TRT-16ª REGIÃO

Sec. de Tecnologia da Informação e Comunicação

PLANO DE CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO 2026

MAIO/2026

SUMÁRIO

1. APRESENTAÇÃO

Este documento tem como finalidade apresentar as ações propostas para o ano de 2026 no âmbito do **Plano de Conscientização e Treinamento em Segurança da Informação e Comunicação**, elaborado pelo Setor de Apoio à Segurança da Informação, em conformidade com o **Ato GP nº 01/2019,** a nova Política de Segurança da Informação e Comunicações (POSIC), instituída pela **Resolução Administrativa TRT16 nº 026/2024** e com a **Estratégia Nacional de Segurança Cibernética do Poder Judiciário** (ENSEC-PJ).

O plano tem como objetivo fomentar uma cultura organizacional voltada à segurança da informação e à proteção de dados pessoais, por meio da prevenção de incidentes, disseminação de boas práticas e promoção da conformidade com as normas internas e a Lei Geral de Proteção de Dados (LGPD). Busca-se capacitar magistrados, servidores, estagiários e colaboradores terceirizados de ambas as instâncias quanto aos riscos e ameaças que envolvem o manuseio de informações, destacando a importância da proteção desses ativos para evitar fraudes e prejuízos à imagem institucional do Tribunal Regional do Trabalho da 16ª Região perante a sociedade.

Ressalta-se que a segurança da informação não se limita apenas ao ambiente digital; por esse motivo, o cronograma prevê ações mensais de maio a novembro (excetuando-se julho e dezembro) que contemplam situações cotidianas que podem representar riscos ao sigilo e à integridade das informações, integrando as diretrizes da POSIC e das normas complementares de uso de recursos de TIC, internet e correio eletrônico.

A elaboração deste plano atende também às recomendações de auditoria relativas à LGPD, destinadas às áreas administrativas e judiciais, fundamentando-se nas diretrizes de órgãos de controle e fontes especializadas, tais como:

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br);
- Internet Segura;
- Center for Internet Security (CIS);

- Conselho Nacional de Justiça (CNJ).
- Computer Security Resource Center;
- Antispam.br.

2. DA ESTRUTURA DO PLANO

Este plano está estruturado em formato de tabela em que na primeira coluna tem-se o mês previsto da ação; na segunda, a descrição resumida da atividade; na terceira, o público-alvo.

3. DO PLANEJAMENTO PARA 2026

Mês	Atividade	Público Alvo
Maio	• Trabalho Remoto: Trabalhe de forma segura; • LGPD: O que são dados pessoais e o papel de cada usuário no tratamento seguro.	Magistrados, Servidores, Estagiários e Terceirizados.
Junho	• Uso do Correio Eletrônico: Regras de segurança, verificação de procedência de anexos e uso de CCO; • Direitos dos Titulares (LGPD): Como a segurança da senha protege a privacidade dos dados do cidadão.	Magistrados, Servidores, Estagiários e Terceirizados.
Agosto	• Phishing e E-mail Spoofing: Como identificar mensagens falsas e proteger a rede; • Princípio da Finalidade: Uso de dados e recursos apenas para o	Magistrados, Servidores, Estagiários e Terceirizados.

	estrito cumprimento das funções laborais.	
Setembro	• Uso de Internet: Regras para navegação segura e finalidades permitidas no tribunal; • LGPD: Tratamento de dados sensíveis e anonimização	Magistrados, Servidores, Estagiários e Terceirizados.
Outubro	• Vazamento de Credenciais: Importância de senhas fortes e uso de certificado digital; • Ciclo de Vida do Dado: Coleta, armazenamento e descarte seguro para evitar infecções por malware.	Magistrados, Servidores, Estagiários e Terceirizados.
Novembro	• Acesso e Equipamentos: Responsabilidade sobre senhas, uso de biometria e guarda de certificados; • Resposta a Incidentes de dados pessoais: O fluxo de comunicação ao encarregado de dados e à Seção de Segurança em caso de vazamento.	Magistrados, Servidores, Estagiários e Terceirizados.