº 8/2025, editada pelo Gabinete de Segurança Institucional, que estabelece requisitos de segurança para o tratamento de informações classificadas. Avaliou-se que esse normativo representa avanço significativo ao definir parâmetros sobre quais informações podem ser processadas em ambientes externos ao território nacional, como nuvens públicas, e quais demandam infraestrutura sob controle nacional.

Apesar desse avanço, foram elencados desafios persistentes. O primeiro refere-se à superação da dependência histórica de tecnologias externas, questão reconhecida como de difícil solução e sem respostas imediatas. O segundo desafio diz respeito à efetiva implementação dos normativos existentes, evitando que permaneçam restritos ao plano formal. O terceiro desafio envolve a conciliação entre os requisitos de segurança associados ao uso de nuvem pública e as demandas por economia de escala, redução de custos e restrições orçamentárias enfrentadas pelo setor público.

Considerou-se que, para serviços e informações de maior sensibilidade, poderá ser necessário adotar modelos baseados em infraestrutura própria (on-premises), o que demanda reflexão estratégica em nível nacional. Ressaltou-se, ainda, que o país enfrenta limitações estruturais nesse processo, reforçando a complexidade do tema.

Foi mencionado que o Tribunal de Contas da União se encontra em fase de conclusão de trabalho específico voltado à avaliação da temática da nuvem soberana, cujos resultados, embora ainda não divulgados, deverão fornecer subsídios relevantes para o debate nacional.

Dimensão Geopolítica da Soberania Digital

Encerrada a manifestação do Tribunal de Contas da União, foi destacada a relevância do tema da soberania digital também sob a perspectiva geopolítica. Ressaltou-se que essa dimensão não se limita à condição do país como consumidor de tecnologia, mas se estende ao seu papel como ator relevante no sistema internacional.

Observou-se que, embora o Brasil dependa do consumo de tecnologias externas, o país figura como grande produtor de informações enquanto Estado de relevância global. Essa condição reforça a necessidade de refletir sobre a soberania digital não apenas como questão técnica ou administrativa, mas como elemento estratégico inserido nas dinâmicas geopolíticas contemporâneas.

Soberania Digital sob a Perspectiva da Inteligência, Pesquisa e Cooperação Institucional

A discussão foi ampliada a partir de um paralelo histórico com o contexto da divulgação dos documentos do WikiLeaks, ocorrido em meados da década de 2010, período marcado por instabilidade

geopolítica e por iniciativas pontuais do Estado brasileiro voltadas à proteção de suas informações. Observou-se que, naquele momento, embora tenham sido adotadas algumas medidas específicas — como propostas de soluções de comunicação segura, ainda não havia uma compreensão estruturada e integrada do conceito de soberania digital como hoje se delineia.

No cenário atual, caracterizado por maior complexidade geopolítica e tecnológica, a soberania passou a ser compreendida de forma mais clara como um objetivo estratégico do Estado brasileiro. Ressaltou-se que a soberania digital possui múltiplas vertentes, que devem ser consideradas de maneira articulada.

Entre essas vertentes, há o aspecto tecnológico, associado à capacidade de desenvolver tecnologia própria ou, alternativamente, à permanência em uma posição de dependência como consumidor de soluções externas. Essa condição foi apontada como um dos fatores que contribuem para a predominância de grandes empresas de tecnologia no cenário nacional.

Considerando a multiplicidade de dimensões envolvidas, foi defendida a necessidade de priorização estratégica. Avaliou-se que nem todas as instituições possuem condições de atuar em todas as frentes da soberania digital, sendo mais eficaz concentrar esforços nas áreas de maior tradição, competência técnica e capacidade institucional. No caso da Agência Brasileira de Inteligência, cuja atuação envolve o tratamento de informações restritas e sigilosas, a confidencialidade foi observada como eixo prioritário, sem prejuízo das dimensões de integridade e disponibilidade.

