ATA DE REUNIÃO - TRE-DF/PR/DG/STIC/COIE

Trata-se de reunião Ordinária da Comissão de Segurança da Informação - CSI, realizada dia 30/10/2025, às 14hs, remotamente via *google meet.*

O convite para reunião, foi enviado por e-mail, pelo Gestor de Segurança da Informação, para Andrey Bernardes Correia - Secretário de TIC, João Paulo Carneiro Rodrigues - COIE, Fábio Moreira Lima - SJU, Adriana Aparecida Coelho Pereira - SGP, Paulo Saldanha - SAO, Guilherme de Sousa Juliano - PR, Wildice Lima Ferro Cabral - SCE, Lucia Carvalho Bitar Yung-Tay - DG e Fernando de Castro Velloso - ASCOM. A servidora Wildice Lima Ferro Cabral, Gestora responsável pela Secretaria da Corregedoria Regional Eleitoral - SCE, não pode participar e o servidor Guilherme de Sousa Juliano, Gestor responsável pelo Gabinete da Presidência, também no participou, porém sua substituta, a servidora Cintia Barbosa Coelho, substituta do mesmo, participou.

O Gestor de Segurança da Informação, perguntou a todos os presentes, se poderia gravar a reunião e todos foram unanimes em autorizar, e de pronto foi iniciada a gravação da reunião, que se encontra disponível para consulta em caso de necessidade, no link Gravação_Reunião.

O Gestor de Segurança da Informação, Marcelo Nogueira Lino, iniciou a apresentação que se encontra no arquivo (1930448), cujo resumo segue abaixo:

Cintia Barbosa Coelho iniciou a terceira reunião da Comissão de Segurança e Formação, na qual Marcelo Nogueira Lino detalhou as pendências, incluindo o bloqueio de dispositivos de armazenamento externo via USB, uma medida de segurança que Marcelo Nogueira Lino garantiu que será revalidada para não impactar serviços institucionais após a preocupação levantada por Andrey Bernardes Pousa Correa sobre o circuito eleitoral e a leitura de mídias da urna eletrônica. Marcelo Nogueira Lino também informou que a automação XDR para bloqueio de ransomware está funcionando e, após um debate com Andrey Bernardes Pousa Correa e Lucia Carvalho Bitar Yung-Tay, aceitou retirar a proposta de bloqueio do WhatsApp Web devido à iminente contratação da solução Omni Channel, usada para comunicação com mesários e eleitores, e o uso do WhatsApp Web pela Corregedoria e Secretaria Judiciária. Por fim, Marcelo Nogueira Lino apresentou propostas futuras de melhoria, como a continuidade do projeto IGA para gestão de identidades e o planejamento estratégico de segurança, com Lucia Carvalho Bitar Yung-Tay expressando preocupação com o custo de R$ 2 milhões para a contratação do IGA.

A servidora Cintia Barbosa Coelho, substituta do titular do Gabinete da Presidência, deu início à terceira reunião da Comissão de Segurança e Formação, com Marcelo Nogueira Lino apresentando a pauta. Marcelo Nogueira Lino detalhou as pendências de reuniões anteriores, destacando o bloqueio de dispositivo de armazenamento externo, que está em andamento com a implementação de um portal para instalação de sistemas operacionais via rede, eliminando a necessidade de USB. Essa ação visa proteger o ambiente, dada a alta incidência de contaminação por uso de pen drives pelos usuários, citando um incidente recente no cartório da 11ª zona eleitoral.

O Secretário da STIC, Andrey Bernardes, levantou uma preocupação sobre o bloqueio de USB, já que várias máquinas utilizadas no processo eleitoral, aquelas que utilizam o sistema SIS, necessitam das portas USB para leitura de mídias da urna eletrônica e de dados do Jedi. O Gestor de SI, Marcelo Nogueira Lino, reconheceu a preocupação, e afirmou que a possibilidade de desbloqueio para máquinas com finalidade institucional já havia sido identificada em testes anteriores e seria revalidada para garantir que não haja impacto nos serviços. O Coordenador da COIE, João Paulo Carneiro Rodrigues, questionou o Gestor de SI sobre a resolução de problemas de *delay* na console de administração da ferramenta XDR da Trend, que é utilizada para bloqueio e liberação de máquinas, e se a questão foi resolvida. O Gestor informou que ajustes foram realizados na configuração da console do XDR junto com a empresa parceira, DFTI, mas que seriam realizados novamente, para dirimir qualquer dúvida. Ainda

sobre o assunto bloqueio das portas USB, o Gestor de SI, esclareceu que o bloqueio se aplica apenas para mídias de armazenamento que utilizarem as portas USBs, e que tokens de certificado digital estão liberados e foram testados sem impactos. O Coordenador da COIE, João Paulo, questionou ainda o Gestor de SI sobre a vigência do contrato da ferramenta XDR, que foi confirmada que está vigente até o primeiro semestre de 2027, e que como foi um projeto prioritário que veio do TSE, entende que provavelmente nova contratação será realizada, para manutenção deste serviço. De toda forma, o Gestor de SI informou que tomará as precauções levantadas e realizará novos testes, submetendo a decisão final de bloqueio à STIC e a COIE, e após deliberarão à CSI.

