	PODER JUDICIÁRIO DO ESTADO DO RIO DE JANEIRO **SECRETARIA GERAL DE ADMINISTRAÇÃO (SGADM)** **DEPARTAMENTO DE APOIO AOS ÓRGÃOS COLEGIADOS ADMINISTRATIVOS (DEACO)** **DIVISÃO DE APOIO TÉCNICO E ADMINISTRATIVO (DICOL)** **SERVIÇO DE APOIO TÉCNICO AOS ÓRGÃOS COLEGIADOS ADMINISTRATIVOS PERMANENTES (SEAPE)**

Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro (CGSI)		**Ata de Reunião nº 02/2024**
Data: 04/03/2023	**Horário: 14h**	**Local: Sala 01 da SGADM**

Presentes na reunião, realizada de forma presencial, os seguintes participantes:

Des. **Marcos André Chut**, Presidente do Comitê;
Juiz **Alberto Republicano de Macedo Júnior**, Auxiliar da Presidência e Coordenador;
Juíza **Daniela Bandeira de Freitas**, Auxiliar da Corregedoria-Geral de Justiça;
Juiz **Ricardo Lafayette Campos**;
Sr. **Daniel de Lima Haab**, Secretário-Geral da SGTEC;
Sra. **Aline Cabral Muniz**, Diretora do Departamento de Segurança da Informação (DESEG);
Sr. **Jorge Luiz Monteiro Rodrigues**, representante da Secretaria-Geral de Segurança Institucional com especialidade em segurança física;
Sra. **Virna Amorim**, representante da SGTEC/DEATE;
Sr. **Wagner da Silva Andrade Júnior**, representante da SGSEI;
Sr. **Vitor da Luz Telles**, representante da SGGIC;
Sr. **Guilherme Rukuiza Czekay**, representante da SGTEC;
Sr. **Luiz Cláudio de Azevedo Chaves**, representante da SGTEC;
Sr. **Bruno Brasil Soares**, representante da SGTEC.
Sra. **Renata Bricio Vianna**, representante da SGTEC; e
Sra. **Renata Alves Damasco**, representante da Corregedoria-Geral da Justiça.
Sr. **Tomaz Gaio Soriano**, representante da SGTEC.

O Des. **Marcos André Chut**, Presidente do Comitê de Governança de Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro (CGSI), agradece a presença de todos e inicia os trabalhos às 14h05. Justificadas as ausências do Dr. **João Felipe Nunes Ferreira Mourão** e da Dra. **Criscia Curty de Freitas Lopes**. Em seguida, a palavra é concedida à Diretora do Departamento de Segurança da Informação, **Sra. Aline Cabral Muniz**.

1- Apresentação do Relatório do Departamento de Segurança da Informação;

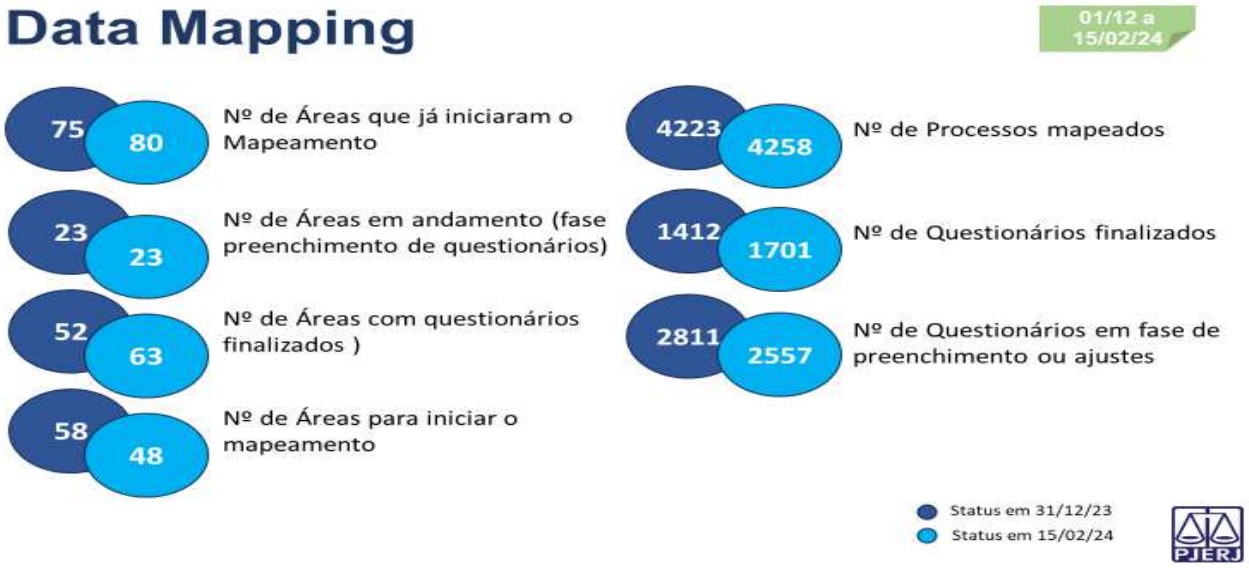
Sra. Aline Cabral Muniz inicia a apresentação expondo o desenvolvimento das atividades do DESEG (Departamento de Segurança da Informação) no período de 01/01/2024 a 15/02/2024. A respeito da defesa cibernética, explicita que foram detectados 8.755 alertas que geraram 503 investigações para possíveis incidentes. Houve 933 ações de resposta autônoma sugeridas pela Inteligência Artificial e 1 ação de resposta executada pela plataforma para impedir um ataque cibernético. Acrescenta que a ferramenta que gera esses alertas é a *Darktrace*.

