27 de novembro de 2022

3ª Entrega

Transformar a Segurança da Informação e a Segurança Cibernética na Administração Pública Federal

Uma nova perspectiva para a proteção da informação e para a garantia da qualidade e da confiança na prestação de serviços públicos

Líder:
Larissa Maria Melo Ambrozio de Assis

Equipe:
Alfredo Tiburcio Paiva Frota
Ana Maria Bezerra Pina
Diego Braga Serpa
Ériko Tadashi Sedoguchi
Evaldo Matheus
Pedro Jorge Sucena Silva
Virgínia de Melo Dantas Trinks

LIDERAGOV
Desenvolvendo talentos para transformar o Brasil

1 O problema da Segurança da Informação e da Segurança Cibernética na Administração Publica Federal

No Brasil, a responsabilidade de coordenação e realização de ações destinadas à gestão de incidentes computacionais na Administração Pública Federal (APF) está a cargo do Gabinete de Segurança Institucional (GSI) por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo [1]. Até outubro de 2022, o Centro registrou mais de 15 mil notificações, a ocorrência de mais de três mil incidentes e a identificação de quase três mil vulnerabilidades.

Os incidentes registrados pelo CTIR Gov têm impactos de grave potencial sobre os dados pessoais dos cidadãos brasileiros e a continuidade dos serviços públicos. Tais impactos evidenciam um problema público relevante de necessidade de proteção da segurança da informação (SegInfo) e da segurança cibernética (SegCiber) na Administração Pública Federal (APF)[2].

É possível entender a dimensão desses impactos a partir do ataque à infraestrutura do Ministério da Saúde (MS) durante a pandemia de COVID-19. Em 10 de dezembro de 2021, o MS informou que falhas de SegInfo/SegCiber comprometeram seus serviços digitais. O Portal para divulgação de dados da COVID-19, o e-SUS Notifica[3], o SI-PNI[4] e o ConecteSUS[5] foram impactados.

Além da falta de informações públicas oficiais nacionais sobre o avanço da pandemia no Brasil, o ataque deixou milhares de brasileiros com dificuldades de acessar seus comprovantes de vacinação digital contra a COVID-19, cuja apresentação era obrigatória para viagens ao exterior e para entrar em estabelecimentos comerciais em alguns dos estados da federação. De acordo com a perícia, o acesso à nuvem pelos hackers ocorreu pelo uso de um perfil legítimo de administrador, o que facilitou o ataque.

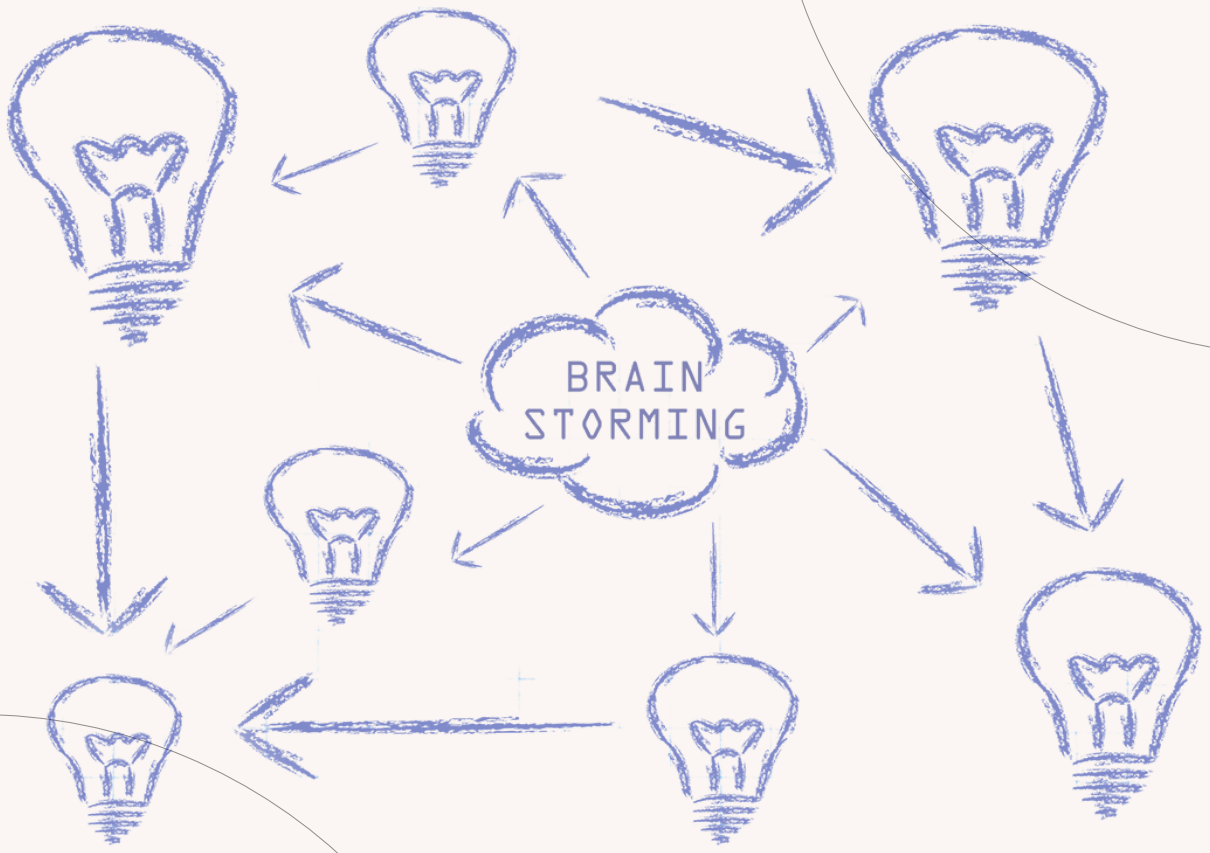
Os cidadãos brasileiros são, portanto, diretamente impactados por incidentes SegInfo/SegCiber nos órgãos da APF. Conforme a Estratégia Nacional de Segurança Cibernética (E-Ciber) (Decreto nº 10.222/2020), o vazamento sistêmico de dados pessoais e de informações sensíveis reduz a confiabilidade do serviço público brasileiro e propaga transtornos e prejuízos incalculáveis para os cidadãos, os quais podem vir a ser alvos de fraude com a exposição de seus dados.

Corroborando essas constatações, auditorias recentes do Tribunal de Contas da União (TCU) destacam uma série de impactos e prejuízos para a sociedade resultantes das falhas de SegInfo/SegCiber nas organizações públicas, tais como indisponibilidade de serviços públicos, vazamento de informações pessoais dos cidadãos e estratégicas ao desenvolvimento do país, perda da integridade dos dados públicos e pessoais, violação do direito à privacidade dos cidadãos e perdas financeiras[6].

O Tribunal incluiu a SegInfo/SegCiber em sua Lista de Alto Risco da Administração Pública, na consideração de que o "processo de transformação digital da Administração, ao mesmo tempo em que disponibilizou e otimizou acesso a serviços públicos, tornou o governo e a sociedade brasileira mais dependentes de soluções tecnológicas".[7]. Tal é a relevância desse ponto que a Organização de Cooperação e de Desenvolvimento Econômico (OCDE) incluiu entre as metas para a acessão do Brasil a eficiência e a confiabilidade da gestão de dados no serviço público[8].

Em fevereiro de 2022, o Congresso Nacional promulgou a Emenda Constitucional n.º 115, reconhecendo a proteção dos dados pessoais, inclusive nos meios digitais, como direito fundamental, alocado no artigo 5º da Constituição Federal de 1988. Proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive em meios digitais, é uma obrigação do Estado brasileiro para com seus cidadãos.

Desde o início deste século, vários organismos internacionais vêm apontando, cada vez mais, para a segurança da informação como uma necessidade premente no contexto da revolução digital. As recomendações da OCDE são vanguardistas na questão e já apontam para a necessidade de investimento no setor desde a edição das Diretrizes da OCDE para a Segurança de Sistemas e Redes de Informação em 2002. Em 2015, a Organização reconheceu a necessidade de evoluir da inicial necessidade de segurança de sistemas de informação para uma gestão de riscos de segurança digital com a edição da Recomendação sobre Gestão de Riscos de Segurança Digital para Prosperidade Econômica e Social.



Confira os apontamentos do processo de reflexão no Anexo I

Com base nessas evidências, apresentamos o problema público da necessidade de proteção da segurança da informação e da segurança cibernética na APF, de modo a proteger os dados e a privacidade dos cidadãos, a proteger informações relevantes ao interesse do estado, a garantir qualidade e constância nas entregas do Estado e no acesso à informação, evitando quaisquer prejuízos que ataques cibernéticos possam gerar.