O Gestor de SI, informou que a ativação da automação do XDR para bloqueio de ransomware já está em funcionamento, mitigando contaminações sem impactar os serviços. Sobre o uso do WhatsApp Web, este ainda mencionou que havia estancado a iniciativa de estudo e bloqueio devido a questões culturais e de uso na comunicação via esta solução com os cidadãos. Que com a migração para o Microsoft 365 e o Teams, ele propôs retomar a discussão para usar o Teams para comunicação institucional interna e manter o WhatsApp somente via celulares institucionais ou ramais fixos para áreas de negócio.

Ainda sobre o assunto bloqueio do WhatsApp Web, o Secretário da STIC, Andrey Bernardes e a Diretora Geral, Lucia Carvalho Bitar Yung-Tay, informaram sobre a iminente contratação da solução Omni Channel, que utiliza o WhatsApp para comunicação com mesários e eleitores, com previsão de entrada em operação no início do próximo ano. Lucia Carvalho Bitar Yung-Tay ressaltou que a Corregedoria e a Secretaria Judiciária utilizam o WhatsApp Web, o que torna o bloqueio um grande transtorno para o tribunal. Diante das informações novas, o Gestor de SI, ficou de conversar com o servidor da Corregedoria Diego Batista, pois o mesmo já testou a solução, e poderá esclarecer qualquer dúvida sobre a solução Omni Channel, para que possíveis impactos possam ser dimensionados.

O Gestor de SI resumiu as ações da assessoria, que incluem o monitoramento do ambiente com diversas ferramentas e a atuação preventiva para mitigar riscos, além do tratamento de eventos reportados por empresas como GRGTECH, responsável pelo suporte e monitoração do ambiente via console da solução DARKTRACE, e DFTI, responsável pelo suporte e monitoração do ambiente via console da solução XDR da fabricante TRENDMICRO. As ações preventivas baseiam-se em relatórios diários de alertas sobre possíveis ações vulnerabilidades que possam comprometer o ambiente do Tribunal, que são identificadas por estas soluções, como por exemplo, o uso de pen drives que podem alertar a existência de um malware. A assessoria também solicita atualizações do ambiente com base em relatórios gerados pelo TENABLE SC, outra solução que analisa vulnerabilidades em computadores servidores.

O Gestor de SI, detalhou o processo de tratamento de um alerta crítico identificado pelas soluções que administram, que pode começar com o monitoramento realizado pela solução Darktrace e a análise de eventos pela inteligência artificial da ferramenta, e que em seguida, eles analisam o mesmo dispositivo na solução de XDR da Trend para avaliar o índice de risco e os detalhes, como versões antigas de sistemas operacionais (ex: Windows 10, versão 22H2). O processo continua com a análise dos relatórios diários entregues pela contratada DFTI, onde são identificadas e analisadas várias informações, como por exemplo instalações de softwares não autorizados (ex: PDF Creator) e, por fim, um chamado é aberto, para que a equipe de N2 do Helpdesk possa realizar uma investigação mais profunda, que podem por vezes, levar à formatação das máquinas, como ação preventiva para garantir a segurança do ambiente.

O Gestor ainda, apresentou sete propostas de melhoria, que incluem o tema já discutido anteriormente, o bloqueio das portas USB (aguardando nova análise), criar VLANs específicas para ambientes de desenvolvimento/homologação/produção, e ampliar a proteção de aplicações no F5/Big-IP. Outra proposta apresentada foi a desabilitação das placas Wi-Fi nos desktops. Sobre este ponto em específico, o Secretário da STIC, Andrey Bernardes, contrapôs, explicando que a aquisição de novos computadores e notebooks para uso nas eleições, especialmente no segundo andar da Sede, exige o uso de Wi-Fi, pois não foi possível passar cabos de rede, devido à limitação de infraestrutura. O Gestor de SI concordou com a flexibilidade da segurança para não impactar os usuários, reconhecendo que o futuro da integração e interconexão das redes serão as redes WiFi.

