Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSIPDP)
Biênio 2022/2024

Extrato da Ata da 1ª Reunião de 2024

1. Informações da reunião

Data: 01/02/2024 **Hora:** 16:00 **Tipo:** ordinária

Formato: híbrido **Plataforma:** Meet **Local:** Auditório do 24º andar do Edifício Sede

2. Participantes

Integrantes (membros)	
Excelentíssima Desembargadora Ouvidora Dra.	Sueli Tomé da Ponte
Excelentíssima Juíza Auxiliar da Presidência Encarregada pela Proteção de Dados Pessoais Dra.	Roberta Carolina de Novaes e Souza Dantas
Excelentíssimo Juiz Auxiliar da Vice-Presidência Administrativa Dr.	Eber Rodrigues da Silva
Excelentíssima Juíza Titular da 13ª Vara do Trabalho da Zona Sul de São Paulo Dra.	Juliana Jamtchek Grosso
Excelentíssimo Juiz Titular da 4º Vara do Trabalho de Cubatão Dr.	Moisés dos Santos Heitor
Secretaria-Geral da Presidência	Sra. Telma Ferreira Rocha Bandoni
Secretaria da Corregedoria Regional	Sr. Conrado Augusto Pires
Diretor-Geral da Administração	Sr. Rômulo Borges Araújo
Diretora da Secretaria de Gestão Estratégica e Projetos Substituta (SGEP)	Sra. Patrícia Andrade Castro Carvalho
Diretor da Secretaria de Segurança Institucional (SSI)	Sr. Hélcio Nalon Alves
Diretor da Secretaria de Tecnologia da Informação e Comunicação (SETIC)	Sr. Marcio Nisi Gonçalves
Diretor da Coordenadoria de Segurança de TIC Substituto (CSTIC)	Sr. Leonardo Luis Soares

Diretora da Coordenadoria de Governança e Projetos (CGP)	Sra. Patrícia Andrade Castro Carvalho
Diretor da Coordenadoria de Apoio ao Planejamento e à Governança de TIC (CAPGTIC)	Sr. Rogério Machado de Almeida
Diretor da Coordenadoria de Apoio aos Serviços de TIC (CASTIC)	Sr. Alexandre Gomes Barriento
Diretor da Coordenadoria de Infraestrutura de TIC (CITIC)	Sr. Cristiano Munerati
Diretor da Coordenadoria de Sistemas de TIC (CSISTIC)	Sr. Hudson Lincoln Gomes dos Santos
Diretora da Secretaria da Ouvidoria	Sra. Claudia Polachini Kayatt

Convidados(as)	
Servidor da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)	Ramon Chiara
Servidor com lotação na Coordenadoria de Segurança de TIC (CSTIC)	Renato Monteiro Selmer

3. Pauta

Item	Assunto
I	Uso de Dropbox, OneDrive e soluções similares
II	Plano de Gestão e Comunicação de Incidentes Cibernéticos
III	Migração da solução de Firewall
IV	Registro de acessos à Internet em equipamentos corporativos fora da rede do TRT
(Extra pauta)	Incidente cibernético

4. Breve relato

I. Uso de Dropbox, OneDrive e soluções similares

Após iniciada a reunião pela Vice-coordenadora do Comitê, a SETIC explanou acerca da necessidade de validação sobre a utilização de soluções como Dropbox, OneDrive, e similares, nos equipamentos corporativos, considerando as funcionalidades e garantias contratuais presentes na solução contratada de correio eletrônico/colaboração.

Foi esclarecido que o assunto já havia sido discutido em composições anteriores do Comitê, e o entendimento foi de que o uso desse tipo de solução não deveria ser liberado.

Com o passar do tempo, algumas dessas soluções passaram a não exigir mais permissões administrativas para sua instalação, possibilitando a instalação pelo próprio usuário e há conhecimento que usuários utilizam essas soluções tanto para o armazenamento de arquivos

corporativos quanto de arquivos pessoais, situação que implica em riscos adicionais ao uso dessas soluções. Por exemplo, já foi noticiado vazamento de dados da ferramenta Dropbox há alguns anos atrás. E, quanto mais soluções forem instaladas nos equipamentos, maior a probabilidade de alguma falha ou vulnerabilidade ser identificada e explorada, aumentando o risco na utilização dessas soluções.