2 Brasil, liderança mundial em SegInfo e SegCiber: um futuro desejado

O Brasil tem obtido avanços consideráveis em índices de governo digital e segurança cibernética. Considerando essa tendência positiva, é possível projetar um futuro desejado em que, com a adoção de planos estratégicos em relação às principais causas do problema, o país esteja entre os países mais destacados em SegInfo/SegCiber no mundo.

Entre 2021 e 2022, o Brasil subiu cinco posições no ranking GovTech Maturity Index do Banco Mundial, que mede a maturidade em governo digital de 198 economias globais. Foi o maior avanço entre todos os países considerados. O Brasil agora ocupa a vice-liderança da lista, atrás apenas da Coreia do Sul. O índice é composto por quatro elementos: Índice de Sistemas Governamentais Centrais, Índice de Prestação de Serviços Públicos, Índice de Engajamento do Cidadão e Índice de Habilitadores GovTech[9]. Em relação à SegCiber, o Brasil saltou da 71ª para a 18ª posição dos 194 países analisados do Índice de SegCiber 2020 da União Internacional de Telecomunicações (UIT)[10].

Assim, vislumbramos um futuro em que, enfrentando-se de forma coordenada o problema da SegInfo/SegCiber na Administração Pública federal brasileira, possamos mitigar em grande escala o impacto de incidentes e vulnerabilidades, protegendo dados pessoais e serviços públicos e fazendo do Brasil um integrante do “top” mundial nessas áreas.

3 Capacidade do Brasil em SegInfo e SegCiber e Causas do Problema

As debilidades da SegInfo/SegCiber na APF brasileira têm causas de ordem normativa, de governança, de gestão, de tecnologia e de cultura e capacitação. Essa última causa se destaca, por um lado, por ser uma das condicionantes para superar as demais e, por outro, por ser diretamente ligada à maior parte dos incidentes segundo os estudos mais atuais sobre o tema.

Na revisão da capacidade de SegCiber do Brasil promovida pelo Centro Global de Capacidade de Segurança Cibernética (GCSCC) da Universidade de Oxford em parceria com a Organização dos Estados Americanos (OEA), apontam-se cinco dimensões de avaliação: normas, organizações e tecnologias; política e estratégia de segurança cibernética; cultura cibernética e sociedade; educação, treinamento e competências em segurança cibernética; e estruturas jurídicas e regulamentares.[11]. Cada uma das dimensões está dividida em fatores com relação aos quais a maturidade foi avaliada, conforme a figura 1 a seguir.

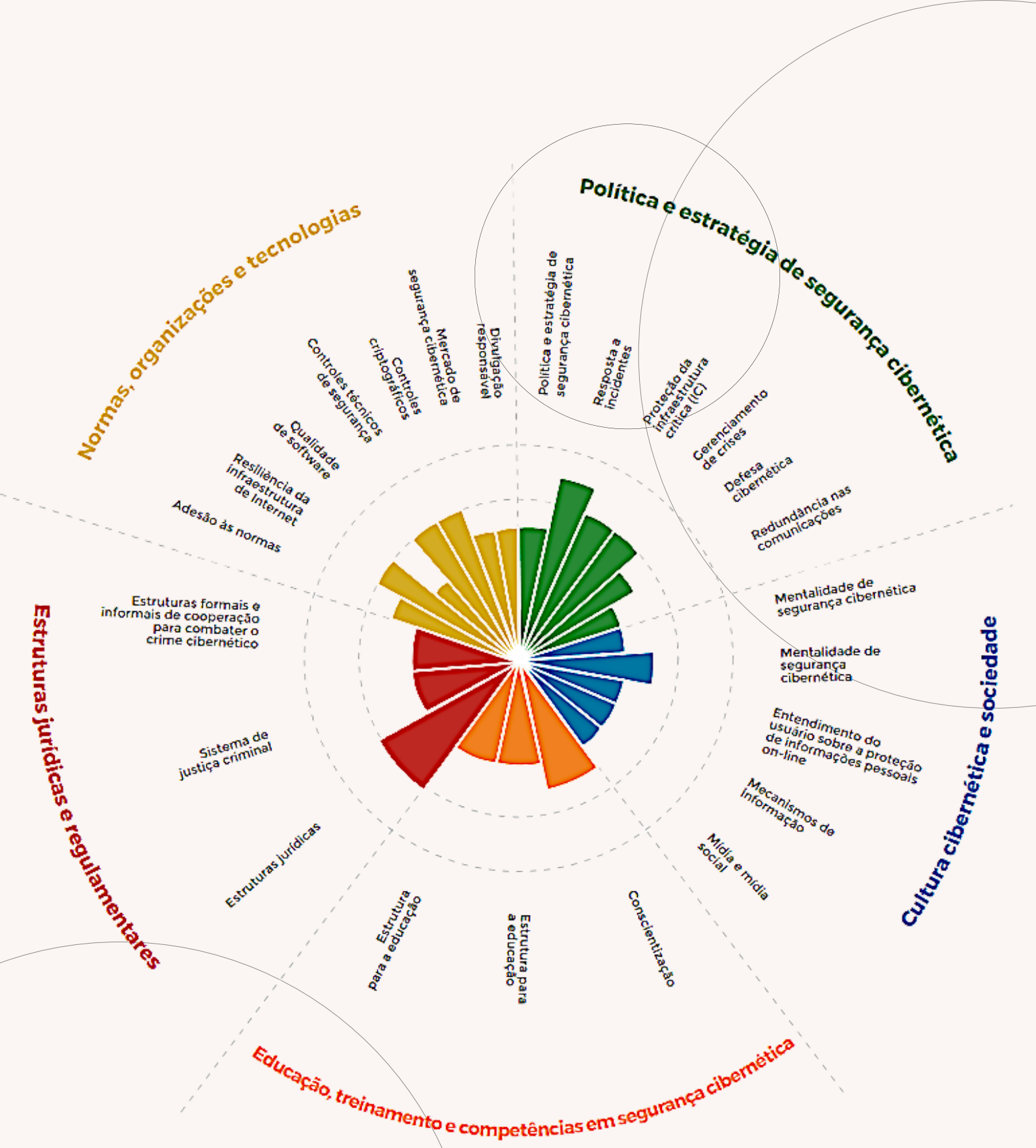


Fig. 1. Representação geral da capacidade de segurança cibernética no Brasil
(Fonte: OEA. Revisão da Capacidade de Cibersegurança da República Federativa do Brasil, 2020)

Abordaremos cada uma dessas dimensões nos aspectos que dizem respeito à APF.

Política e Estratégia de SegCiber

Nessa dimensão, o Brasil conta com uma Política Nacional de Segurança da Informação (Decreto n.º 9.637/2018) e com uma Estratégia Nacional de Segurança Cibernética (Decreto 10.222/2020). A revisão aponta que seria necessário, para melhor implementá-las:

- promover o compartilhamento de inteligência de ameaças entre as Equipes de Resposta a Incidentes de Segurança Cibernética (Cert);
- criar um mecanismo de identificação do nível de maturidade de governança de TI;
- transformar as lições aprendidas em incidentes cibernéticos em políticas estruturais; e
- melhorar a governança em SegCiber.

Reforçando esse último ponto, o TCU considera que "a macroestrutura nacional responsável pela governança e gestão de Segurança da Informação e de Segurança Cibernética, apesar de atuante, não é adequada"[12].

Normas, Organizações e Tecnologias

Na dimensão "normas, organizações e tecnologias", o GCSCC destacou positivamente:

- a existência de normas infralegais de SegCiber na APF;
- a auditoria sobre o cumprimento dessas normas;
- a adoção de controles técnicos; e
- a gestão de vulnerabilidades.

A infraestrutura de tecnologia da informação da APF também apresentaria resiliência.

O TCU, por outro lado, aponta problemas em relação às políticas de backups e de gestão de incidentes[13].

Estruturas jurídicas e regulamentares

Com relação às "estruturas jurídicas e regulamentares", o GCSCC considerou que o Brasil, à época do levantamento (2018-2019), carecia de uma estrutura regulamentar abrangente que considerasse expressamente a segurança cibernética. Não obstante, houve avanços consideráveis em relação à SegCiber e à proteção de dados pessoais recentemente.

Na vertente dos direitos e garantias fundamentais, a já mencionada Emenda Constitucional nº 115, de 10 de fevereiro de 2022, inseriu a proteção de dados pessoais no rol de direitos do art. 5.º da Constituição (inciso LXXIX), ao lado da inviolabilidade da intimidade (art. 5º, X) e das comunicações (art. 5º, XII) e do acesso à informação (art. 5º, XIV e XXXIII), todos direitos derivados da dignidade da pessoa humana (art 1º, III).