Nesse contexto, exemplificou-se que diferentes instituições contribuem para a soberania digital de maneiras complementares: algumas, como aquelas responsáveis pela prestação de serviços públicos e pela infraestrutura tecnológica, fortalecem a soberania por meio da oferta de serviços de nuvem e de plataformas essenciais; outras contribuem por meio do desenvolvimento de tecnologias específicas; enquanto há aquelas que atuam no fomento à pesquisa, à inovação e à produção de conhecimento.

Ressaltou-se que o Brasil possui reconhecida capacidade de fomento ao desenvolvimento científico e tecnológico, seja por meio de financiamento público, seja por iniciativas de cooperação entre instituições públicas e privadas. As universidades também foram apontadas como importantes produtoras de conhecimento. Entretanto, identificou-se como lacuna a ausência de uma visão mais centralizada e integrada sobre o conjunto de iniciativas e soluções tecnológicas em desenvolvimento no país.

Concluiu-se que, ao concentrar esforços em suas áreas de maior expertise, cada instituição contribui com peças específicas que, somadas, compõem o arcabouço necessário à construção da soberania digital. Essa abordagem colaborativa e complementar foi apresentada como estratégia viável para enfrentar a complexidade do desafio.

Cooperação Interinstitucional e Redução de Esforços Dispersos

Em seguida, apresentou-se a relevância do fortalecimento da cooperação interinstitucional como fator de aceleração da construção da soberania digital. Observou-se que o aumento da capacidade de compartilhamento de conhecimento e a redução da duplicidade de esforços frequentemente verificada na repetição de iniciativas semelhantes por diferentes órgãos contribuem para maior eficiência e eficácia das ações estatais.

Ressaltou-se que essa lógica de cooperação interagências representa um amadurecimento das práticas institucionais, permitindo ganhos de escala, racionalização de recursos e maior coerência estratégica na atuação do Estado brasileiro.

Soberania Digital como Processo Contínuo de Construção

A soberania digital foi caracterizada como um processo contínuo e relacional, não se tratando de um atributo absoluto ou binário. Ressaltou-se que a soberania se constrói sempre em relação a outros atores e que, nesse sentido, o Brasil já apresenta níveis relevantes de soberania em determinadas áreas, ao mesmo tempo em que desenvolve capacidades em outros domínios. À medida que ações setoriais se consolidam ao longo do tempo, tende a emergir um conjunto nacional mais autônomo e resiliente.

No âmbito da Estratégia Nacional, foi evidenciada a representação gráfica que posiciona a soberania como uma camada mais externa, evidenciando tratar-se de um objetivo de longo prazo, cuja consecução não ocorre de forma simples ou imediata. Essa perspectiva reforça a compreensão de que a soberania digital demanda esforços graduais, cumulativos e sustentados.

Foi enfatizado que cada novo ciclo tecnológico representa, simultaneamente, um recomeço e uma oportunidade estratégica. No contexto atual, marcado pela ascensão da inteligência artificial, apontou-se a possibilidade de o país se posicionar de maneira mais avançada em relação a tecnologias emergentes. De modo semelhante, mencionou-se o potencial de adoção de técnicas criptográficas pós-quânticas de forma transversal na Administração Pública, condicionada à existência de vontade política e de consciência tecnológica nacional. Observou-se que a recorrente perda de oportunidades decorre menos de limitações técnicas absolutas e mais da ausência de decisões estratégicas coordenadas.

Defendeu-se a necessidade de construção contínua a partir do que há de mais avançado em termos tecnológicos. Em determinados espaços de formulação estratégica, a soberania digital tem sido decomposta em dimensões — como soberania de dados, soberania operacional e soberania tecnológica — com o objetivo de tornar o problema mais manejável. Reconheceu-se, entretanto, que a soberania tecnológica, entendida como a capacidade de produzir equipamentos e tecnologias de ponta, representa um dos maiores desafios estruturais.

