TECNOLOGIA DA INFORMAÇÃO

LEVANTAMENTO SOBRE SEGINFO E SEGCIBER DA APF

O QUE O TCU FISCALIZOU

Em virtude do processo de transformação digital da Administração Pública federal e consequente digitalização dos serviços públicos, o Tribunal de Contas da União (TCU), entre 27/1 e 12/6/2020, realizou auditoria para entender a macroestrutura de governança e gestão de segurança da informação (SegInfo) e segurança cibernética (SegCiber) da Administração (legislação, políticas, normativos, atores, papéis e responsabilidades), levantar ações em andamento, consolidar informações nessas áreas e identificar principais riscos e vulnerabilidades envolvidos, de modo a sugerir estratégia para que o TCU atue na fiscalização e no acompanhamento da segurança dessas informações digitais.

PRINCIPAIS FUNÇÕES E ÓRGÃOS IDENTIFICADOS

- **SegInfo, SegCiber e inteligência cibernética**: Gabinete de Segurança Institucional da Presidência da República (GSI/PR)
- **Defesa cibernética (DefCiber)**: Ministério da Defesa (MD)
- **Investigação de crimes cibernéticos**: Ministério da Justiça e Segurança Pública (MJSP)
- **Auxiliares**: Secretaria de Governo Digital do Ministério da Economia (SGD/ME), Controladoria-Geral da União (CGU), Instituto Nacional de Tecnologia da Informação (ITI) e Comitê Gestor da Internet (CGI.br).

O QUE O TCU ENCONTROU

De modo geral, os órgãos estruturantes estão cientes da necessidade de se elevar a maturidade da Administração Pública federal em SegInfo e SegCiber, já tendo sido editados instrumentos legais com esse propósito, a exemplo da Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e dos Decretos 9.637/2018 – Política Nacional de Segurança da Informação (PNSI) e 10.222/2020 – Estratégia Nacional de Segurança Cibernética (E-Ciber).

A macroestrutura nacional responsável pela governança e gestão dessas áreas, no entanto, apresenta carências: i) DefCiber: o investimento está aquém da sua importância estratégica para o país; ii) SegInfo e SegCiber: o principal órgão (GSI/PR) e o arcabouço normativo atual têm alcance restrito ao Poder Executivo federal, inexistindo órgão ou agência com autoridade ampla ou lei que regule esses temas em todo o território; iii) a capacidade de resposta a incidentes de SegInfo dos órgãos individualmente e da rede de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIRs) é insuficiente.

Sob o prisma normativo, as grandes transformações tecnológicas em curso na Administração Pública federal têm contemplado aspectos, requisitos e riscos de SegInfo e SegCiber, destacando-se o papel da SGD/ME, órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo federal (Sisp).

Faz-se necessário reforçar os papéis da CGU – responsável por auditar as ações de responsabilidade dos órgãos; do ITI – Autoridade Certificadora Raiz da ICP-Brasil; e dos órgãos e estruturas que combatem crimes cibernéticos, a exemplo do Laboratório de Inteligência Cibernética do Ministério da Justiça e Segurança Pública (CiberLab/MJSP) e do Serviço de Repressão a Crimes Cibernéticos do Departamento de Polícia Federal (SRCC/DPF), que prestam serviços de inteligência cibernética e desenvolvem soluções criptográficas de Estado – Agência Brasileira de Inteligência (Abin), bem como que atuam na prevenção, na resposta e no tratamento a incidentes de SegInfo e SegCiber – Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), Centro de Estudos, Resposta e Tratamento de

Incidentes de Segurança no Brasil (CERT.br) e Centro de Operações de Segurança (Security Operations Center) do Serviço Federal de Processamento de Dados (SOC/Serpro).

PROPOSTA DE ENCAMINHAMENTO

O levantamento compilou os principais aspectos (legislação, normativos, estruturas, orçamento, papéis, responsabilidades, iniciativas) envolvidos na governança e gestão da SegInfo e SegCiber da Administração Pública federal e, com base nos diagnósticos citados, sugeriu estratégia de atuação para que o TCU, ao longo dos próximos anos, acompanhe e induza a boa gestão dessas áreas. Ademais, gerou diversos produtos, como o painel de consulta aos dados do levantamento integrado de governança, o infográfico da estratégia, o quadro referencial normativo e o relatório de *feedback* às ETIRs.

A referida estratégia, já aprovada, prevê a realização de ações e iniciativas específicas para ajudar a melhorar o panorama atual, incluindo auditoria na implementação da LGPD e proposta de acompanhamento ágil de controles críticos de SegCiber, considerada essencial para conscientizar os órgãos da Administração Pública federal como um todo quanto à importância das questões de SegInfo e SegCiber.

PRÓXIMOS PASSOS

A partir da execução dessa estratégia, pretende-se fomentar uma cultura de SegInfo nos órgãos e nas entidades da Administração Pública federal, de modo que mantenham processos bem definidos de governança e gestão de SegInfo e SegCiber, contribuindo, assim, para elevar a segurança, resiliência e capacitação dos quadros de pessoal especializado das organizações públicas brasileiras e minimizar os riscos e possíveis impactos de ataques cibernéticos e incidentes de segurança da informação.

DADOS DA DELIBERAÇÃO

Acórdão: 4035/2020-TCU-Plenário
Data da sessão: 08/12/2020
Relator: Ministro Vital do Rêgo
TC: 001.873/2020-2
Unidade Técnica Responsável: Secretaria de Fiscalização de Tecnologia da Informação (Sefti)