No plano infraconstitucional, destacam-se três leis:

- a Lei nº 12.965/2014, o Marco Civil da Internet, resultado de um processo de consulta que envolveu múltiplos atores, estabelece princípios e garantias para o uso da rede mundial de computadores no país, a exemplo da proteção da privacidade (art. 3º, II) e dos dados pessoais (art. 3º, III);
- a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Estabelece, portanto, hipóteses em que poderá ocorrer o tratamento de dados pessoais, bem como as limitações relativas a esta atividade, disciplinando segurança, sigilo de dados, boas práticas e governança; e
- a Lei nº 12.527/2011, denominada Lei de Acesso à Informação (LAI), dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º da LAI, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

Essas leis estruturam um microssistema de tratamento de dados que conjuga a legítima proteção de informações sensíveis à publicidade que é o vetor de qualquer regime democrático, o que se traduz em enormes desafios de governança frente à intensa digitalização dos serviços públicos brasileiros, à qual já fizemos referência.

Como novidade nesse contexto, a Lei nº 14.460, de 25 de outubro de 2022, transformou a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial. A ANPD é responsável por proteger os direitos fundamentais da liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º), atuando no estabelecimento de padrões mínimos para a adoção de medidas de segurança, técnicas de proteção de dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de vulneração de dados [14].

Dado seu escopo de atuação, a transformação da ANPD em autarquia de natureza especial, com autonomia técnica e decisória, é um movimento de fortalecimento da proteção de dados pessoais no Brasil.

Cultura de SegCiber e Sociedade

Já sobre "cultura de segurança cibernética e sociedade", a revisão aponta que a maturidade varia entre as organizações da APF, a qual ainda carece de um mecanismo que avalie esse aspecto.

No geral, a "sociedade como um todo ainda carece de uma mentalidade de segurança cibernética; ainda que estejam cientes dos riscos [...] os usuários, muitas vezes, deixam de agir de maneira adequada [...]" [15].

A revisão também considerou que, à época, a proteção de dados pessoais também carecia de ações concretas.

Educação, treinamento e competências de SegCiber

Por fim, na dimensão "educação, treinamento e competências de segurança cibernética", a revisão apontou a carência de um programa nacional de conscientização sobre SegCiber, mencionando também que os líderes das organizações têm formação deficitária na área.

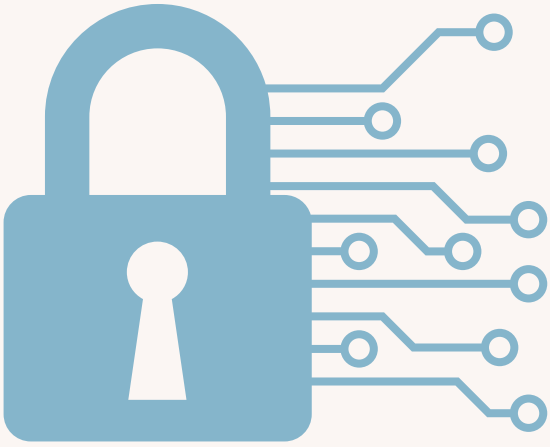
Os atores da APF que participaram do levantamento informaram a necessidade de aprimorar a educação em SegCiber nas escolas e universidades e de formar profissionais na área. Faltaria um currículo nacional, bem como dotação orçamentária específica para a formação em SegCiber. A maioria dos profissionais do setor público dependeria de certificação estrangeira.

Causas de maior impacto: cultura e capacitação

As dimensões “cultura cibernética e sociedade” e “educação, treinamento e competências em segurança cibernética” concentram grande atraso de desenvolvimento e possuem impactos para o alcance dos outros quesitos. Por exemplo, sem mentalidade de SegInfo, as políticas, estruturas normativas e de regulamentação não são materializadas em processos.

De fato, outros estudos sobre a capacidade de segurança cibernética no Brasil indicam deficiências em cultura e capacitação em SegInfo/SegCiber. Especialistas da área afirmam que 70% dos incidentes aconteceriam devido à negligência humana e que o comportamento dos profissionais de segurança é a causa de 43% das violações de dados [16]. A conclusão é de que o fomento da cultura de segurança da informação é um componente essencial para incorporar comportamentos de conformidade com a política de SegInfo nas organizações. Esse processo é complexo, por envolver múltiplos fatores, tais como educação, atores humanos e tecnologia, todos necessários para gerenciar um modelo de segurança da informação[17].

Um dos levantamentos realizados pelo TCU também aponta para a necessidade de reforço no que tange ao “aspecto humano” da SegInfo e da proteção cibernética[18]. O TCU constata que práticas de conscientização e treinamento da APF são deficientes no que respeita aos riscos e às boas práticas de SegCiber nas organizações públicas federais. Das 377 organizações públicas questionadas, 219 (58%) responderam que não mantinham um programa de conscientização em segurança. Partindo dessas constatações em relação ao impacto da cultura e da capacitação na situação da APF em SegInfo/SegCiber, realizamos entrevistas semi-estruturadas com colaboradores de organizações da APF para aprofundar esses aspectos.



Os seguintes atores foram entrevistados:

- A Divisão de Tecnologia da Informação da Secretaria-Geral da Presidência da República (Ditec/SG/PR);
- A Secretaria de Fiscalização de Tecnologia da Informação do TCU (Sefti/TCU);
- O Departamento de Governança de Dados e Informações da Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG) do Ministério da Economia (DGDI/SGD/SEDGG/ME);
- O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Agência Brasileira de Inteligência (CTIR/Abin); e
- Um consultor contratado pelo Ministério da Saúde.

Ditec/SG/PR: "[...] as campanhas de conscientização e capacitação acabam atingindo apenas os escalões mais baixos. Na verdade, as autoridades precisam ser atingidas para que sigam as melhores práticas e deem um patrocínio mais resoluto às iniciativas. É como dizem: 'a palavra convence, o exemplo arrasta'".

As entrevistas mantiveram o foco em entender a participação do "fator humano" nas causas e nas possíveis soluções para os incidentes de SegInfo/SegCiber. A íntegra das entrevistas está reproduzida no Anexo II.

Confirmando os dados acima, a maioria dos entrevistados avaliou que o despreparo do usuário, por falta de uma cultura de segurança desenvolvida, é o fator principal nos incidentes cibernéticos enfrentados pela APF.

Por outro lado, a maior parte dos entrevistados avalia que há um tendência de melhoria em SegInfo/SegCiber na APF em médio prazo, tendo em vista tanto pressões externas, devido ao aumento do número de ataques, quanto circunstâncias internas, como a edição de novas normas e a crescente institucionalização de processos de segurança.

A necessidade de capacitação em SegInfo/SegCiber foi o desencadeamento lógico das entrevistas, como proposta de solução para o problema. Os entrevistados sugeriram que os treinamentos devem ser menos teóricos e mais voltados a situações rotineiras dos usuários para que possam ter a efetividade necessária. Apontaram que as ações de sensibilização devem apresentar propósitos claros e estar orientadas por um plano bem construído e personalizado a cada setor.

Por fim, a maioria dos entrevistados apontou para a necessidade de desenvolver o envolvimento da alta administração e das lideranças nas iniciativas de SegInfo/SegCiber. Segundo afirmaram, o patrocínio efetivo aliado ao monitoramento de qualidade são essenciais para uma política de segurança efetiva. Houve ainda destaque para a carência de conhecimento sobre a temática por parte dos gestores.

Nesse sentido, estudos vêm enfatizando a necessidade de serem incluídas na formação de líderes, nos setores público e privado, habilidades para adotar uma postura de segurança e desenvolver estratégias e políticas abrangentes para lidar com riscos cibernéticos em constante evolução. A inclusão da SegInfo/SegCiber, por intermédio de suas competências básicas, é preconizada, por exemplo, nos cursos de graduação e pós-graduação e nos programas de capacitação continuada para profissionais dos setores privado e público [19]. Essa formação não deve se restringir ao ensino de "o que" e "como" fazer, mas, sobretudo, deve explicar as razões ("por que") por trás de cada uma das questões de segurança abordadas e mostrar-lhes os objetivos da SegInfo e os impactos potenciais, positivos e negativos, dos seus diferentes comportamentos e condutas sobre a organização [20].

Entendemos, portanto, que as deficiências em termos de cultura e capacitação em SegInfo/SegCiber são as causas de maior impacto em relação ao número de incidentes na APF, bem como por ser uma condição para avançar em maturidade nas demais dimensões.

Por que + cultura e capacitação?

DEGSI/SGD/SEDGGD/ME: "As ações de capacitação têm de ter um norte e uma metodologia de trabalho bem construída, centrada no "mão na massa". É necessário colocar recursos nessa metodologia. Ações descoordenadas ou pontuais não são efetivas".