Nesse contexto, foi rejeitada a ideia de conformismo diante das limitações atuais. Argumentou-se que, embora existam condicionantes históricos e estruturais, essas não devem ser interpretadas como destino inevitável. Ao contrário, ressaltou-se a necessidade de ação deliberada e progressiva, orientada pela comparação com referências internacionais e pela valorização das capacidades nacionais existentes.

Assim, a soberania digital constitui um desafio permanente, uma vez que a evolução tecnológica é contínua e imprevisível. Ainda assim, salientou-se que esse caráter dinâmico não exime o Estado da responsabilidade de adotar uma postura ativa, estratégica e adaptativa, voltada à construção de relações mais soberanas no ambiente digital.

Adaptação Permanente diante da Mutabilidade dos Desafios

Por fim, foi reforçada a compreensão de que o processo de construção da soberania digital exige constante capacidade de adaptação. Observou-se que os desafios se transformam ao longo do tempo, impondo a necessidade de reorganização contínua das estruturas institucionais, das estratégias adotadas e das formas de atuação do Estado, de modo a responder de forma eficaz às mudanças do ambiente tecnológico e geopolítico.

Certificação, Mitigação de Dependências Tecnológicas e Caminhos Intermediários de Soberania

Foi acrescentada ao debate a reflexão sobre os limites práticos da busca por supremacia tecnológica plena. Foi observado

que a obtenção de supremacia integral demandaria a existência de uma indústria nacional suficientemente robusta para competir em escala internacional com grandes empresas de tecnologia, o que implicaria décadas de investimentos públicos intensivos e a adoção de políticas industriais altamente estruturadas. Observou-se que apenas um número muito restrito de países dispõe atualmente dessas condições.

Diante desse cenário, foi apresentada a experiência adotada por outros Estados como alternativa intermediária viável, também prevista na Estratégia Nacional de Segurança Cibernética, consistente na implementação de esquemas nacionais de certificação de sistemas de informação. Esses mecanismos permitem ao Estado avaliar, de forma soberana, se determinadas tecnologias atendem aos requisitos definidos como estratégicos e se tais requisitos são efetivamente cumpridos.

Ressaltou-se que esse modelo não elimina por completo a dependência tecnológica externa, mas estabelece uma camada adicional de mitigação e de gestão dessa dependência, alinhada aos interesses nacionais. Trata-se, portanto, de uma abordagem pragmática, que busca equilibrar limitações estruturais com a necessidade de exercer maior controle e autonomia decisória sobre tecnologias críticas.

Nesse sentido, observou-se que a construção de requisitos nacionais, mecanismos de validação e esquemas de certificação constitui caminho intermediário relevante entre a dependência total e a busca por uma supremacia tecnológica de difícil alcance. Essa abordagem tem sido objeto de reflexão no âmbito do Núcleo de Segurança e Credenciamento, como parte das estratégias para fortalecimento da soberania digital.

Debate sobre Perspectivas Futuras

Na sequência, foi reconhecida a pertinência da discussão sobre certificações e padrões nacionais como elemento estratégico necessário à construção da soberania digital. Ressaltou-se que a definição de matrizes e padrões nacionais de certificação representa iniciativa fundamental para orientar a adoção segura de tecnologias e fortalecer a capacidade do Estado de exercer controle sobre sistemas e dados críticos.

Em seguida, iniciou-se o terceiro bloco do webinário, dedicado à discussão das perspectivas futuras. Informou-se que, nessa etapa, o debate se concentraria nas estratégias de implementação da Política Nacional de Segurança da Informação, recentemente publicada, e em sua materialização por meio de iniciativas concretas nos órgãos públicos.

A questão inicial dirigida aos participantes buscou identificar como as instituições representadas planejam ou já vêm planejando — a implementação de ações alinhadas à Política Nacional de Segurança da Informação, considerando seu papel como diretriz orientadora para os órgãos da Administração Pública. Foi proposta a reflexão sobre quais aspectos do ecossistema nacional de segurança da informação demandam aprimoramento e de que forma as iniciativas institucionais podem contribuir para esse fortalecimento.

