



PODER JUDICIÁRIO  
**TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO**  
Divisão de Segurança da Informação

**Comitê de Segurança da Informação e Proteção de Dados**  
**Relatório de Entregas – 2023**

## **1. Política de Segurança da Informação**

**Atualização da POSIC:** Deliberou-se pela revisão da Política de Segurança da Informação e Comunicação, com foco na reestruturação da Equipe de Tratamento e Resposta a Incidentes (ETIR). A nova redação institucionaliza a designação de uma equipe fixa e a obrigatoriedade de reuniões periódicas para o tratamento de temas correlatos.

**Conformidade com Auditoria:** Como resposta direta às recomendações da auditoria coordenada pelo CSJT, foi incluída na norma a regulamentação sobre a publicação de serviços, suprimindo lacuna identificada pelos órgãos de controle.

## **2. Estratégia**

**Infraestrutura e Defesa Tecnológica:** Consolidação de investimentos estratégicos voltados à redução da superfície de ataque.

**Monitoramento de Vulnerabilidades:** Conclusão da implantação de ferramenta adquirida. Apresentação de painéis e gráficos técnicos nas reuniões do Comitê para acompanhamento dinâmico dos índices de exposição a ameaças.

**Auditoria TCU:** Acompanhamento dos trabalhos da auditoria do TCU voltada ao exame da implementação dos controles do framework CIS Controls, conforme as exigências da Portaria 162/2021 do CNJ.

**Alinhamento Institucional:** Registro da ciência do Comitê quanto à participação da Secretaria de Auditoria (SEAUD) nas reuniões deliberativas, visando o fortalecimento do controle interno e da transparência.

**Índice de Conformidade (ICPPDU-CSJT):** O Tribunal atingiu o nível "Aprimoramento" na meta 2023-2024, alcançando pontuação máxima em três das sete dimensões avaliadas pelo Conselho Superior da Justiça do Trabalho.



PODER JUDICIÁRIO  
**TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO**  
Divisão de Segurança da Informação

### **3. Adequação à LGPD (Proteção de Dados)**

**Privacidade por Concepção (Privacy by Design):** Instituição de projeto junto à área de sistemas para adoção de metodologia de desenvolvimento seguro na esteira de produção de software do Tribunal.

**Rastreabilidade e Inventário:** Elaboração de formulário para mapeamento dos processos de tratamento de dados pessoais. Para viabilizar a coleta fidedigna, determinou-se o nivelamento de conceitos (definição técnica de "coleta" e "tratamento") entre as áreas gestoras.

**Segurança Jurídica no Compartilhamento:** Decidiu-se pela adoção e publicação, no Portal da LGPD, do Guia Orientativo da ANPD, visando padronizar e conferir lastro jurídico ao repasse de informações a entes públicos.

**Dimensão Governança:** Inclusão do Programa Institucional de Privacidade de Dados no plano de comunicação anual da SECOM. Deliberou-se pela elaboração do Relatório de Impacto à Privacidade de Dados (RIPD) como ferramenta essencial para a verificação de riscos.

### **4. Cultura em Segurança da informação**

**Gestão de Identidades:** Implementação da campanha de Senha Forte, com monitoramento semanal da evolução das contas. A ação mitigou o risco de vazamento de credenciais — identificado como o principal vetor de exploração de vulnerabilidades no ambiente — sem gerar impactos operacionais na Central de Serviços.

**Capacitação Especializada:** Autorização para a contratação de treinamento técnico específico voltado aos integrantes da ETIR, visando ao aprimoramento da capacidade de resposta a incidentes críticos de segurança da informação.