Sefti/TCU: "[...] não há ações em capacitação e cultura que sejam condizentes a essa necessidade. A oferta de cursos em SegInfo/SegCiber é insuficiente. A adoção em massa do teletrabalho durante a pandemia, por exemplo, veio desacompanhada de preocupações com segurança. Os sistemas informatizados poderiam ser utilizados nesse sentido, como uma forma de induzir o servidor a trabalhar com mais segurança, uma forma de orientar o comportamento. Se o sistema limitar o servidor a opções seguras, a chance de falhas pode ser severamente reduzida".

CTIR/Abin/GSI/PR: "[...] o fator cultura e capacitação é uma necessidade constante, eterna e cíclica. Quanto maior a organização, mais é um fator problemático. Principalmente para organizações que custodiam informações sensíveis. [...] Os servidores de outros órgãos, em geral, não têm consciência sobre a sensibilidade das informações com que lidam. [...] Os dados podem ser estratégicos para o país; mesmo que não o sejam a credibilidade do governo sempre será afetada. Por isso, é necessária a formação e a especialização dos gestores; os gestores têm de ser profissionalizados para a atuação no serviço público".

Ditec/SG/PR: "[...] as campanhas de conscientização e capacitação acabam atingindo apenas os escalões mais baixos. Na verdade, as autoridades precisam ser atingidas para que sigam as melhores práticas e deem um patrocínio mais resoluto às iniciativas. É como dizem: 'a palavra convence, o exemplo arrasta'".

4 Desafios para SegInfo e SegCiber

Com base nas entrevistas realizadas, pesquisa bibliográfica e consultas aos levantamentos de órgãos competentes, e tomando como foco a cultura e a capacitação em SegInfo/SegCiber, percebe-se que o país precisa superar sérias deficiências, tais como:

- Falta de envolvimento, sensibilização e patrocínio das autoridades;
- Campanhas de conscientização inexistentes ou massificadas, não ligadas à atividade cotidiana dos atingidos;
- Desconhecimento e falta de uma mentalidade de segurança;
- Falta de propósitos claros nas atividades de capacitação;
- A ausência de uma linguagem compartilhada para se referir às questões de segurança cibernética/digital na sociedade;
- A associação de segurança cibernética com assuntos, responsabilidades e competências de instituições militares;
- O desconhecimento de riscos específicos e compartilhados entre setores;
- A ausência de mecanismos para o compartilhamento de informações sobre riscos/ameaças e conhecimento em segurança entre setores; e
- A existência de diferentes níveis de maturidade da sociedade em segurança cibernética.

Para superar esses desafios há que se investir, de forma mais efetiva, no desenvolvimento da capacitação e da cultura de SegInfo/SegCiber. Treinamentos e ações de conscientização, se bem aplicadas, podem contribuir para reduzir as deficiências anteriormente mencionadas, proporcionando, por exemplo, a utilização de uma linguagem comum, a consciência acerca dos riscos e ameaças existentes, clareza sobre as responsabilidades de cada agente/ator, entre outros benefícios.

Assim como programas contínuos e permanentes de conscientização e treinamento em segurança devem desenvolver nos servidores habilidades para adotarem comportamentos e procedimentos mais seguros na realização das suas tarefas e rotinas de trabalho cotidianas, os gestores e a alta administração dos órgãos também devem ser formados e treinados, de modo a serem capazes de reconhecer suas funções e responsabilidades específicas relacionadas à SegInfo/SegCiber.

Nesse sentido, ressalta-se a necessidade de se desenvolver lideranças em SegInfo/SegCiber, não circunscritos à área de TI nos órgãos públicos. Essas lideranças têm responsabilidades no desenvolvimento de políticas de segurança, formulação de estratégias, aplicação, adoção e comunicação, entre outras ações, em prol da cultura de segurança institucional.

Os funcionários geralmente consideram que a segurança da informação é responsabilidade da equipe de tecnologia da informação e não se identificam como parte integrante da corrente de segurança da informação. A compreensão do "por que" proteger é considerada, assim, afeta a um grupo restrito de funcionários. Para mudar essa visão, as organizações devem cultivar uma boa cultura de segurança, e a alta administração deve desempenhar seu papel.

Vale observar que muitas vezes as políticas e os planos de comunicação e de capacitação são mais focados em outras técnicas de dissuasão e receio da punição. Os estudos indicam, todavia, que as punições e a dissuasão por incentivos nem sempre são a melhor maneira de mitigar o descumprimento de normativos de segurança. A relação entre teoria e a prática pode ser aprimorada a partir da socialização dos funcionários sobre comportamentos de proteção[21].

Uma gestão de ação positiva – consciente e capacitada – da alta administração, somada ao comportamento coletivo, são fatores importantes para melhorar a segurança e formar uma boa cultura de SegInfo/SegCiber, bem como constituem as bases da proposta de solução diferenciada para o problema apresentado.

5 Modelos de Solução

Buscando soluções para as deficiências em termos de cultura e capacitação em SegInfo/SegCiber, encontramos iniciativas de organismos internacionais, do setor público estrangeiro, do Estado brasileiro e da própria APF.

No plano internacional, há o padrão IEC 62443, da Comissão Internacional Eletrotécnica, que não se limita ao setor de tecnologia, pois também considera a mitigação de ameaças cibernéticas em relação a processos, colaboradores e contramedidas. Outra referência é o NIST SP800-12, do Instituto Nacional de Padrões e Tecnologias dos Estados Unidos (NIST), que aborda os princípios básicos da segurança cibernética e foi desenvolvido para ser usado em agências governamentais.

No Estado brasileiro, como já mencionado, o TCU tem desenvolvido uma iniciativa de avaliação da maturidade das organizações da APF em SegInfo/SegCiber, divulgando análise confiável da macroestrutura nacional responsável pela governança e gestão de Segurança da Informação e de Segurança Cibernética da APF[22].

Adicionalmente, a própria APF mantém iniciativas na área. O Programa Nacional de Proteção do Conhecimento Sensível (PNPC), de responsabilidade da Agência Brasileira de Inteligência (Abin), é uma consultoria de segurança com foco na prevenção de espionagem, sabotagem e vazamento de informações. Desde 1997, busca promover a proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas. O PNPC atua na sensibilização de pessoas, na identificação de ameaças e vulnerabilidades nos sistemas de proteção da instituição e na apresentação de recomendações para redução de risco de incidentes.

Já o Programa de Privacidade e Segurança da Informação (PPSI) da SGD possui uma série de ações de adequação nas áreas de privacidade e segurança da informação, desenvolvidas dentro do escopo de múltiplas disciplinas de governança, todas com o fim de aumentar o grau de maturidade e de resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo federal[23]. O programa está estruturado em cinco torres. A torre de pessoas integra diversas ações de capacitação contínuas e esporádicas, tais como a 1ª Semana de Segurança Cibernética (CyberGov) e a 1ª Semana de Proteção de Dados Pessoais. O foco seria criar um centro de excelência, tomando o exemplo do NIST. O programa já publicou 18 guias sobre privacidade e SegInfo e desenvolveu um framework próprio de avaliação de maturidade para a APF (framework de privacidade e segurança da informação).

A continuidade do problema, diante dessas iniciativas, mostra a necessidade de ampliar a abordagem, atuando sobre os desafios apontados na seção anterior.

Atores envolvidos

O problema é transversal a todos os setores da APF e, portanto, necessita de uma abordagem ampla e agregada de diversos órgãos de modo que possa obter resultados tempestivos e qualitativos frente à dimensão gigantesca do problema. Sugere-se que os órgãos responsáveis pelo governo digital se unam tanto a órgãos de controle e monitoramento, como a órgãos de educação, tudo sob a coordenação do GSI, encarregado legal do tema, e da SGD, órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal (Sisp). Com isso, esperamos criar uma abordagem prática e resolutiva que envolva desde programas de comunicação dos normativos e ferramentas existentes até projetos educativos para lideranças da APF.

6 Plano Estratégico de Ação: intencionalidade na transformação da cultura de SegInfo e SegCiber

Em linha com as evidências e as constatações registradas, propomos um plano estratégico com foco na transformação da cultura de SegInfo/SegCiber na APF, com diferenciais na orientação prática ("mão na massa"), no envolvimento e na formação das lideranças.

O foco da mudança é a conscientização e o treinamento sobre riscos de segurança. Destaca-se essa estratégia, em especial, porque a superação das fragilidades dependem do aprimoramento da cultura de SegInfo/SegCiber e da capacitação nessa área.

A motivação do plano é contrapor o aumento do número de incidentes de segurança na APF e os impactos negativos que estes acarretam. Como visto na seção 1, tais incidentes podem afetar a continuidade dos serviços públicos e representar prejuízos à coletividade também na vertente do vazamento de dados pessoais. Isso deve ser combatido pela APF, inclusive diante da crise contemporânea de legitimidade do Estado.