Foram apresentadas, ainda, duas questões específicas. A primeira, direcionada ao Tribunal de Contas da União, abordou como o órgão pretende conduzir seus ciclos de auditoria diante de cenários de indefinição e de possíveis mudanças regulatórias. A segunda, dirigida ao Núcleo de Segurança e Credenciamento, tratou dos principais projetos previstos não apenas para o curto prazo, mas para um ciclo mais amplo de implementação da nova Política Nacional de Segurança da Informação, bem como das estratégias para operacionalização dos normativos associados.

Iniciativas do Cepesc/ABIN alinhadas à Política Nacional de Segurança da Informação

No âmbito da Agência Brasileira de Inteligência, e em especial do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, foi compartilhado que a atuação institucional tem sido historicamente concentrada no campo da criptografia. Nesse contexto, as iniciativas alinhadas à Política Nacional de Segurança da Informação voltam-se, de forma prioritária, ao fortalecimento da segurança da informação e à proteção de infraestruturas críticas e serviços essenciais, por meio do emprego de mecanismos criptográficos avançados.

Ressaltou-se o desenvolvimento de pesquisas em criptografia pós-quântica, bem como os esforços voltados à preparação do cenário de transição para esse novo paradigma tecnológico. O objetivo central consiste na incorporação progressiva de soluções criptográficas pós-quânticas em sistemas estruturantes do governo, em articulação com outros órgãos da Administração Pública Federal.

Essas iniciativas visam assegurar a proteção adequada dos dados por meio de seu encapsulamento criptográfico, garantindo os pilares da segurança da informação — integridade, disponibilidade e confidencialidade aplicáveis a dados pessoais, dados sensíveis e informações sigilosas. Foi observado que o Cepesc possui capacidade de prover essas soluções não apenas para a ABIN, mas também para o Sistema Brasileiro de Inteligência (SISBIN) e para a Administração Pública Federal de forma mais ampla.

Nesse sentido, encontram-se em desenvolvimento aplicações de comunicação segura, bem como plataformas de processamento e armazenamento de dados baseadas em criptografia robusta. Essa linha de atuação foi apresentada como a principal contribuição do Cepesc no escopo da Política Nacional de Segurança da Informação, com potencial de impacto estruturante para o fortalecimento do ecossistema nacional de proteção da informação.

Reconhecimento da Atuação Institucional

Na sequência, foi registrado o reconhecimento da relevância estratégica do papel desempenhado pela ABIN e pelo Cepesc diante dos desafios emergentes em segurança da informação. Salientou-se o estreitamento progressivo da cooperação institucional e a percepção de que as capacidades técnicas desenvolvidas pelo Centro são fundamentais para o fortalecimento da segurança da informação em toda a Administração Pública Federal, especialmente no contexto de tecnologias emergentes e de ameaças em constante evolução.

Contribuições do GSI à Implementação da Política Nacional de Segurança da Informação

No que se refere às ações alinhadas aos objetivos da Política Nacional de Segurança da Informação, foram destacadas iniciativas diretamente relacionadas ao disposto no inciso II do artigo 4º, que trata da salvaguarda das infraestruturas críticas. Essa atuação ocorre tanto no plano operacional e técnico, por meio das atividades desenvolvidas pelo CETIR-GOV, quanto no plano da articulação institucional conduzida no âmbito do Gabinete de Segurança Institucional.

Ressaltou-se que o conceito de serviços essenciais, incorporado pela Política Nacional de Segurança da Informação, representa avanço conceitual relevante ao ampliar o escopo tradicional das infraestruturas críticas. Essa abordagem passa a contemplar, de forma mais abrangente, setores estratégicos como saúde e justiça, exigindo ações coordenadas para o fortalecimento da resiliência desses serviços frente a riscos e ameaças à segurança da informação.