Outras Propostas e Projetos Estratégicos foram abordados pelo Gestor de SI, que apresentou, outras propostas de ações futuras, como atualizar a solução de vulnerabilidades TENABLE-SC, implementar mais um nível de proteção para os backups, com a utilização de armazenamento em

nuvem, *backup as a service* (BaaS). Ele destacou que a concretização dessas propostas depende do apoio e disponibilidade das equipes da SETEL, SESOP e SEAPU. Ainda referente às novas propostas, o Gestor de SI, mencionou a entrega dos Protocolos que fazem parte da Portaria 162/2021 do CNJ, que estão incluídos no Planejamento Estratégico institucional como meta a ser atingida, e que serão entregues todos com 100% de aderência aos normativos existentes. Além disso, mencionou ainda a entrega da Análise de Impacto nos Negócios (BIA) e do Plano de Continuidade de Negócio (PCN), ambos previstos para o final do ano, Dez/2025.

O Gestor de SI comentou ainda que o projeto de ZTNA(*Zero Trust Network Access*) + SWG(*Secure Web Gateway*) + IGA(*Identity Governance Administration*), que substituirá a VPN, e melhorará sobremaneira a gestão automatizada de credenciais e identidades, atendendo aos achados da auditoria interna realizada em 2022 no processo de Gestão de Segurança da Informação, conforme processo SEI 0004797-28.2024.6.07.8100, em reunião com equipe do TSE (Zottmann, Marcelo Carneiro e Venício), ficou decidido que o TSE irá tocar o projeto de ZTNA + SWG, pois afirmaram que o deles está mais adiantado, e que o TRE-DF poderá tocar o projeto já em trâmite (0002653-81.2024.6.07.8100), porém contemplando somente o IGA e NGFW(Next Generation Firewall) + Microsegmentação. A Diretora Geral, Lucia Carvalho Bitar Yung-Tay questionou o Gestor de SI, sobre o custo, e este respondeu que foi estimado para o projeto em torno de R$ 2 milhões para a contratação do IGA. A Diretora Geral expressou preocupação com a fonte de recursos e o orçamento para o próximo ano, especialmente com as contratações eleitorais de 2026, e solicitou que quando este projeto em desenvolvimento pelo Gestor, estiver com os artefatos prontos, que antes da tramitação, fosse realizada um alinhamento com o Secretario da STIC e com o Coordenador da COIE, e após com a Diretora Geral.

Próximas etapas sugeridas

1. Referente ao bloqueio das USBs nas máquinas disponibilizadas ao usuários, o Gestor de Segurança da Informação, irá revalidar e realizar novos testes no ambiente para desbloqueio das portas USB em máquinas específicas, para garantir o funcionamento sem impactar os serviços dos usuários. Na sequência, irá demonstrar para o Secretário da STIC e para o Coordenador da COIE, Andrey Bernardes e João Paulo, respectivamente, os casos de uso no ambiente, para então decidirem qual ação será tomada quanto a ativação do bloqueio das USBs das máquinas dos usuários.

2. Referente à proposta de bloqueio do WhatsApp Web, o Gestor de Segurança da Informação, irá conversar sobre a solução Omni Channel, com Diego Batista da Corregedoria, para conhecer em detalhes a solução que está em implementação no Tribunal, para após, deliberar em conjunto com o Secretário da STIC e o Coordenador da COIE, qual solução será tomada.

A reunião então foi encerrada após a finalização da apresentação, das discussões e deliberações apresentadas acima.

Documento assinado eletronicamente por **Marcelo Nogueira Lino**, **Assessor**, em 10/11/2025, às 16:52, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ADRIANA APARECIDA COELHO PEREIRA**, **Secretária**, em 10/11/2025, às 17:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **PAULO TADEU MOREIRA SALDANHA**, **Secretário**, em 11/11/2025, às 13:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FÁBIO MOREIRA LIMA**, **Secretário**, em 11/11/2025, às 15:32, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CINTIA BARBOSA COELHO**, **Chefe de Gabinete Substituto**, em 11/11/2025, às 17:09, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FERNANDO DE CASTRO VELLOSO FILHO**, **Assessor**, em 11/11/2025, às 18:03, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LÚCIA CARVALHO BITAR YUNG-TAY**, **Diretora-Geral**, em 12/11/2025, às 07:58, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANDREY BERNARDES POUSA CORREA**, **Secretário**, em 13/11/2025, às 15:51, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-df.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1930450** e o código CRC **21CB60F3**.