Além disso, a causa principal desses incidentes é o "fator humano", ou seja, as deficiências em cultura e capacitação em SegInfo/SegCiber, como vimos nas seções 3 e 4.

O plano envolve os seguintes atores, a partir das considerações da seção 5:

- GSI, encarregado legal do tema;
- SGD, órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo federal (Sisp), por meio do Programa de Privacidade e Segurança da Informação (PPSI);
- ANPD, como colaboradora na disponibilização de materiais e conteúdo e em ações de capacitação;
- ABIN, por meio do Programa Nacional de Proteção ao Conhecimento Sensível (PNPC) e pela Escola de Inteligência (Esint);
- Escola Nacional de Administração Pública (Enap), como parceira, provedora e indutora de ações de capacitação em SegInfo/SegCiber;
- TCU, pela função de auditoria da SegInfo/SegCiber na APF; e
- Assessorias de Comunicação (Ascom) dos órgãos, pela função de divulgação dos materiais em eventos setoriais e pela promoção de eventos anuais de conscientização.

Indicamos como público-alvo 10 órgãos anualmente selecionados pela SGD, órgão central do Sisp, como prioritários, com base no Framework de Privacidade e Segurança da Informação. Dessa maneira, busca-se mitigar o risco em órgãos potencialmente mais expostos a ameaças e incidentes. Na medida em que a lista for atualizada, novos órgãos da APF serão atendidos, mantendo o ciclo de conscientização e capacitação essenciais para manter a cultura de proteção.

Em termos de abrangência do plano a longo prazo, considera-se que virtualmente todos os órgãos da APF tem investido na transformação digital de suas atividades. O Portal Gov.BR, a plataforma digital de relacionamento do cidadão com o Governo federal, hospeda atualmente quase 4.800 serviços, disponibilizados por vários órgãos e entes públicos. Logo, a intervenção pretendida com este plano detém abrangência nacional e possui espectro suficiente para impactar todo o conjunto da APF.

Fixamos os seguintes objetivos e resultados-chaves (objectives and key results, OKRs) para o plano, a seguir expostos.

Objetivo 1: Formar lideranças transformadoras da cultura de SegInfo/SegCiber na APF

Resultado-chave 1

- Engajamento das lideranças da alta administração dos órgãos prioritários na transformação da cultura de SegInfo/SegCiber na APF;

Resultado-chave 2

- Conscientização de lideranças da alta administração dos órgãos prioritários, com enfoque na compreensão das ameaças e riscos relacionados aos dados geridos; e

Resultado-chave 3

- Capacitação da alta administração e de potenciais lideranças dos órgãos prioritários, com enfoque prático e direcionado às suas atividades cotidianas.

Métricas

- Reunir-se anualmente com 70% de integrantes da alta administração dos órgãos prioritários para atendimento personalizado, conscientização e feedback sobre SegInfo/SegCiber;
- Capacitar ao menos 70% dos integrantes da alta administração e 50% das potenciais lideranças dos órgãos prioritários em SegInfo/SegCiber com enfoque nas competências e dados geridos pelo órgão;
- Integrar a participação de ao menos um membro da alta administração do órgão prioritário em ao menos 50% dos exercícios práticos do quadrimestre;
- Capacitar 90% dos gestores de SegInfo dos órgãos prioritários;
- Apresentar anualmente resultados do avanço do projeto, com dados relacionados à auditoria do TCU sobre o órgão, se houver, dados estatísticos de avaliação e espaço para sugestões de adaptação do projeto a mudanças de paradigma do órgão.

Objetivo 2: Transformar a cultura de SegInfo/SegCiber na APF

Resultado-chave 1

- Conscientização dos servidores dos órgãos prioritários, com enfoque na compreensão das ameaças e riscos relacionados aos dados tratados; e

Resultado-chave 2

- Capacitação dos servidores dos órgãos prioritários, com enfoque prático e direcionado a suas atividades cotidianas.

Métricas

- Mapear e parametrizar os padrões conhecidos de risco de forma individualizada para cada setor;
- Visitar, no quadrimestre, ao menos 50% dos setores dos órgãos prioritários para conscientizar os servidores e realizar exercícios práticos de SegInfo/SegCiber, baseados nas atividades cotidianas do setor, com enfoque na compreensão das ameaças e riscos relacionados aos dados tratados nessas atividades;
- Capacitar 40% dos servidores dos órgãos prioritários;
- Promover avaliações quadrimestrais de feedback sobre a condição do projeto;
- Realizar ao menos 3 treinamentos “mão-na-massa” por quadrimestre; e
- Promover um evento quadrimestral por órgão prioritário de conscientização sobre SegInfo/SegCiber, com enfoque na compreensão das ameaças e riscos relacionados aos dados geridos pelo órgão.

Objetivo 3: Elevar o Brasil para o Top 5 global de SegCiber

Resultado-chave 1

- Entrada do Brasil no Top 5 de Segurança Cibernética Global da UIT em até 5 anos; e

Resultado-chave 2

- Manutenção da proteção da informação, qualidade e confiança dos serviços públicos.

Métricas

- Promover avaliação quadrimestral de feedback pelos usuários dos serviços públicos dos órgãos prioritários;
- Realizar benchmarking dos países Top 5 em SegCiber buscando diferenciais e boas práticas em cultura e capacitação;
- Realizar, anualmente, estudo de viabilidade de implementação de programas e projetos identificados em outros países, que propiciem a redução dos incidentes de SegCiber e de sugestões apresentadas por servidores, pela alta administração e pelos cidadãos;
- Mapear e monitorar os programas e projetos de cultura e capacitação em SegInfo/SegCiber na APF que possam impulsionar melhores resultados; e
- Acompanhar a maturidade das organizações quanto à implementação dos controles críticos de SegInfo/SegCiber, por meio do Framework de Privacidade e Segurança da Informação da SGD e das auditorias do TCU e estabelecer ações e medidas de aprimoramento dos planos de ação de acordo com os critérios da UIT.

Para alcançar os resultados-chaves, estruturamos o plano nas seguintes etapas, a seguir.

Etapas

Enap e Esint

- Elaboram em conjunto materiais didáticos para desenvolver a compreensão de ameaças, riscos e impactos dos incidentes de SegInfo/SegCiber. O enfoque é a importância de manter a cultura de proteção e de reportar os incidentes, não a responsabilização do servidor; e
- Inserem esses conhecimentos em cursos para a formação de lideranças para o setor público, voltados para o desenvolvimento de competências, habilidades e atitudes em SegInfo/SegCiber.

Alta administração dos órgãos prioritários

- Acompanha de forma ativa a transformação da cultura de SegInfo/SegCiber, monitorando a implementação do plano com o apoio da SGD e da Abin; e
- Participa em parte dos exercícios práticos, tanto para incentivar os servidores quanto para se capacitar.

Ascoms

- Promovem a divulgação dos materiais de conscientização e dos eventos setoriais e anuais.

SGD, Abin e setores de SegInfo/SegCiber do público-alvo

- Mapeiam e parametrizam as ameaças, os riscos e as necessidades de melhoria individualizadas do público-alvo;
- Elaboram plano de ação personalizado para aprimorar Seginfo/Segciber. O plano de ação adapta o material didático base para incluir situações da rotina dos servidores do órgão e de sua alta administração, com exercícios práticos; e
- Apresentam e validam o plano perante a alta administração do público-alvo.

Setores responsáveis pela SegInfo/SegCiber do público-alvo

- Promovem os exercícios práticos com as equipes e a alta administração; e
- Atualizam os exemplos e as atividades conforme a mudança da realidade do seu órgão.

A partir da estrutura proposta, consideramos que o plano é viável e exequível, já que a intervenção não enseja grandes impactos orçamentários, não tem contornos que envolvam debates políticos ou ideológicos, está em linha com o que previsto normativamente para o tema e observa as recomendações e boas práticas encorajadas, inclusive, por organismos multilaterais. Sendo esse o quadro, não deve experimentar dificuldades para a inserção na agenda governamental.

Consideramos, por fim, que o plano estratégico proposto contribui para alcançar o futuro desejado consistente na visão do Brasil como liderança em SegInfo/SegCiber (seção 2). O plano volta-se a reforçar a capacidade do aparato estatal de oferecer respostas efetivas às necessidades e legítimas expectativas da coletividade nessas áreas. Com efeito, o plano gera valor público ao mitigar riscos à garantia de continuidade dos serviços públicos e à preservação dos dados dos cidadãos – em última análise, protegendo o seu direito constitucional à privacidade –, pelo que oferece resposta efetiva a um problema público relevante.