Outro ponto enfatizado refere-se ao inciso VIII do mesmo artigo, que estabelece como objetivo a construção de uma rede abrangente e colaborativa. Identificou-se nesse dispositivo um alinhamento direto com a atuação da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). À medida que essa rede é fortalecida, ampliada e consolidada, observa-se o fortalecimento sistêmico da segurança da informação no âmbito nacional.

Embora frequentemente caracterizada como um "ecossistema", foi observado que a REGIC opera, na prática, como um sistema estruturado, o qual demanda monitoramento contínuo, coordenação central, elos institucionais robustos e normativos coerentes. O fortalecimento desse sistema, de suas conexões e de suas interações foi apresentado como elemento fundamental para a proteção de todas as informações e serviços que nele circulam.

Concluiu-se que a atuação concentrada nesses dois eixos — a proteção de infraestruturas críticas e serviços essenciais, e o fortalecimento de uma rede colaborativa estruturada constitui a principal contribuição do Gabinete de Segurança Institucional para a implementação dos objetivos da Política Nacional de Segurança da Informação.

Reconhecimento da REGIC como Iniciativa Estruturante

Na sequência, foi destacado o reconhecimento da Rede Federal de Gestão de Incidentes Cibernéticos como uma das iniciativas mais bem-sucedidas no âmbito da Secretaria, ressaltando-se seu elevado potencial de expansão e de fortalecimento do sistema nacional de segurança da informação. Observou-se que a efetividade da REGIC na promoção da segurança da informação e da segurança cibernética já se mostra significativa, consolidando-se como instrumento estruturante para a atuação coordenada dos órgãos públicos frente aos desafios contemporâneos.

Perspectivas Futuras do Núcleo de Segurança e Credenciamento

No que se refere às perspectivas futuras das atividades do Núcleo de Segurança e Credenciamento, foi contextualizada a trajetória institucional da unidade, que possui aproximadamente quinze a dezesseis anos de existência, antecedendo inclusive a promulgação da Lei de Acesso à Informação. Observou-se que a estrutura atual de proteção das informações classificadas no âmbito federal apresenta elevado grau de descentralização, o que tem gerado dificuldades significativas para os órgãos na condução de seus próprios processos de proteção.

Essas dificuldades abrangem, entre outros aspectos, os procedimentos de credenciamento de segurança, a certificação e habilitação de estruturas de segurança física, bem como a habilitação de entidades privadas autorizadas a tratar informações classificadas. Diante desse cenário, foi apresentada a iniciativa de promover maior centralidade à atuação do Núcleo, movimento que tem sido impulsionado, inclusive, por demandas manifestadas por diversos parceiros institucionais.

Nesse contexto, encontra-se em curso a revisão do decreto que regulamenta a Lei de Acesso à Informação no tocante à proteção das informações classificadas. Foi concluída uma primeira rodada de consultas aos órgãos com potencial de contribuição para o processo normativo, iniciando-se, na sequência, a etapa de consolidação das propostas.

Paralelamente à revisão do decreto, estão sendo elaboradas instruções normativas dele decorrentes. Entre elas, foi destacada a norma voltada ao credenciamento de segurança de pessoas, que regulamenta os procedimentos de investigação de segurança. Esse processo foi caracterizado como elemento essencial para a mitigação de riscos associados ao fator humano no tratamento de informações classificadas.

No campo da capacitação e da conscientização, foi anunciada a previsão de lançamento, no início do próximo ano, de um curso nacional aberto ao público, com foco específico na segurança da informação classificada. O curso constituirá requisito para a obtenção de credencial de segurança, ao mesmo tempo em que será disponibilizado a qualquer interessado, inicialmente por meio da plataforma da Escola Nacional de Administração Pública.

Foi mencionada, ainda, a iniciativa de desenvolvimento de um sistema informatizado para apoiar o processo de credenciamento de segurança. Atualmente, a inexistência de uma plataforma unificada resulta na adoção de sistemas e procedimentos distintos por cada órgão, o que compromete a eficiência e a padronização do processo. A proposta consiste na criação de uma solução integrada, capaz de centralizar informações e racionalizar os fluxos de credenciamento.