Sobre esse tópico, **Sr. Guilherme Czekay** questiona se efetuaram algum levantamento para avaliar se ocorreram casos recorrentes nesses incidentes cibernéticos e se houve algum ataque com nível de criticidade alto. **Sra**. **Aline Muniz** responde que essa ameaça cibernética foi considerada de alta criticidade. Informa ainda que 503 investigações também são tratadas como críticas.

Em seguida, comenta sobre monitoramento de marcas. Relata que desses 25 tickets criados para investigações, análise e ação de resposta 04 são de aplicação mobile; 19 de uso indevido da marca e 02 são classificados como outros motivos.

Sra. **Aline Muniz** apresenta exemplos de situações de uso indevido da marca do TJRJ e que foram retirados do ar. Sobre o tema, **Dr. Alberto Republicano** propõe que seja criada uma política de casos que devam ser levados à delegacia especializada.

Em resposta, a **Diretora do DESEG** esclarece que essas situações acontecem diariamente. Acrescenta que o modelo de tratamento de *phishing* foi modificado para tratar, também, dos casos de crime.



Sra. Aline Muniz comunica que houve progresso no mapeamento de dados. Em seguida, apresenta setores que não concluíram ou não iniciaram o preenchimento do questionário (páginas 8, 9 e 10 da apresentação do PowerPoint, em anexo). Ressalta que o DESEG está em contato, semanalmente, com os setores e que foram realizados workshops e reuniões para auxiliá-los neste trabalho.

Dando continuidade, **Sra**. **Aline Muniz** descreve o mapeamento dos Departamentos e Divisões e o número de processos finalizados, atrasados e que ainda vão iniciar.

Sobre o Serviço de Gestão de Vulnerabilidades, que funciona 24 horas nos softwares, informa que, no período em análise, foram identificadas 371 vulnerabilidades, sendo que 74 estão em tratamento (20%) e 297 (80%) já foram resolvidas.

Segurança de Aplicações

01/01 a 15/02/24

- Scans diários em aplicações Web em homologação (entre 00:10 e 07:30 - total de 10 aplicações) a fim de identificar e corrigir vulnerabilidades antes da liberação para produção.

- Alteração da rotina de scan de ativos de infraestrutura para melhoria do indicador no Security Scorecard (de quinzenal para semanal - Terças e Quartas) – Jan/24 – DESEG x DETIC-DISER

A **Diretora do DESEG** relata que foram identificadas 156 aplicações do TJRJ que utilizam o protocolo HTTP, considerado não seguro e sem criptografia. Ressalta que foi criado um Grupo de Trabalho composto por gestores de aplicações e a fábrica de software que realiza reuniões semanais para a atualização destas aplicações para HTTPS.

Sobre o Múltiplo Fator de Autenticação, comunica que foi implementado para 711 usuários e que considera necessária a realização de uma revisão do controle de acessos para melhorar a gestão de acesso ao TJRJ como um todo.

