TRT 15ª REGIÃO

Secretaria de Tecnologia da Informação e Comunicações

PROPOSTA
Protocolo para Investigação de Ilícitos Cibernéticos (PIILC-TRT15)

1 Objetivo

Este protocolo estabelece os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal. Para tal, promove adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética, bem como define requisitos para adequação dos ativos de tecnologia da informação referente à configuração e ao registro de informações de auditoria;

2 Abrangência

O protocolo tem abrangência em todo o Tribunal Regional do Trabalho da 15ª Região.

3 Referências legais e normativas

Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 21/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

Resolução Administrativa nº 023/2018, de 14 de dezembro de 2018, que dispõe sobre a Gestão de Segurança da Informação (GSI) no âmbito deste Tribunal, conduzida pelo Comitê de Governança de Segurança da Informação (CGSI).

Resolução CNJ 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança

Cibernética do Poder Judiciário (ENSEC-PJ).

Portaria GP nº 032/2022, de 8 de fevereiro de 2022, que institui e designa os membros do Comitê Gestor de Crises do Tribunal Regional do Trabalho para apoio à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

4 Diretrizes

4.1 Disposições gerais

4.1.1 A implementação do Protocolo de Investigação de Ilícitos Cibernéticos (PIILC-TRT15) deverá ser realizada de maneira progressiva, controlada, prévia e amplamente divulgada aos usuários visando o menor impacto para o ambiente de TIC da Instituição.

4.1.2 Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo de Gestão de Crises Cibernéticas.

4.1.3 As ações deste protocolo são complementares às políticas, às normas, aos processos de trabalho, às práticas e aos procedimentos relacionados à Segurança da Informação do TRT15.

4.1.4 A estrutura de Segurança da Informação presente na Resolução Administrativa nº 023/2018 embasa este protocolo.

4.2 Configurar os Ativos de TIC para o registro de informações de rastreamento

4.2.1 Os ativos de TIC do Tribunal (ex.: estações de trabalho, servidores, serviços, sistemas, dentre outros) devem:

- estar configurados de acordo com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);
- estar configurados de forma a registrar o máximo possível de eventos relevantes de Segurança da Informação, bem como de informações que possibilitem a depuração de incidentes e de problemas;
- registrar, sempre que possível, as seguintes informações: identificação inequívoca do usuário que acessou o recurso; natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.; data, hora e fuso horário, observando-se a HLB; e endereço IP (Internet Protocol), porta de origem da conexão, identificador do ativo de informação e demais informações que possibilitem identificar a origem do evento;;

4.2.2 O armazenamento dos registros de auditoria deve ser realizado remotamente (e não apenas localmente), por meio do uso de tecnologia aplicável, para, ao menos, os ativos tecnológicos considerados críticos.

4.3 Coletar e preservar evidências

4.3.1 A investigação do ilícito cibernético deve ser realizada de acordo com as normas estabelecidas na Política de Segurança da Informação vigente, especificamente no tocante ao assunto de gestão de incidentes de Segurança da Informação e à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

4.3.2 Os incidentes de segurança cibernética devem ser registrados conforme Processo de Trabalho de Gestão de Incidentes de Segurança Cibernética.

4.3.3 Caso seja necessária coleta de evidências, essa deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.

4.3.4 Se o incidente de segurança envolver a suspeita de crime, os órgãos competentes devem ser acionados, nos termos da legislação vigente.

4.4 Revisão e aprimoramento

4.4.1 Este documento deve ser revisado anualmente ou a qualquer momento em caso de necessidade detectada.