1 Objetivo

Instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), grupo de servidores com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação em ambiente tecnológico.

2 Abrangência

Tratamento de incidentes de Segurança da Informação em ambiente tecnológico da Instituição.

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 Missão

A missão prioritária para a ETIR é a atividade de prevenção, tratamento e resposta a incidentes de segurança da informação de segurança cibernética, bem como o registro, coleta e preservação de evidências de incidentes de segurança cibernética e a comunicação às autoridades competentes.

5 Público Alvo

5.1 O público-alvo da ETIR são os usuários do ambiente tecnológico deste Tribunal.

5.2 A ETIR relaciona-se, internamente, com as diversas unidades da Secretaria de Tecnologia da Informação e Comunicações (SETIC), com o Comitê de Governança de Segurança da Informação e com o Comitê de Crise, considerando os termos do Protocolo de Gerenciamento de Incidentes e de Crises Cibernéticas, constante da Resolução CNJ 396/2021.

5.3 Externamente, a ETIR se relaciona com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cert.br e outros órgãos do Poder Judiciário Federal.

6 Modelo de Implementação

6.1 Estrutura

6.1.1 Enquanto não efetivado pelo Tribunal Regional do Trabalho da 15ª Região o Art. 21 da Resolução CNJ nº 396/2021, a ETIR estará temporariamente subordinada e deverá se reportar ao Comitê Gestor de TIC.

6.1.2 Para o desenvolvimento dos seus trabalhos, a ETIR poderá, sob supervisão e concordância do Comitê de Governança de Segurança da Informação (CGSI), solicitar informações, apoio e participação de toda e qualquer Unidade Administrativa deste Regional.

6.2 Atribuições do Comitê Gestor de TIC

6.2.1 O Comitê Gestor de TIC atua de forma gerencial e enquanto não efetivado pelo Tribunal Regional do Trabalho da 15ª Região o Art. 21 da Resolução CNJ nº 396/2021 temporariamente será o responsável por:

a) administrar as atividades determinadas e priorizadas pelo CGSI;

b) submeter ao CGSI, ações estratégicas para a ETIR, considerando estratégicas as que envolvem outras unidades além da SETIC e que atendam resoluções nacionais;

c) acompanhar a realização das atividades da ETIR, auxiliando e colaborando na resolução de problemas;

d) prestar contas das atividades da ETIR ao Comitê de Governança de Segurança da Informação (CGSI);

e) receber as sugestões de ações dos membros da ETIR, definir seu aceite e priorização, bem como, se necessário, seu encaminhando ao CGSI;

f) receber, aprovar, recusar, priorizar o pedido para participação da ETIR em relação aos processos de trabalho que envolvam Segurança da Informação;

6.2.2 Deverá ser elaborado, implantado e divulgado o Plano Anual de Capacitações da ETIR visando desenvolver e aprimorar as competências técnicas necessárias de seus componentes à operacionalização de suas funções e atribuições, permitindo manter atualizados os conhecimentos sobre o tema.

6.2.3 O Plano Anual de Capacitações da ETIR é parte integrante do Plano Anual de Capacitação da Instituição, devendo ser revisado semestralmente ou antes disso, se necessário, devendo constar do respectivo Processo de Trabalho do Plano de Capacitação Institucional.

6.2.4 Também devem ser promovidos, para os profissionais diretamente envolvidos na área de segurança cibernética, treinamentos contínuos e preparatórios que possibilitem a obtenção de Certificações Internacionais (certificações de TI são declarações formais emitidas por uma empresa que possua credibilidade, servindo para comprovar as habilidades de um determinado profissional sobre algum área de conhecimento tecnológico), certificações estas reconhecidas e válidas no mercado.

6.2.5 É atribuição do Comitê de Governança de Segurança da Informação promover a construção e revisões anuais do Plano Anual de Capacitações da ETIR, encaminhando e buscando as aprovações perante a Administração do TRT.

6.2.6 Enquanto não efetivado pelo Tribunal Regional do Trabalho da 15ª Região o Art. 21 da Resolução CNJ nº 396/2021, o monitoramento da execução do Plano de Capacitação dos membros da ETIR temporariamente será de responsabilidade do Comitê Gestor de TIC.

6.3 Atribuições da ETIR

6.3.1 Atuar diretamente ou colaborar em atividades que envolvam Segurança da Informação relacionada ao ambiente tecnológico, tais como: análise de ataques e intrusões, cooperação com outras equipes, inclusive de outros Tribunais e organizações, participação em fóruns e redes nacionais e internacionais relacionadas ao tema.

6.3.2 Dar apoio em atividades previstas em Processos de Trabalho que envolvam o tema Segurança da Informação, tais como Gestão de Incidentes de Segurança Cibernética, Gerenciamento de Mudanças, dentre outros.

6.3.3 Estabelecer, manter, revisar anualmente e aperfeiçoar quando necessário o Processo de Gestão de Incidentes de Segurança Cibernética, o qual deve ser formalmente instituído como norma de cumprimento obrigatório no prazo de 90 dias a partir da nomeação de seus membros componentes.

6.3.4 A ETIR, de forma colegiada ou por um de seus membros, exercerá o papel de Gestor de Serviço para os Serviços de TIC ofertados e diretamente relacionados com o tema de Incidentes de Segurança da Informação.

