TRT 15ª REGIÃO

Secretaria de Tecnologia da Informação e Comunicações

PROPOSTA
Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-TRT15)

1 Objetivo

Este protocolo tem como objetivo estabelecer diretrizes para a prevenção de incidentes cibernéticos, de forma a promover alinhamento às regulamentações, normas e melhores práticas relacionadas à Segurança Cibernética. O resultado definido é, assim, estabelecer os meios para ações de prevenção e resiliência aos incidentes cibernéticos.

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).

4 Diretrizes

4.1 Disposições gerais

4.1.1 A implementação do Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-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 Gerenciamento de Crises Cibernéticas e o Protocolo para Investigação de Ilícitos Cibernéticos.

4.1.3 Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos

4.1.4 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.

4.1.5 A estrutura para a Gestão de Segurança da Informação no âmbito do TRT15 definida na Resolução Administrativa nº 023/2018 possui diretrizes para as funções definidas neste protocolo.

4.1.6 Os principais atores envolvidos na prevenção a incidentes cibernéticos são:

- Comitê Gestor de Governança da Segurança da Informação (CGSI);
- Secretaria de Tecnologia da Informação e Comunicações;
- Escola Judicial;
- Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)**;**

4.1.7 Com base na ENSEC-PJ, as funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar.

4.2 Identificar

4.2.1 A função identificar consiste em atividades para identificar ativos tecnológicos críticos, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade.

4.2.2 Essa atribuição é contemplada na Gestão de Riscos do TRT15, que contempla a Gestão de Riscos de TIC, cujo conteúdo e modo de operação se encontra na página específica na do TRT15 (na página encontrada na intranet do TRT15, em “Aplicações da Intranet / Sistemas Administrativos / Comitês e Comissões / Comitê de Gestão de Riscos”).

4.3 Proteger

4.3.1 A função *proteger* consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados, além de contribuir para a eficiência e eficácia da prestação de serviços. No TRT15 realiza-se tal função com as atividades descritas abaixo:

- Execução da Gestão de Segurança da Informação (GSI) do TRT15;
- Plano de Gestão de Continuidade de TIC;
- Processos de Trabalho de Gerenciamento da Disponibilidade, Gerenciamento de Capacidade de TIC, Gerenciamento de Mudança e Gerenciamento Liberação de Serviços;
- Aplicação da normatização de Segurança da Informação (na página encontrada na intranet do TRT15, em “Aplicações da Intranet / Sistemas Administrativos / Comitês e Comissões / Comitê de Governança de Segurança da Informação (CGSI)”);
- Realização de cópias de segurança do ambiente tecnológico, conforme norma técnica complementar estabelecida pela PORTARIA GP nº 061/2019;
- Implementação de boas práticas de gerenciamento e proteção do ambiente tecnológico, observando normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002 e CIS Controls), tais como:
    - Gerenciamento de vulnerabilidades;
    - Implementação de soluções de segurança do ambiente (firewall, IPS, filtro de conteúdo web, proteção de endpoint, detecção e resposta de endpoint, dentre outras);
    - Hardening de serviços e de sistemas;
- Adequação gradual, observando a especificidade do ambiente no TRT15 em relação à segurança cibernética, aos seguintes Manuais de Referência da ENSEC-PJ: Proteção de Infraestruturas Críticas de TIC e Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital.

4.4 Detectar

4.4.1 A função detectar consiste no desenvolvimento e aplicação de medidas para identificação de eventos e/ou incidentes de segurança cibernética. No TRT15, tais medidas estão previstas no Processo de Trabalho de Tratamento de Incidentes Cibernéticos, bem como na rotina de monitoramento de ativos de TIC, executada pelas unidades responsáveis.

4.5 Responder

4.5.1 A função responder consiste na definição e implementação de medidas para responder com eficiência e eficácia a incidentes de segurança cibernética. No TRT15, tais medidas estão previstas no Processo de Trabalho de Tratamento de Incidentes Cibernéticos, bem como nas atribuições e estrutura definida para a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, formalizada pela portaria 30/2022 e definida pela portaria 31/2022

4.6 Recuperar

4.6.1 A função recuperar consiste no desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos quando da ocorrência de eventos e/ou incidentes de segurança cibernética, sendo contempladas no TRT15 pelas seguintes atividades:

- Processo de Trabalho de Tratamento de Incidentes Cibernéticos;
- Trabalho desenvolvido pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;
- Plano de Gestão de Continuidade de TIC.

4.7 Revisão e aprimoramento

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

.