NORMA COMPLEMENTAR 01, DE 03 DE AGOSTO DE 2020

Dispõe sobre o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Federal do Sertão Pernambucano.

OBJETIVO

Art.1º Instituir e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR, do Instituto Federal do Sertão Pernambucano - IF Sertão-PE.

DEFINIÇÕES

Art.2º Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

I. **Agente Responsável**: Coordenador de Infraestrutura de Redes e Segurança na área de Tecnologia da Informação da Reitoria do IF Sertão-PE, incumbido de chefiar e gerenciar a ETIR;

II. **Artefato Malicioso**: é 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;

III. **Comunidade ou Público Alvo**: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV. **CTIR GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR**: Grupo de pessoas com a responsabilidade de receber,

analisar e responder às notificações e atividades relacionadas a incidente de segurança em redes de computadores;

VI. **Incidente de Segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII. **Serviço**: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

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

IX. **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos (lógicos ou físicos) indesejáveis ou não autorizados.

X. **TI** - Tecnologia da Informação.

MISSÃO

Art.3º A ETIR do IF Sertão-PE tem por missão receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança da informação em sistemas computacionais no âmbito do IF Sertão-PE, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da Instituição.

MODELO DE IMPLEMENTAÇÃO

Art.4º O IF Sertão-PE adotará o modelo de implementação da ETIR proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, qual seja, Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI.

Art.5º De acordo com a referida norma, no modelo não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de Rede. A Equipe será formada a partir dos membros das equipes de TI do próprio órgão ou entidade, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais. Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas por analistas e/ou técnicos de Tecnologia da Informação e/ou técnicos de laboratório.

Art.6º A Equipe desempenhará suas atividades de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades proativas. Além disso, os membros da ETIR poderão propor atividades proativas ao Agente responsável.

ESTRUTURA ORGANIZACIONAL

Art.7º A estrutura organizacional da ETIR será composta pelo Agente Responsável pelos demais Membros da Equipe.

Art.8º O Agente Responsável será o Servidor Público efetivo Coordenador de Infraestrutura de Redes e Segurança da Reitoria do IF Sertão-PE, incumbido de chefiar e gerenciar a ETIR.

Art.9º O Membro da Equipe deverá ser ocupante de qualquer um destes cargos no IF Sertão-PE: Analista de TI, Técnico de TI ou Técnico de Laboratório. Este será incumbido de receber, analisar e responder às notificações e atividades

relacionadas aos incidentes de segurança em redes de computadores e demais atividades descritas nesta norma.

Art.10º Cada unidade do IF Sertão-PE deverá possuir ao menos um Membro de Equipe na ETIR. Este será responsável por tratar quaisquer incidentes de segurança em redes de computadores ocorrido em sua unidade e relatá-los ao ETIR.

I. Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.
II. Em caso de licença, afastamento ou férias do Agente Responsável, este deverá designar como seu substituto um Membro da Equipe.
III. O Agente Responsável e Membro da Equipe lotado na Reitoria, deverá ser nomeado por meio de portaria interna da reitoria.
IV. O Membro da Equipe que compõe a ETIR lotado em campus deverá ser nomeado por meio de portaria interna, por indicação do diretor geral do campus.
V. O Gestor de Segurança da Informação da organização (GSI) será o responsável por definir, junto à área de gestão de pessoas do IF Sertão-PE, as necessidades de capacitação e o aperfeiçoamento técnico dos membros da Equipe.

AUTONOMIA

Art.11º A ETIR trabalhará de forma autônoma e com apoio dos setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas deverão ser adotadas.

Art.12º A Equipe poderá recomendar e/ou realizar 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 o Gestor de Segurança da Informação.

ATRIBUIÇÕES

Art.13º Garantir que os incidentes em Redes Computacionais do IF Sertão-PE sejam monitorados e tratados;

Art.14º Apoiar os treinamentos relacionados à segurança da Informação, fornecendo casos práticos de incidentes de segurança, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer como reagir a tais incidentes e como evitá-los no futuro;

Art.15º Recolher provas o quanto antes após a ocorrência de um incidente de segurança da Informação;

Art.16º Executar análise sobre os registros de falha para assegurar que estas foram satisfatoriamente atendidas;

Art.17º Investigar as causas dos incidentes de segurança da Informação;

Art.18º Submeter ao Gestor de Segurança procedimentos adotado e as ocorrências de violação às normas de segurança da informação do IF Sertão-PE;

Art.19º Indicar a necessidade de controles para limitar a frequência e os danos de futuras ocorrências de incidentes de segurança em redes de computadores;

Art.20º Emitir relatório anual ou sob-requisição do Gestor de Segurança da Informação contendo o resumo das ocorrências de incidentes de segurança para apresentação ao CGSI;

Art.21º Notificar o Gestor de Segurança da Informação a respeito dos eventos e incidentes de segurança da informação na rede de computadores do IF Sertão-PE que ensejem aplicação de penalidades previstas na PSI;

Paragrafo Único: Comunicar a ocorrência de incidentes de segurança em redes de computadores ao CTIR Gov, conforme procedimentos definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal, bem como a geração de estatísticas.

DISPOSIÇÕES GERAIS

Art.22º Os servidores e colaboradores devem comunicar a ETIR, o mais breve possível, toda e qualquer falha, anomalia, ameaça ou vulnerabilidade identificada, mesmo que seja apenas uma suspeita.

Art.23º O canal de comunicação com a ETIR é o e-mail etir@ifsertao-pe.edu.br.

Art.24º A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo CTIR GOV.

Art.25º A ETIR poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar ou Normas Internas do IF Sertão-PE.

Art.26º A troca de informações e a forma de comunicação entre a ETIR e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

VIGÊNCIA

Art.27º Esta Norma entra em vigor na data da sua publicação.