6.3.5 A equipe da ETIR será responsável por:

I. monitorar, receber e registrar eventos, elaborar relatórios de incidentes de segurança e alertas;

II. categorizar, priorizar e atribuir eventos e incidentes de segurança;

III. analisar os impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos;

IV. prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicação;

V. oferecer resposta eficiente, adequada e proporcional aos incidentes cibernéticos que apresentem risco à integridade, disponibilidade ou confidencialidade das informações hospedadas nos sistemas ou redes de computadores do TRT15;

VI. apoiar a manutenção da segurança de todo o ambiente computacional;

VII. oferecer suporte técnico ao Comitê de Governança de Segurança da Informação;

VIII. atender, por meio do Service Desk, todos os usuários dos serviços de tecnologia fornecidos pelo TRT15 que comunicarem eventos que possam ser relacionados a incidentes de segurança cibernética;

IX. implementar e desempenhar os serviços de:

A. tratamento de incidentes de segurança cibernética;

B. tratamento de vulnerabilidades técnicas no ambiente computacional; e

C. coleta e preservação de evidências digitais em incidentes cibernéticos penalmente relevantes.

7 Nível de autonomia da ETIR

7.1 Participa no resultado de decisões dos temas sob sua competência, atuando como membro consultivo no processo decisório, sendo que tal equipe poderá sugerir os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da Organização.

7.2 As ações pró-ativas devem ser incentivadas e potencializadas conforme o decorrer dos trabalhos e amadurecimento dos membros da equipe, na forma de sugestões de ações aos Comitês e encaminhadas ao Comitê Gestor de TIC; bem como realização de ações autorizadas pelo Comitê Gestor de TIC a serem feitas de forma rotineira, desde atendimento de chamados, investigações preventivas e manutenções periódicas.

7.3 Deve desempenhar suas atividades de forma reativa, realizando as atividades determinadas pelo CGSI e Comitê Gestor de TIC em temas como Tratamento de Incidentes de Segurança Cibernética, Tratamento de Artefatos Maliciosos, Tratamento de Vulnerabilidades.

8 Designação de integrantes

8.1 A ETIR será composta por servidores da Secretaria de Tecnologia da Informação e Comunicações(SETIC), que, além de suas funções regulares, desempenharam as atividades relacionadas ao tratamento e à resposta a incidentes de segurança da informação, as quais são prioritárias.

8.2 Enquanto não efetivado pelo Tribunal Regional do Trabalho da 15ª Região o Art. 21 da Resolução CNJ nº 396/2021, a ETIR temporariamente será formada por servidores da Secretaria de Tecnologia da Informação e Comunicação deste Regional.

8.3 Os membros técnicos da ETIR serão indicados pelo Comitê de Governança de Segurança da Informação com consultoria do Comitê Gestor de TIC.

8.4 A indicação de que trata o presente artigo deverá considerar o perfil profissional adequado às funções a serem exercidas.

8.5 As funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores técnicos de sistema ou de segurança, administradores de banco de dados,

administradores de rede, analistas de suporte ou quaisquer outras pessoas da Organização com conhecimento técnico mínimo sobre o tema.

9 Canal de comunicação de incidentes de Segurança da Informação

9.1 É competência da ETIR estabelecer, manter, revisar no mínimo anualmente e aperfeiçoar quando necessário o Processo de Gerenciamento de Incidentes de Segurança da Informação, o qual deve ser formalmente instituído como norma de cumprimento obrigatório no prazo de 90 dias a partir da nomeação de seus membros componentes.

9.2 No processo de trabalho deverá ser definida a forma de comunicação de todos os incidentes de segurança e problemas de Segurança de Informação relacionados ao escopo da ETIR.

10 Serviços que serão prestados

10.1 Para a definição dos serviços que serão prestados deverá se observar as necessidades e limitações, a missão, o modelo de implementação adotado e a autonomia da ETIR;

10.2 Recomenda-se que a ETIR defina os serviços a serem oferecidos aos usuários e, na medida em que forem oferecidos, que o sejam de forma gradativa e de acordo com a maturidade da equipe;

10.3 Os serviços prestados pela ETIR se relacionam exclusivamente a incidentes de segurança e problemas de Segurança de Informação, atuando conforme modelo de trabalho previsto nesta Norma.

10.4 Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores,

10.5 Descrição, puramente exemplificativa, dos possíveis serviços de tratamento de incidentes de segurança em redes de computadores, não esgotando a possibilidade de implementação de outros serviços inerentes às peculiaridades da ETIR:

10.5.1 Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa contra estes artefatos;

10.5.2 Tratamento de vulnerabilidades - Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em hardware ou software , objetivando analisar sua

natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

10.5.3 Emissão de alertas e advertências - Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema;

10.5.4 Anúncios - Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças;

10.5.5 Prospecção ou monitoração de novas tecnologias – Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Este serviço inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema;

10.5.6 Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da organização com base em requisitos da própria organização ou em melhores práticas de mercado. O serviço pode incluir: revisão da infraestrutura, revisão de processos, varredura da rede e testes de penetração;

10.5.7 Desenvolvimento de ferramentas de segurança - Este serviço consiste no desenvolvimento de qualquer ferramenta nova específica de tratamento de incidentes de segurança em redes de computadores, para a ETIR ou para comunidade;

10.5.8 Detecção de intrusão - Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETIR e o CTIR Gov;

10.5.9 Disseminação de informações relacionadas à segurança - Este serviço fornece de maneira fácil e abrangente a possibilidade de encontrar informações úteis no auxílio do tratamento de incidentes de segurança cibernética.