7 Plano de Comunicação

O material de apresentação aos atores envolvidos e stakeholders para implementação do plano de ação deve ser de fácil e célere compreensão, de modo a ressaltar os pontos chaves da análise desenvolvida e com destaque para o potencial de melhora dos resultados a partir de sua implementação.

A cultura deve ser apresentada como uma dimensão essencial e deve ser considerada quando uma instituição planeja estabelecer um programa de segurança da informação e ser compreendida de forma centrada no “fator humano”, ou seja, seus valores e premissas de ação, tacitamente compartilhadas, sobre SegInfo/SegCiber. A cultura organizacional precisa ser entendida como um aspecto importante que pode melhorar o desempenho, determinar a estratégia e os objetivos da organização e empregado para influenciar o comportamento dos servidores em prol da proteção do órgão.

O objetivo do plano de comunicação é, assim, informar esses atores envolvidos e stakeholders da importância e do potencial de formar melhor a alta administração e os servidores do Poder Executivo federal, com o intuito de desenvolver uma cultura de SegInfo/SegCiber.

A apresentação deve, portanto, demonstrar que a alta administração e corpo de servidores precisam compreender a necessidade de mudança de paradigma para o tratamento de dados pelo "saber-fazer", com a compreensão real sobre as ameaças e o potencial lesivo dos incidentes para o país.

Ademais, a capacitação também deve ser ressaltada com enfoque no diferencial de ser voltada para aplicação prática, com treinamentos de rotina que indicam maior potencial de redução dos incidentes de SegInfo/SegCiber.

Destaques para apresentação aos atores envolvidos

Estratégia 1

- conscientizar alta administração e corpo de servidores sobre ameaças com materiais produzidos pela SGD/ME e ABIN/GSI/PR, em parceria com os demais atores envolvidos, e apresentações setoriais e anuais promovidas pelas Ascoms;

Estratégia 2

- Capacitar, com viés prático, a alta administração, lideranças potenciais e o corpo de servidores, com treinamentos contínuos personalizados para realidade do órgão, voltados para atividades de rotina, a partir de ação integrada entre Enap, Esint, Ascoms e setores de SegInfo/SegCiber do público-alvo.

Avaliação

A partir das métricas estabelecidas:

1) abrir enquetes anuais de avaliação dos servidores com espaço para sugestões, com intento de aprimorar os cursos e treinamento;
2) ofertar a participação pública de avaliação; e
3) criar espaço de avaliação da alta administração sobre compreensão da proposta, os resultados obtidos e a estatística de avaliação, bem como para sugestão de adequações.

Referências

[1] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral>. Acesso em 21 nov. 2022.

[2] Conforme o Decreto 9.637, de 26 de dezembro de 2018, que dispõe sobre a Política Nacional Segurança da Informação (PNSI), a Segurança da Informação engloba: (i) a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. Dessa forma, como define a PNSI, entende-se que a SegCiber faz parte da SegInfo.

[3] Plataforma do Governo federal para notificação de casos suspeitos e controle epidemiológico. Disponível em: <https://notifica.saude.gov.br/>

[4] Sistema de Informações do Programa Nacional de Imunizações. Disponível em: <http://sipni.datasus.gov.br/>

[5] Plataforma oficial de comunicação entre o cidadão e o SUS. Disponível em: <https://conectesus.saude.gov.br/>

[6] BRASIL. Tribunal de Contas da União. Acórdão nº 4035/2020. Plenário. Relator: Ministro Vital do Rêgo. Processo TC 001.873/2020-2. Ata nº 47/2020. Sessão: 08/12/2020.

[7] BRASIL. Tribunal de Contas da União. Acórdão nº 1384/2022. Plenário. Relator: Ministro Augusto Nardes. Processo TC 036.301/2020-1. Ata nº 22/2022. Sessão: 15/06/2022. Disponível em: <https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html>. Acesso em: 21 nov. 2022.

[8] Organização de Cooperação e Desenvolvimento Econômico (OCDE). Relatório Global de Segurança Cibernética, 4ª Edição, 2020. Disponível em: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>. Acesso em: 30/10/2022.

[9] Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/2022/novembro/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo>. Acesso em: 21 nov. 2022.

[10] União Internacional de Telecomunicações (UTI). Índice de Segurança Cibernética 2020. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>. Acesso em: 21 nov. 2022.

[11] Organização dos Estados Americanos. Revisão da Capacidade de Cibersegurança da República Federativa do Brasil, 2020. Disponível em: <https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf>. Acesso em: 30/10/2022.

[12] BRASIL. Tribunal de Contas da União. Acórdão nº 1768/2022. Plenário. Relator: Ministro Vital do Rêgo. Processo TC 036.301/2021-3. Ata nº 30/2022. Sessão: 03/08/2022.
[13] BRASIL. Tribunal de Contas da União. Lista de Alto Risco da Administração Pública. Brasília: Tribunal de Contas da União, 2022. Disponível em: <https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html>. Acesso em: 21 nov. 2022.
[14] Anexo I da Portaria CD/ANPD nº 1, de 8 de março de 2021.
[15] Organização dos Estados Americanos. Revisão da Capacidade de Cibersegurança da República Federativa do Brasil, 2020. p. 16. Disponível em: <https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf>. Acesso em: 30/10/2022..
[16] ALI, Rao Faizan et al. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, v. 11, n. 8, p. 3383, 2021.
[17] ALI, Rao Faizan et al. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, v. 11, n. 8, p. 3383, 2021.
[18] BRASIL. Tribunal de Contas da União. Acórdão nº 1768/2022. Plenário. Relator: Ministro Vital do Rêgo. Processo TC 036.301/2021-3. Ata nº 30/2022. Sessão: 03/08/2022.
[19] Spidalieri, Francesca. One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat. Pell Center for International Relations and Public Policy: Newport, Rhode Island, 2013. Disponível em: <https://www.academia.edu/3137267/One_Leader_at_a_Time_The_Failure_to_Educate_Future_Leaders_for_an_Age_of_Persistent_Cyber_Threat>. Acesso em: 12 de outubro de 2022.
[20] Hurel, L.M. Cibersegurança no Brasil: Uma Análise da Estratégia Nacional de Cibersegurança. Instituto Igarapé. Artigo Estratégico 54, 2021.
[21] ALI, Rao Faizan et al. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, v. 11, n. 8, p. 3383, 2021.
[22] BRASIL. Tribunal de Contas da União. Lista de Alto Risco da Administração Pública. Brasília: Tribunal de Contas da União, 2022. Disponível em: <https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html>. Acesso em: 21 nov. 2022.
[23] PPSI SGD. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/PPS>.

Anexo I - Apontamentos e Reflexões

Brainstorming

O problema público de SegInfo/SegCiber é um tema recorrente de trabalho entre os integrantes do grupo, que já assumiram funções de gerir a temática ou enfrentaram as consequências de incidentes nos seus órgãos, que afetaram a continuidade da prestação de serviços públicos aos cidadãos.

Após a escolha do tema, passamos a compartilhar um link do Miro com textos, apontamentos e ideias para a delimitação do problema público relacionado à temática escolhida. O grupo desenvolveu uma metodologia de trabalho fluída que promoveu o diálogo e o aprimoramento da aprendizagem contínua de seus membros:

- Estruturamos uma local em nuvem para a troca livre de ideias no miro;
- Buscamos estudos científicos de autores e revistas de propriedade no setor;
- Mapeamos o conjunto dos atores implicados na solução do problema;
- Listamos iniciativas já existentes sobre uma possível solução do problema; e
- Realizamos pesquisa de campo com as principais partes interessadas sobre o tema na APF, tendo por base o mapeamento do item 3.

Cada passo foi cercado pelo trabalho colaborativo e pela troca livre de informações, na prática construímos sessões de debates coordenados para melhor entendimento dos resultados obtidos ao longo de toda a pesquisa. Por fim, utilizamos a ferramenta dos objetivos e Resultados-Chave (OKRs), por entendermos que ela seria a mais eficaz para a definição e comunicação de metas a partir de marcos claros. Entendemos que esse foi o melhor método para expressarmos uma estratégia inequívoca a partir das ideias de soluções surgidas durante o processo de elaboração do trabalho.

Para delimitarmos o tema e concluir o plano de ação, realizamos reuniões semanais e dividimos tarefas de fichamento dos textos, entrevista dos atores chaves sobre o problema, revisão e formatação do texto, que foi construído de forma dinâmica e simultânea, com arquivo .DOC compartilhado em nuvem.

