PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO

Institui normas para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta do Processo Administrativo nº 14484/2014,

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, assim como o conteúdo das normas de segurança da informação instituídas pelo TRT e a ela alinhadas;

CONSIDERANDO a Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19/08/2010, que trata da gestão de ETIR e das diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal (APF);

CONSIDERANDO a Seção 16 da norma ABNT NBR ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação),

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui normas para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

Art. 2º Para os fins desta Portaria, consideram-se as definições

constantes do art. 2º da Resolução Administrativa TRT 18ª nº 145/2019, as definições constantes do ato normativo que Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR e as seguintes:

I – ameaça: causa potencial de um incidente indesejado, que pode resultar em um dano para um sistema ou para a organização;

II – fragilidade : vulnerabilidade em um ativo de informação (do ponto de vista da segurança), ou em uma medida de tratamento de risco relacionada a esse ativo, e que pode ser explorada por uma ameaça.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 3º Compete ao chefe da unidade de Relacionamento e Atendimento de TIC preparar e orientar a unidade de Atendimento para atuar como ponto de contato entre usuários e unidades da Secretaria de Tecnologia da Informação e Comunicação (STI) no que diz respeito a receber e registrar notificações de eventos, incidentes e fragilidades de segurança da informação, assim como para proporcionar o retorno sobre os respectivos tratamentos em andamento ou concluídos.

Art. 4º Compete aos usuários, público-alvo da ETIR:

I – notificar ao ponto de contato, o mais breve possível, os eventos, incidentes e fragilidades de segurança da informação de que tenham conhecimento, orientando-se pelos procedimentos de notificação previamente divulgados;

II – não testar fragilidades, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou sistemas de informação e resultar em responsabilidade administrativa/legal para o indivíduo que executou o teste.

Art. 5º Compete ao agente responsável pela ETIR:

I – elaborar, solicitar aprovação da Comissão de Gestão de TIC (CGTIC) e divulgar a lista com os tipos de incidentes tratados pela ETIR;

II – elaborar, solicitar aprovação da CGTIC e divulgar procedimentos sobre:

a) monitoramento, detecção, análise e notificação de eventos e incidentes de segurança da informação;

b) registro das atividades de gerenciamento de incidentes;

c) manuseio de evidências forenses;

d) avaliação e decisão sobre classificação/reclassificação entre evento e incidente de segurança da informação;

e) resposta a incidentes, incluindo escalonamento, recuperação controlada de um incidente e comunicação às pessoas ou organizações, internas e externas;

III – divulgar às partes interessadas os limites de atuação da ETIR;

IV – observar a Missão, o Modelo de Implementação, a Estrutura Organizacional e a Autonomia explicitados no normativo que institui a ETIR, assim como coordenar a prestação dos serviços desta equipe ao respectivo público-alvo;

V – coordenar entre os membros da ETIR o registro de eventos, incidentes e fragilidades de segurança da informação que sejam detectados automaticamente por ferramentas de monitoramento;

VI – decidir pela reclassificação de eventos em incidentes de segurança da informação e vice-versa;

VII – observadas as normas e procedimentos de segurança da informação, iniciar e conduzir as atividades de tratamento e resposta por autorização, prévia ou sob consulta, ou convocação do diretor da STI;

VIII – encaminhar aos responsáveis, para o devido tratamento, os registros de notificações que não se enquadrem no escopo de atuação da ETIR;

IX – fornecer informações sobre o desempenho do gerenciamento de incidentes de segurança da informação à Comissão de Segurança da Informação, quando solicitadas;

X – buscar meios formais de colaboração entre a ETIR e o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov;

XI – comunicar a ocorrência de incidentes de segurança em redes computacionais ao CTIR Gov, conforme procedimentos por ele definidos, com vistas a permitir que sejam dadas as soluções integradas para a APF, bem como a geração de estatísticas.

XII – havendo indícios de ilícitos criminais durante o gerenciamento de

incidentes de segurança em redes computacionais:

a) acionar as autoridades competentes para a adoção de procedimentos legais necessários;

b) observar procedimentos que o TRT tenha adotado ou determinado para a preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia;

c) priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos referidos na alínea anterior.

Art. 6º Compete aos gestores de ativos e respectivos custodiantes:

I – efetuar a resposta a incidentes de segurança da informação sob coordenação da ETIR;

II – providenciar ações de redução de riscos advindas de fragilidades detectadas nos ativos de informação sob custódia ou gestão, seja diretamente ou sob a coordenação da ETIR;

III – registrar, conforme procedimentos previamente divulgados, as ações realizadas durante o tratamento de incidentes e de fragilidades de segurança da informação;

IV – disponibilizar à ETIR acesso para monitoramento dos ativos de informação críticos e das respectivas medidas para tratamento de riscos de segurança da informação, observadas as normas de controle de acessos e de tratamento da informação sigilosa e da informação pessoal.

Art. 7º Compete ao diretor da STI:

I – convocar a ETIR para atuar no tratamento de incidente de segurança da informação de que tome conhecimento e entenda ser crítico para os serviços de TIC;

II – a depender do nível de autonomia da ETIR, autorizar ou negar pedido de tratamento de incidente solicitado pelo agente responsável, seja para evento em curso ou para eventos que possam ocorrer no futuro;

III – prover recursos necessários e suficientes para o bom funcionamento da ETIR.

Art. 8º Compete à unidade de Apoio à Governança de TIC:

I – obter, junto à ETIR, informações necessárias para elaborar e manter:

a) plano de conscientização, treinamento e capacitação em segurança da informação;

b) rotinas de medição, monitoramento, auditoria e análise crítica do Sistema de Gestão de Segurança da Informação;

c) estatísticas sobre o gerenciamento de incidentes de segurança da informação no TRT18;

II – colaborar com a ETIR na divulgação dos serviços, procedimentos e recursos necessários para o gerenciamento de incidentes de segurança da informação no âmbito do TRT18.

CAPÍTULO II
DAS DISPOSIÇÕES FINAIS

Art. 9º É recomendado que os serviços prestados pela ETIR, a exemplo do tratamento de incidentes de segurança em redes computacionais, sejam representados por fluxos de processos integrados aos demais processos de gerenciamentos de serviços de TIC previstos na Política de Gestão e Governança de TIC, no que couber.

Art. 10. A presente Portaria substitui o conteúdo da norma “NO06 - Gerenciamento de Incidentes de Segurança da Informação”, cujo nome é referenciado em alguns documentos e atos normativos atualmente existentes.

Art. 11. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria GP/DGOV nº 017/2019.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
PAULO PIMENTA
Desembargador-Presidente
TRT da 18ª Região

Goiânia, 7 de dezembro de 2020.
[assinado eletronicamente]

PAULO SÉRGIO PIMENTA

DESEMB. PRES. DE TRIBUNAL