Outro eixo de atuação refere-se aos estudos sobre esquemas de certificação e acreditação de segurança. No âmbito do Núcleo, essa iniciativa concentra-se na certificação de sistemas e processos que tratam informações classificadas, em consonância com práticas adotadas por outros países. Essa frente dialoga diretamente com a Estratégia Nacional de Cibersegurança, que também prevê a adoção de mecanismos de certificação em escopo mais amplo.

Por fim, foi evidenciada a atuação voltada ao aprimoramento do marco normativo relacionado à chamada segurança industrial, entendida como a proteção de informações públicas sensíveis sob a guarda de entidades privadas. Embora se trate de temática já consolidada em diversos países, observou-se que sua regulamentação no ordenamento jurídico brasileiro ainda se encontra em estágio incipiente.

Nesse sentido, foi mencionada a participação do Núcleo em fórum internacional que reúne países com experiência consolidada na área, com o objetivo de absorver boas práticas e subsidiar o desenvolvimento de um sistema nacional capaz de assegurar proteção mais robusta às informações sensíveis, especialmente aquelas relacionadas ao setor de defesa e a parcerias internacionais estratégicas.

Concluiu-se que as múltiplas frentes em curso avançam de forma gradual e coordenada, orientadas pelo fortalecimento da governança e pelo aperfeiçoamento contínuo do arcabouço normativo que direciona a atuação do Núcleo de Segurança e Credenciamento.

Perspectivas de Auditoria do TCU diante de Tecnologias Emergentes e Riscos Sistêmicos

No âmbito do controle externo, foi esclarecido que a atuação do Tribunal de Contas da União não se concentra na implementação direta da Política Nacional de Segurança da Informação, mas na avaliação de seu cumprimento, de sua efetividade e dos resultados concretos produzidos no contexto da Administração Pública Federal. Essa abordagem reflete a missão institucional do TCU de fiscalizar e avaliar políticas públicas sob a perspectiva de conformidade, desempenho e impacto.

No que se refere à metodologia adotada nos ciclos recentes de auditoria, observou-se o desenvolvimento, ao longo dos últimos três anos, do programa Protege TI, por meio do qual foram realizadas diversas auditorias técnicas em segurança da informação. Esse programa tomou como referência o encadeamento típico de um ataque de ransomware, estruturando auditorias específicas para cada etapa desse tipo de incidente. Paralelamente, foram promovidas ações de disseminação de conhecimento, como eventos e transmissões públicas em plataforma digital.

A experiência acumulada com o programa Protege TI foi avaliada como fundamental para o fortalecimento dos controles básicos de segurança da

informação, funcionando como etapa preparatória para a elevação do nível de maturidade institucional. Superada essa fase inicial, foram identificados novos temas emergentes que demandarão atenção prioritária nos próximos ciclos de auditoria.

Um dos temas ressaltados foi a inteligência artificial. Avaliou-se que, em horizonte próximo, será necessário examinar de forma sistemática o uso de soluções de IA no serviço público, considerando aspectos como governança, segurança dos sistemas, riscos associados à inserção de informações em modelos de linguagem, confidencialidade, vazamento de dados e uso indevido. Reconheceu-se o potencial da inteligência artificial como ferramenta de aumento de produtividade, ao mesmo tempo em que se ressaltou a necessidade de tratamento adequado dos riscos inerentes à sua adoção. Nesse sentido, foi informado que o Tribunal vem investindo na capacitação interna necessária para a auditoria desse tipo de tecnologia.

Outro tema apontado como estratégico refere-se à computação quântica. Observou-se que estudos e discussões internacionais indicam que, em determinado momento, o avanço da computação quântica poderá comprometer os mecanismos criptográficos atualmente utilizados. Certificados digitais e tecnologias de proteção vigentes poderão tornar-se vulneráveis diante de aplicações quânticas efetivas, o que impõe à Administração Pública a necessidade de tratar esse risco de forma sistêmica e antecipatória. Foi mencionada a possibilidade de elaboração de nota técnica sobre o tema, com o objetivo de subsidiar decisões estratégicas.