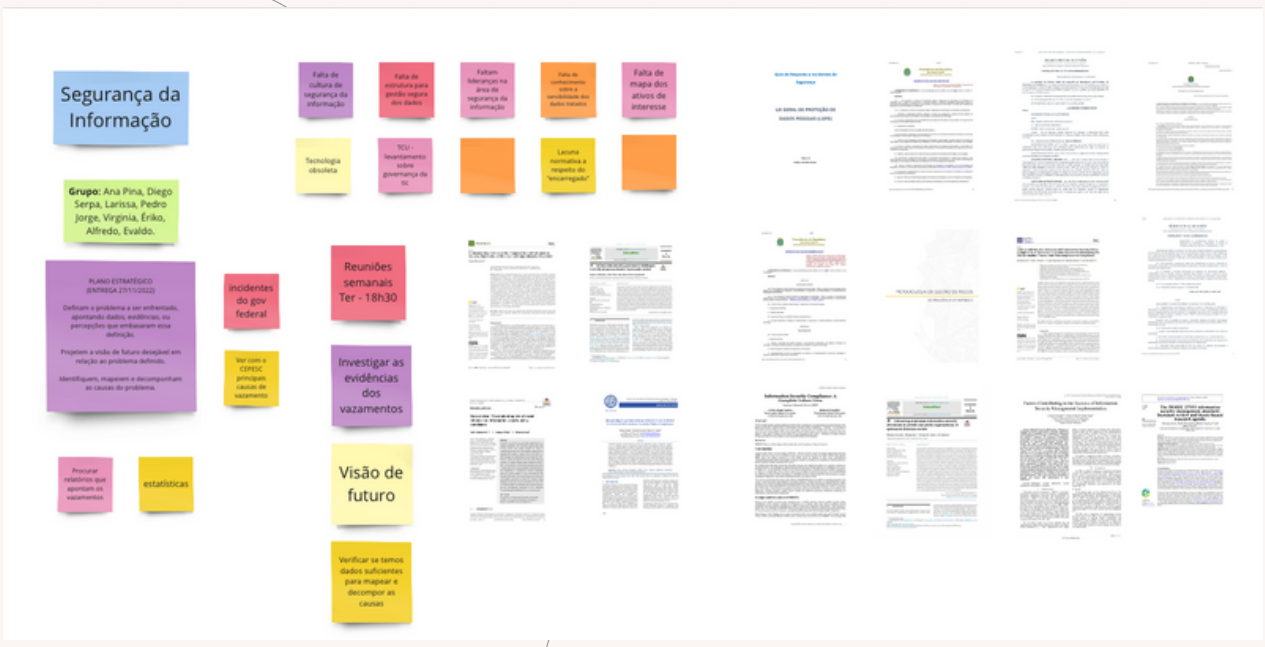


Fig. 1 - Imagem do painel do Miro

Anexo II - Entrevistas

Entrevista Ditec/SG/PR

04 de novembro de 2022
10h

Entrevistado: Edson Floriano, coordenador da Ditec/PR

1. Qual é sua experiência na área?

- Estou há cinco anos na Ditec, o último como coordenador.

2. Entre infraestrutura e usuário, qual é o fator mais preponderante nos incidentes na PR?

- Entre infraestrutura e usuário, o entrevistado acredita que as maiores vulnerabilidades realmente estão associadas às condutas dos usuários

3. Como vê o fator cultura e capacitação em SegInfo/SegCiber nos incidentes na PR?

- Na Presidência, a rotatividade do público interno é um desafio para evoluir em matéria de conscientização. Em comparação com a FAB, de onde vim, os servidores chegam aqui pouco ou nada doutrinados em matéria de segurança. Fala conhecimento a respeito do que é uma ameaça, mesmo em relação àquelas mais básicas. O usuário é muito "inocente" e cai em armadilhas simplórias. As campanhas de conscientização não sensibilizam a contento.

4. Quais são as iniciativas da PR para abordar esse quadro?

- A SegInfo na PR hoje tem muitos *players*. Há um comitê estruturado, há o papel do GSI... Esses atores se esforçam constantemente para elevar o nível de cultura e de capacitação por meio de campanhas, palestras etc., apesar do impacto da rotatividade do público. Creio que, para sensibilizar o usuário, só mesmo trazendo a questão a sua temática individual: sua conta; sua imagem; o prejuízo ao seu trabalho ou ao do órgão etc.

5. Você acrescentaria algum aspecto importante para melhorar a cultura de SegInfo/SegCiber?

- É essencial sensibilizar a alta gestão para a segurança. Vejo que as campanhas de conscientização e capacitação acabam atingindo apenas os escalões mais baixos. Na verdade, as autoridades precisam ser atingidas para que sigam as melhores práticas e deem um patrocínio mais resoluto às iniciativas. É como dizem: "a palavra convence, o exemplo arrasta".

Entrevista Sefti/TCU

09 de novembro de 2022
14h

Entrevistado: grupo de auditores do TCU

1. No Acórdão 1768/2022, o TCU, com base em relatório da Sefti, apontou seis achados relacionados à baixa governança de dados nas organizações federais. A Sefti percebe a preponderância de algum desses aspectos? Qual seria o aspecto mais problemático do ponto de vista da governança de dados?

- Não há preponderância, todos os aspectos são relevantes. O treinamento e a conscientização são a base da boa governança. Na sequência, é necessário que os processos estejam bem estruturados. Por fim, é importante "arregaçar as mangas" e executar proativamente processos como a gestão de vulnerabilidades.

2. A Sefti tem percepção sobre as possíveis causas quanto ao cenário preocupante relacionado à conscientização e à capacitação dos colaboradores da APF em SegInfo/SegCiber (quinto achado do acórdão 1768/2022)?

- Os órgãos não priorizam SegInfo/SegCiber porque as entregas relacionadas não "aparecem", não são vistosas. Essas áreas geralmente são relegadas ao segundo plano. Não obstante, têm ganhado mais prioridade atualmente em razão do aumento do número de incidentes, o que tem aumentado a percepção de risco. O regramento também é muito recente (2020 em diante) e só agora há a tendência de o *enforcement* estruturar-se e aumentar (exemplo ANPD). Por fim, não há uma autoridade central em SegInfo/SegCiber no Executivo; a figura está dispersa entre GSI — que normatiza, mas não fiscaliza — e SGD.

3. Entre as ações previstas na Estratégia de Fiscalização do TCU em SegInfo/SegCiber 2020-2023, está a indução de boas práticas e do cumprimento de normas. Quais são as iniciativas relacionadas a promoção de cultura e capacitação em SegInfo/SegCiber? Quais são as iniciativas relacionadas ao diagnóstico de falhas relacionadas à cultura e à capacitação?

- O tema da governança de dados tem sido abordado em acórdãos há mais de uma década. Infelizmente, os órgãos fiscalizados acabam não implementando as recomendações em maior grau. Ainda prevalece uma cultura de "apagar incêndios", de agir apenas quando o problema é premente. A Sefti tem seguido na linha de fiscalizar, coletar boas práticas e difundi-las para os outros órgãos por meio de recomendações. Apesar de a estratégia de fiscalização não prever iniciativas diretamente relacionadas à promoção de cultura e de capacitação, o TCU pode estimular a oferta de cursos na Enap.

4. Como tem sido a interação com a Secretaria de Governo Digital do Ministério da Economia enquanto órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp)? A SGD informou alguma iniciativa relacionada a cultura e capacitação em cumprimento às recomendações do Acórdão 1768/2022?

- A Sefti e a SGD têm uma parceria de longa data, a qual gerou frutos como a evolução do marco de contratações em TIC. A SGD é ponto focal para uso compartilhado e coordenado de dados, uso do portal gov.br etc., mas a Sefti desconhece se há alguma ação relacionada a cultura e capacitação.

5. A Sefti vê então uma tendência positiva quanto à governança de dados?

- Não existe uma tendência, existe uma obrigação de melhorar. Os incidentes, que são um vetor do enforcement, estão ocorrendo e os órgãos não podem se dar ao luxo de negligenciar o tema. Por isso, a situação deve evoluir com rapidez. Todavia, não há ações em capacitação e cultura que sejam condizentes a essa necessidade. A oferta de cursos em SegInfo/SegCiber é insuficiente. A adoção em massa do teletrabalho durante a pandemia, por exemplo, veio desacompanhada de preocupações com segurança. Os sistemas informatizados poderiam ser utilizados nesse sentido, como uma forma de induzir o servidor a trabalhar com mais segurança, uma forma de orientar o comportamento. Se o sistema limitar o servidor a opções seguras, a chance de falhas pode ser severamente reduzida.

Entrevista CTIR/Abin

09 de novembro de 2022
16h

Entrevistado: João Pincovscy, chefe do CTIR/Abin

1. Estamos conversando com outros órgãos sobre o fator "cultura e capacitação" nos temas de SegInfo/SegCiber e de governança de dados. Esse é o fator mais importante do ponto de vista dos incidentes detectados pela Abin?