A respeito do tema, Sr. **Daniel Haab** sugere que sejam verificados os números do Múltiplo Fator de Autenticação por tipo de integrantes do tribunal com o percentual de desembargadores, juízes, servidores e terceirizados com a finalidade de melhor enfocar as políticas de reforço de necessidades do MFA.

Certificados Digitais SSL

- Identificado o uso de cerca de **53** certificados gratuitos (let´s encrypt) que possui diversas vulnerabilidades que podem ser exploradas. O uso desses certificados deve ser evitado, por conta dos riscos envolvidos, principalmente para serviços "expostos" à internet;

- Projeto de atualização e adequação dos certificados SSL em andamento com o DETIC-DISER.
- Reativação da certificadora Microsoft interna a fim de trazer maior segurança as aplicações internas e evitar custos adicionais;
  - ➢ Instalação de certificados confiáveis emitidos por certificadoras ICP-Brasil em todos os serviços que estão expostos para a internet.

70 revisados

PJERJ

Sobre os Certificados Digitais, **Sra. Aline Muniz** explica que a maioria dos sites utilizava certificado digital gerado por uma empresa, chamados de *Let's encrypt*. Esclarece que são certificados gratuitos e possuem diversas vulnerabilidades. Comenta que foi realizada uma reunião com o DETIC-DISER e identificado o número de 70 certificados que estão sendo revisados. Nesse momento, estão sendo emitidos novos certificados pela ICP-Brasil, nos serviços expostos à internet.

Programa Permanente de Segurança da Informação

- Mudança do procedimentos para tratamento de incidente de Phishing

Dando continuidade à apresentação, a **Sra. Aline Muniz** frisa que houve uma mudança de procedimentos para tratamento de incidentes de *phishing*. Foi elaborada uma retificação da campanha e criação de um canal de atendimento. Acrescenta que essa campanha foi publicada no *Teams*, nos Sistemas Judiciais e no Sistema SEI.

A respeito do tema, **Dr. Alberto Republicano** propõe que seja solicitada ao DECOI (Departamento de Comunicação Interna) a publicação de uma notícia sobre o Programa de Segurança da Informação e divulgando a existência desse canal direto com o DESEG. **(Deliberação 1)**

Sobre o nível de exposição do ambiente, a **Diretora do DESEG** menciona notícia sobre o aumento de ataques cibernéticos contra os órgãos do governo. Ressalta que o número de exposição do TJRJ é 322, enquanto os outros órgãos governamentais estão com o número de 400. Explica que o critério de aferição dessa métrica é feito com base em todas as vulnerabilidades.

Incidente nas Redes Sociais do TJRJ

01/01 a 15/02/24

Publicações que ocorreram em 06/02 e 07/02

Ações tomadas:

- ✓ Orientações iniciais ao serviço de redes sociais;
- ✓ Solicitação de logs a mlabs;
- ✓ Solicitação de logs de acesso as redes sociais do Tribunal;
- ✓ Parecer técnico e notificação enviada para empresa;
- ✓ Relatório final (em desenvolvimento).

Nesse momento, **Sra. Aline Muniz** comenta sobre o vazamento ocorrido no dia 23 de janeiro de 2023, considerado o maior vazamento de dados da história, inicialmente, sem dados do TJRJ.

Comenta que, nos dias 06 e 07 de fevereiro do ano de 2024, aconteceram publicações não oficiais nas redes sociais do TJRJ. Foi verificado que o usuário usava a credencial pessoal para fazer gestão das redes sociais do Tribunal. Informa que foi feito contato com o usuário e sua equipe, incluindo o Diretor de Departamento, no sentido de

passar todas as orientações pertinentes. Por fim, comunica que essa investigação ainda não foi concluída.

Sr. Daniel Haab sugere a apresentação do mapeamento, mais específico, da quantidade de tentativa de exploração de vulnerabilidades que acontecem a cada período e que são defendidas. Explica a importância da Instituição entender o quanto isso é um grande e permanente problema, mas que existe defesa, e que o contrato com a *Cyber* Segurança se justifica diante dessa repetição intensa de ataques, diariamente defendidos.