Foi ressaltado que a contratação do Google Workspace visa atender às demandas corporativas de armazenamento de arquivos e que não há suporte para outras ferramentas similares, cujas licenças são particulares e não contratadas pelo Tribunal. Também foi esclarecido que tais soluções podem continuar a serem utilizadas pelos usuários por meio do navegador Web mesmo sem o cliente instalado nos equipamentos.

A SETIC indicou a necessidade de promoção de campanhas informativas relativas à utilização do Google Drive, considerando que informações corporativas devem ser mantidas em ferramentas corporativas e que informações particulares não devem ser mantidas em tais ferramentas. Conforme levantamento realizado, há aproximadamente 400 máquinas corporativas que possuem o Dropbox instalado.

Após ampla discussão e votação, o CSIPDP decidiu pelo bloqueio futuro da instalação e uso do aplicativo Dropbox e similares, permanecendo liberado o uso via navegador Web, estabelecendo que devem ser promovidas campanhas prévias na Intranet para utilização da ferramenta contratada pelo Tribunal, incluindo avisos e orientações para que os usuários que fazem uso de outras soluções passem a utilizar o Google Drive, eventualmente utilizando o suporte do Service Desk e informando os usuários acerca da data limite para a migração.

Com relação ao uso do OneDrive, cuja utilização possui particularidades técnicas distintas, por se tratar de uma ferramenta com integração ao MS-Office, disponibilizado para parte dos usuários do TRT, ficou decidido que será efetuada análise mais aprofundada para a desativação desta ferramenta, e os resultados desta análise devem ser tratados na próxima reunião do Comitê.

II. Plano de Gestão e Comunicação de Incidentes Cibernéticos

Foi apresentado ao Comitê, o “Plano de Gestão e Comunicação de Incidentes Cibernéticos”, artefato do processo de “Gestão de Incidentes Cibernéticos”.

Foi apresentada a estrutura macro do plano, com esclarecimentos dos termos técnicos contidos nos tópicos do documento, tais como: definição de incidentes cibernéticos; categorização dos tipos de incidentes tratados, sua respectiva definição e “playbook” associado; cálculo da criticidade de um incidente, o qual é registrado em relatórios compartilhados mensalmente; quando e para quem são comunicados esses incidentes, conforme cada caso e definições da ENSEC; e quais são os relatórios a serem enviados trimestralmente para o CSIPDP.

Adicionalmente, foi esclarecido o conceito de “playbook”, que se trata de um documento que estabelece procedimentos a serem realizados em caso de incidentes específicos, sendo um

roteiro (script) de ações a serem tomadas quando necessário. Alguns desses artefatos já estão estabelecidos, outros estão em revisão.

A SETIC esclareceu que o Plano de Gestão e Comunicação de Incidentes Cibernéticos está em revisão pelo Comitê de Gestão de TIC (CGTIC) e será posteriormente submetido ao CSIPDP para avaliação.

O CSIPDP autorizou que, após aprovação pelo CGTIC, a SETIC poderá enviar nova versão do documento para aprovação via FRAD. Neste sentido, observações poderão ser encaminhadas por meio de e-mail e eventuais dúvidas também poderão ser pautadas na próxima reunião do Comitê.

III. Migração da solução de Firewall

A SETIC informou ao Comitê a respeito da migração da solução de Firewall, contextualizando o histórico da transição entre a contratação anterior (Checkpoint) e a atual contratação (Palo Alto), as quais se tratam de duas entre as três maiores fornecedoras deste tipo de equipamento.

Em que pese se tratar de procedimento complexo, foi observado que não houve impactos relevantes na migração e a pequena série de incidentes identificados foi rapidamente contornada.