- Nosso público é diferente nesse sentido. Temos pouquíssimos problemas. Fugimos bastante ao perfil da Esplanada. Porém, no geral, o fator cultura e capacitação é uma necessidade constante, eterna e cíclica. Quanto maior a organização, mais é um fator problemático. Principalmente para organizações que custodiam informações sensíveis. Isso não é uma falha da APF, isso é uma falha de todas os organizações no mundo inteiro. Vide ações do CERT.br, que se esforça muito para melhorar a difusão de boas práticas de SegInfo/SegCiber. O problema extrapola e muito a APF.

2. Você falou que Agência tem pouquíssimos incidentes, contrastando com a realidade de outros órgãos da APF. Qual é a principal causa desses poucos incidentes que ocorrem? Ela é diferente do quadro geral?

- Apesar da diferença no número de incidentes, a principal causa dos incidentes na Abin é similar à causa nos outros órgãos: o usuário. A tendência natural das pessoas, com o tempo, é "baixar a guarda", mesmo com a cultura de segurança existente na Agência. Existe, adicionalmente, uma diferença no perfil geracional dos servidores. Os servidores mais jovens cresceram vivendo num mundo digital e conseguem detectar mais facilmente ameaças comuns, como o phishing.

3. Como vê as iniciativas relacionadas a cultura e capacitação na APF?

- No caso da Agência, a missão de conscientização e reciclagem não está sendo abraçada formalmente por ninguém. O que há são iniciativas personalizadas, briefings de segurança para usuários específicos, mas falta institucionalização. Porém, talvez essa estratégia seja mais eficaz: com uma atuação "sob medida" para cada usuário, a qualidade e o aproveitamento são maiores. É necessário que o treinamento seja baseado em casos práticos, inserindo o conteúdo no cotidiano das atividades do usuário. Não vejo a necessidade de um workshop institucional geral porque creio que ele teria baixa efetividade.

09 de novembro de 2022 16h

4. Você mencionou as diferenças entre a cultura da Agência e a cultura da Esplanada em geral. Como vê esse contraste?

- Há uma assimetria total entre essas culturas. Os servidores de outros órgãos, em geral, não têm consciência sobre a sensibilidade das informações com que lidam. São vários os casos que eu poderia relatar para ilustrar esse aspecto, como, por exemplo, o uso de serviços de nuvem particulares por um alto gestor para armazenar documentos contendo informações sensíveis.

5. E em relação as diferenças entre gestores e servidores, nota muita diferença?

- Vejo a diferença entre a cultura dos servidores e dos gestores sem vínculo, os quais muitas vezes carregam uma cultura empresarial. No mundo empresarial, a reparação é a multa paga pela quebra de contrato, o lucro cessante etc. No contexto da administração pública, porém, os danos são irreparáveis, pois envolvem serviços públicos e, geralmente, dados pessoais. Os dados podem ser estratégicos para o país; mesmo que não o sejam a credibilidade do governo sempre será afetada. Por isso, é necessária a formação e a especialização dos gestores; os gestores têm de ser profissionalizados para a atuação no serviço público.

Entrevista Consultor/MS

10 de novembro de 2022
10h

Entrevistado: Leandro Pfeifer, consultor contratado pelo MS

1. Que atividade você está desempenhando hoje?

- Estou construindo um modelo de governança de dados para o Departamento de Monitoramento em Saúde do MS. Governança é construir uma camada estratégica, implementá-la por meio da gestão e então aplicar os requisitos operacionais. Tive experiência em governança de dados na iniciativa privada com duas empresas da área financeira. Lá, a preocupação principal era a padronização e a segurança.

2. Você vê o investimento em capacitação e mudança cultural como uma medida efetiva para melhorar a governança de dados na APF?

- Sou cético... Vejo resultados com capacitação *hands-on* contínua, dentro do contexto de trabalho das pessoas. A mudança em segurança é sempre lenta. Utilizando esse modelo prático, já consegui resultados em cinco organizações diferentes. É importante conjugar a "evangelização" do usuário com um plano bem construído e com monitoramento, principalmente por parte dos gestores. Nessa matéria, a simples omissão ou indiferença dos gestores já é negativa.

3. E na esfera dos usuários de serviços públicos, como você vê a questão da cultura e da capacitação?

- Acho que o governo perdeu uma boa oportunidade de induzir uma mudança positiva por meio do portal Gov.br durante a pandemia, no momento em que os usuários migraram em massa para os serviços públicos digitais. Ainda assim, creio que a LGPD e as ações desencadeadas por ela atuarão na evangelização dessas pessoas a longo prazo.

Entrevista DEGDI/SGD/SEDGGD/ME

10 de novembro de 2022
15h30

Entrevistado: Leonardo Rodrigo Ferreira, Diretor do Departamento de Privacidade e Segurança da Informação

1. No Acórdão 1768/2022, o TCU apontou seis achados relacionados à baixa governança de dados nas organizações federais. Qual é a visão da SGD sobre isso? Percebe a preponderância de algum desses aspectos? Qual seria o aspecto mais problemático do ponto de vista da governança de dados?

- Inicialmente, considera que SegInfo/SegCiber não são necessariamente relacionados a uma baixa governança de dados, mas não entrará nessa discussão doutrinária. A SGD é órgão central do SISP, que congrega 238 órgãos. O DEGDI é um de seus quatro departamentos. Para enfrentar esse desafio com amplitude e profundidade, o Departamento estruturou um programa que já completou mais de um, o Programa de Privacidade e Segurança da Informação (PPSI). Esse programa volta-se a 57 órgãos prioritários, selecionados com base no acórdão TCU 1.889/2020, com a finalidade de aumentar sua maturidade e resiliência em privacidade e SegInfo. O programa foi concebido em articulação com CGU, TCU, GSI e ANPD e está em estruturado em 5 torres de atuação com base nos riscos relevantes. A torre de pessoas integra diversas ações de capacitação contínuas e esporádicas, tais como a 1ª Semana de Segurança Cibernética (CyberGov) e a 1ª Semana de Proteção de Dados Pessoais. O foco atual é criar um centro de excelência, tomando o exemplo do National Institute of Standards and Technology (NIST/EUA). Por meio da torre de metodologia, o programa já publicou 18 guias sobre privacidade e SegInfo e desenvolveu um framework próprio a ser adotado por padrão na APF. O programa também contempla, com base na experiência da SGD com o atendimento de incidentes, a instalação de um Centro Integrado de Segurança Cibernética do Governo Digital, o qual deve estar operacional em 16 de dezembro. Tudo isso partindo da premissa de que a privacidade e a segurança têm de ser trabalhadas de maneira conjunta.

2. Dentre as torres do programa, qual seria a torre fundamental para melhorar a SegInfo e a SegCiber na APF?

- Sem dúvidas, a torre mais relevante é a de governança. É necessário envolver as autoridades desde o primeiro momento; é necessário que elas monitorem e cobrem a consecução das iniciativas; é necessário que elas deem seu patrocínio.

- Por isso, durante todo o programa, a equipe da SGD tem feito reuniões com os Secretários Executivos dos órgãos prioritários, para destacar avanços e superar obstáculos, e para que elas se conectem às áreas executoras nos seus órgãos. O segundo ponto é ter um método estruturado, um planejamento que dê sentido às ações. O terceiro, por fim, é o investimento nas pessoas, para dar sentido ao planejamento e executar a visão da governança.

3. Como se dá a interação SGD x TCU?

- A SGD e o TCU mantêm interações frequentes. Todo o programa desenvolvido pela SGD foi construído por meio de inputs e sugestões, mesmo que informais, do Tribunal. Trata-se de uma grande parceria.

4. Você mencionou que a SGD tem respondido a incidentes na Esplanada. Em sua percepção, qual é o fator que está por trás da maior parte desses incidentes?

- Em geral, tem a ver com o despreparo do usuário.

5. A SGD tem percepção sobre as possíveis causas quanto ao cenário preocupante relacionado à conscientização e à capacitação dos colaboradores da APF em SegInfo/SegCiber?

- As ações de capacitação têm de ter um norte e uma metodologia de trabalho bem construída, centrada no "mão na massa". É necessário colocar recursos nessa metodologia. Ações descoordenadas ou pontuais não são efetivas.

6. A SGD enxerga alguma tendência?

- A médio prazo, enxergamos um movimento vigoroso de aumento de níveis em SegInfo/SegCiber. A implantação do centro de excelência pode ser um grande vetor nesse sentido. A atuação do governo federal está se consolidando numa política de Estado, que veio para ficar.

Obrigado!

alfredofrota@hotmail.com
anabpina@gmail.com
bserpa@gmail.com
eriko.sedoguchi@gmail.com
evaldo.matheus@gmail.com
l.assis0001@gmail.com
sucena.pedro@gmail.com
vividantasnatal@gmail.com