ANEXO

RESOLUÇÃO Nº 11/CEGOV/INSS, DE 31 DE agosto DE 2020

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos **- ETIR-inss**

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações no âmbito do INSS.

Art. 2º As atividades pertinentes à ETIR-INSS englobam os usuários dos serviços de Tecnologia da Informação - TI e os sistemas de informação do INSS e serão realizadas com intercâmbio de informações e em cooperação com as seguintes instâncias:

I - o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV;

II - a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR de empresas prestadoras de serviços de tecnologia contratadas pelo INSS;

III - as ETIRs ou estrutura equivalente dos demais órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos, convênios ou instrumentos congêneres com o INSS; e

IV - o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Art. 3º Para os efeitos desta Resolução ficam estabelecidos os seguintes conceitos e definições:

I - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: equipe de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

III - agente responsável: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta ou militar de carreira incumbido de chefiar e gerenciar uma ETIR;

IV - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

V - Comunidade ou Público Alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR ou estrutura equivalente;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em processo definido, oferecido à comunidade pela ETIR;

VIII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço consistente em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IX - usuário: pessoas que fazem uso de serviços de TI e sistemas de informação de propriedade do INSS, independentemente do cargo ocupado (contratados, consultores, conselheiros, servidores, temporários e etc.); e

X - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que possam resultar em risco para um sistema ou por uma organização, e que possam ser evitados por uma ação interna de segurança da informação.

Art. 4º A implementação e o funcionamento da ETIR-INSS seguirão metodologia definida pelo GSI/PR e as seguintes diretrizes:

I - basear-se no "Modelo 1 – Utilizando a equipe de Tecnologia da Informação", conforme definido pelo GSI/PR;

II - os integrantes da Equipe deverão ser profissionais da área de Tecnologia da Informação, servidores públicos efetivos, lotados na Diretoria de Tecnologia da Informação e Inovação – DTI do INSS, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-INSS;

III - a ETIR-INSS ficará vinculada tecnicamente à Coordenação-Geral de Infraestrutura e Operações – CGIN da DTI;

IV - o Coordenador da ETIR-INSS será nomeado por ato do Diretor de Tecnologia da Informação e Inovação; e

V - na ausência de Coordenador formalmente nomeado, as atribuições relacionadas à coordenação da equipe serão desempenhadas pelo Coordenador-Geral de Infraestrutura e Operações.

Art. 5º A ETIR-INSS será composta por membros:

I - permanentes, que efetivamente atuarão em todos os incidentes registrados;

II - colaboradores, que atuarão, de forma esporádica, no tratamento de incidentes relacionados às suas áreas de atuação; e

III - opcionais, servidores das unidades descentralizadas do INSS sob supervisão da DTI.

§ 1º Os membros da ETIR-INSS serão designados por meio de ato do Diretor de Tecnologia da Informação e Inovação.

§ 2º A distribuição dos membros da ETIR-INSS se dará da seguinte forma:

I - 2 (dois) servidores permanentes, oriundos do Serviço de Segurança de TIC;

II - 2 (dois) servidores colaboradores, oriundos da CGIN;

III - 2 (dois) servidores colaboradores, oriundos da Coordenação-Geral de Projetos e Soluções Digitais da DTI; e

IV - 2 (dois) servidores opcionais, oriundos das unidades descentralizadas do INSS.

Art. 6º A ETIR-INSS terá autonomia limitada para o tratamento de incidentes de Segurança da Informação, devendo implementar ações que possam impactar outras áreas do Instituto somente com anuência do Diretor de Tecnologia da Informação e Inovação e do Gestor responsável pela área/sistema afetada, e poderá, ainda, gerar relatórios técnicos sugerindo a adoção de medidas para resolução de incidentes.

Art. 7º A ETIR-INSS fornecerá o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais, que compreende as seguintes ações:

I - recepção de solicitações e alertas diversos, utilizando como canal de comunicação a caixa postal etir@inss.gov.br, a ser disponibilizada pelo INSS;

II - filtragem de todo conteúdo direcionado à ETIR-INSS, para fins de verificação quanto à necessidade de tratamento pela Equipe e, caso não se trate de incidente de segurança em redes computacionais, encaminhar para a área competente;

III - catalogação dos incidentes detectados em ferramenta a ser indicada pela DTI, com nível de acesso restrito;

IV - classificação dos incidentes detectados quanto ao nível de severidade e impacto;

V - tratamento do incidente com medidas corretivas e indicação de formas de se evitar que ocorra novamente;

VI - resposta às solicitações e alertas encaminhados para a ETIR; e

VII - monitoramento da aplicação do tratamento dos incidentes indicados.

§ 1º A ETIR-INSS deverá analisar os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

§ 2º O detalhamento dos serviços prestados pela ETIR-INSS deverá ser publicado em página específica da Intranet do INSS, no prazo de 30 (trinta) dias a partir da publicação desta Resolução.