Adicionalmente, o Comitê foi informado sobre a migração da VPN, acerca da qual será adotado o mesmo procedimento da migração da ferramenta anterior (Cisco) para a atual, com a distribuição dos novos pacotes de instalação e migração gradual entre as soluções.

Com relação ao filtro de conteúdo, o Comitê foi questionado se seria necessário revisar regra de acesso vigente de forma completa ou com foco apenas nas novas categorias, bem como se o assunto poderia ser enviado para aprovação via FRAD.

Após discussão, o Comitê decidiu que é adequado revisar as duas maiores políticas de acesso, referentes ao acesso geral dos usuários e o acesso ampliado dos Magistrados, com o encaminhamento da relação dessas informações por e-mail, para posterior discussão do assunto na próxima reunião do CSIPDP.

IV. Registro de acessos à Internet em equipamentos corporativos fora da rede do TRT

A SETIC esclareceu que é previsto, pela ENSEC, o controle “Habilitar log de pesquisas sobre Domain Name System (DNS) de forma a detectar buscas por nomes de hosts em domínios reconhecidamente maliciosos”.

Atualmente, este controle é viável de atendimento, entretanto, caso seja habilitado este log, seriam registrados, inclusive, acessos à internet realizados fora do horário de trabalho e fora da VPN. Este registro seria armazenado localmente em cada ativo e poderia ser utilizado em caso de investigação ou necessidade de levantamento de informações.

Foi esclarecido, ainda, que existe a possibilidade de que a ativação deste controle possa causar alguma lentidão na utilização destes dispositivos.

A SETIC ressaltou que os acessos à internet realizados a partir das dependências do TRT já possuem a prerrogativa de serem monitorados, e que este monitoramento pode facilitar a rastreabilidade das ações praticadas no equipamento em cenários específicos, como auditorias e investigações forenses, não se tratando de monitoramento antecipado, mas apenas de registro para resgate eventual, mediante autorização específica.

Após ampla discussão, houve consenso no entendimento de que a aplicação desse controle requer divulgação ampla e ficou decidido que a SETIC realizará piloto para análise de impacto no desempenho dos equipamentos após esta ativação, com os resultados deste piloto sendo pautados para decisão do Comitê sobre sua aplicação.

(Extra-Pauta) Incidente cibernético

Dra. Roberta comunicou ao Comitê sobre determinado incidente cibernético ocorrido.

Foi esclarecido que existem procedimentos estabelecidos que não foram seguidos e que o caso foi reportado à Polícia Federal. Também foi indicado que a Presidência do Tribunal comunicaria formalmente aos magistrados a respeito deste incidente.

Para minimizar a probabilidade de repetição de eventos desta natureza, foram informadas as medidas adotadas.

5. Deliberações

Descrição	Responsável pelo cumprimento
Promover campanhas informativas na Intranet, relativas à utilização do Google Drive, incluindo avisos e orientações para que os usuários que fazem uso de outras soluções passem a utilizar o Google Drive.	SETIC/SECOM
Realizar análise aprofundada específica referente ao bloqueio da ferramenta OneDrive.	SETIC
Após aprovação pelo CGTIC, enviar nova versão do Plano de Gestão e Comunicação de Incidentes Cibernéticos para aprovação, via FRAD, pelo CSIPDP.	SETIC
Encaminhar a relação das regras relativas ao filtro de conteúdo por e-mail, para posterior discussão do assunto na próxima reunião do Comitê.	SETIC
Realizar projeto piloto nas máquinas da SETIC para análise do impacto de performance referente ao registro de acessos	SETIC

à Internet em equipamentos corporativos fora da rede do TRT, para posterior avaliação dos resultados pelo Comitê.	
Promover novas campanhas de conscientização aos usuários, a fim de reforçar a importância do acompanhamento das ações do técnico durante a realização do backup de dados dos equipamentos, utilização dos serviços de armazenamento contratados pelo Tribunal e da separação de arquivos pessoais e corporativos.	SETIC/SECOM

6. Próxima reunião

Data: 04/04/2024 às 16:00.

7. Assinatura da coordenadora do colegiado