2- Processo SEI 2024-06008580 - Alteração da Resolução TJ/OE nº05/2019 - Política de Segurança da Informação (PSI);

A respeito desse tema, a Comissão delibera pela abertura de Plenário Virtual para melhor análise da questão. **(Deliberação 2)**

3- Processo SEI 2024-0602195: Validação de documentos no PJE que permitia aos usuários que possuem acesso *jus postulandi*, cadastrar uma petição inicial e gerar um *hash* de validação, mesmo que o documento não esteja vinculado a um processo:

Grupo é preso em SP após se passar por juiz e falsificar sentenças da Justiça do Rio de Janeiro | São Paulo | G1 (globo.com)

Sobre o processo SEI 2024-06021295, **Sra. Aline Muniz** relata que o DESEG identificou o incidente cibernético como uma falha processual. Explica que qualquer usuário, em posse de um certificado digital, consegue criar um perfil no Sistema PJe *Jus Postulandi*, cadastrar uma petição inicial e gerar um *hash* de validação, mesmo que o documento não esteja vinculado a um processo. A equipe responsável lançou uma Revisão de Mudança Emergencial e fez uma correção dessa falha processual. A investigação ainda está em andamento.

4- Deliberações em Andamento:

Ata nº. 03/2023 Del. 03: **Realizar consulta junto aos magistrados e servidores providos com a possibilidade de acesso às redes sociais, para manifestarem, no prazo de 30 dias, o interesse na manutenção do acesso, com a devida justificativa, à luz do Ato Normativo TJ, 27/2020.**

Dr. Alberto Republicano explica que existe um relatório com 1.072 personagens do TJRJ com acesso às redes sociais. Dentre esses, estão desembargadores, juízes, funcionários de órgãos da Administração da Justiça, além de 5 estagiários. Assim, sugere a reformulação da presente deliberação para que os juízes, desembargadores e aqueles que integram a SGTEC, DGCOM, SGSEI e Gabinete da Presidência permaneçam com acesso às redes sociais e que seja instaurado um processo SEI com a finalidade de encaminhar um memorando aos demais que constam no relatório para que se manifestem e se justifiquem sobre a manutenção do acesso às redes sociais, no prazo de 30 dias. **(Deliberação 3)**

Ata nº. 03/2023 Del. 04: Realização de campanha de conscientização sobre segurança da informação por meio de conteúdo divulgado em películas pedagógicas.

Dr. Alberto Republicano informa que já foi feita a campanha do *Phishing* e que a próxima será do *Malware*, estando, portanto, essa deliberação cumprida.

O Presidente do Comitê agenda nova reunião do CGSI para o dia 08 de abril de 2024, às 14h. (**Deliberação 04**)

O Des. **Marcos André Chut** agradece a presença de todos e encerra a reunião às 15h15.

Des. **MARCOS ANDRÉ CHUT**

Presidente do CGSI

	DELIBERAÇÕES	RESPONSÁVEL	PRAZO
01	Solicitar ao DECOI (Departamento de Comunicação Interna) a publicação de uma notícia sobre o Programa de Segurança da Informação e divulgando a existência desse canal direto com o DESEG.	DESEG	5 dias
02	Promover Plenário Virtual sobre Processo SEI 2024-06008580 - Alteração da Resolução TJ/OE nº05/2019 - Política de Segurança da Informação (PSI) para análise dos membros da minuta de resolução;	SEAPE	Imediatamente, após aprovação da ata
03	Instaurar um processo SEI com a finalidade de encaminhar um memorando aos personagens do TJRJ, excetuando magistrados e aqueles que integram a SGTEC, DGCOM, SGSEI e Gabinete da Presidência, para que se manifestem e se justifiquem sobre a manutenção do acesso às redes sociais, no prazo de 30 dias.	SGTEC	5 dias

04	Enviar convite aos membros do CGSI para a reunião do Colegiado, designada para o dia 08/04/2024, às 14h.	SEAPE	Imediatamente, após aprovação da ata.

Deliberações Encerradas		Ata de Origem	Razão
01	Realizar consulta junto aos magistrados e servidores providos com a possibilidade de acesso às redes sociais, para manifestarem, no prazo de 30 dias, o interesse na manutenção do acesso, com a devida justificativa, à luz do Ato Normativo TJ, 27/2020.	Ata nº 03/2023	Perda de Objeto / Alterada para deliberação 03
02	Realização de campanha de conscientização sobre segurança da informação por meio de conteúdo divulgado em películas pedagógicas.	Ata nº 03/2023	Cumprida