O terceiro eixo observado diz respeito à governança de terceiros e à cadeia de suprimentos (supply chain). Observou-se que a crescente dependência de fornecedores externos na operação de serviços públicos amplia a superfície de risco, exigindo atenção específica à gestão desses relacionamentos. Casos recentes de ampla repercussão evidenciaram vulnerabilidades associadas ao acesso indevido por terceiros, reforçando a necessidade de supervisão rigorosa. Informou-se que o Tribunal já conduz estudos nessa área e que pretende, em breve, intensificar a fiscalização sobre a forma como os órgãos públicos gerenciam riscos associados a fornecedores, especialmente em serviços considerados críticos.

Concluiu-se que os temas da inteligência artificial, da computação quântica e da governança da cadeia de suprimentos constituem eixos prioritários de observação e atuação do Tribunal de Contas da União para os próximos anos, refletindo a evolução do cenário tecnológico e dos riscos sistêmicos associados à segurança da informação.

Relevância do Tema da Cadeia de Suprimentos no Setor Público

Na sequência, foi registrado o reconhecimento da centralidade do tema da cadeia de suprimentos nos debates contemporâneos da Administração Pública. A recorrência dessa temática reforça sua relevância estratégica, tanto para a formulação de políticas de segurança da informação quanto para a atuação fiscalizatória do Tribunal de Contas da União.

Capacitação, Conscientização e Diagnóstico Institucional em Segurança da Informação

Foram apresentados dois pontos considerados estratégicos para o fortalecimento da implementação da Política Nacional de Segurança da Informação, com ênfase na formação de pessoas e no aprimoramento da capacidade institucional da Administração Pública Federal.

O primeiro ponto refere-se à formação e capacitação. Foi informado que o Gabinete de Segurança Institucional, por meio dos Departamentos de Segurança da

Informação e de Segurança Cibernética, vem desenvolvendo iniciativas estruturadas de capacitação. Entre elas, mencionou-se a criação de cursos voltados tanto às boas práticas de segurança da informação quanto à formação específica do gestor de segurança da informação, alinhada à nova Política Nacional de Segurança da Informação. Soma-se a esse esforço o curso nacional sobre segurança da informação classificada, a ser ofertado por meio da Escola Nacional de Administração Pública, conforme anteriormente apresentado.

No âmbito da governança institucional, foi informada a criação de um subcomitê dedicado à capacitação e à conscientização no interior do Comitê Gestor de Segurança da Informação, com foco específico na Administração Pública Federal. Ademais, no Comitê Nacional de Cibersegurança, encontra-se em funcionamento grupo de trabalho voltado à educação cibernética, cujo escopo abrange tanto os órgãos públicos quanto o público externo. Esse conjunto de iniciativas evidencia que a educação e a conscientização foram reconhecidas como pilares centrais para a consolidação da segurança da informação e da segurança cibernética.

O segundo ponto apresentado diz respeito ao Autodiagnóstico da Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal. Informou-se que o instrumento foi encaminhado recentemente aos órgãos e que sua resposta é considerada fundamental para a construção de uma visão situacional abrangente sobre o estágio de maturidade da segurança da informação no setor público federal. A partir desse diagnóstico, será possível formular ações de capacitação, ajustes normativos e iniciativas de cooperação mais aderentes à realidade institucional dos órgãos.

Por fim, foi reforçada a importância da participação ativa dos gestores de segurança da informação no preenchimento do autodiagnóstico, especialmente considerando a presença expressiva desses profissionais no webinário. Tal engajamento foi apontado como condição essencial para subsidiar decisões estratégicas e orientar o aprimoramento do ecossistema nacional de segurança da informação.