UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 03 – GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Tratamento de Incidentes de Segurança da Informação é o serviço que consiste em receber, filtrar, classificar e responder a solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

O Tratamento de Incidentes de Segurança da Informação deve consistir em um conjunto de atividades coordenadas capazes de promover o restabelecimento do serviço e a eliminação ou diminuição dos impactos provenientes de incidentes de segurança.

As diretrizes para estruturação de um plano de tratamento de incidentes de segurança incluem, mas não se limitam às seguintes etapas:

- Identificar as fragilidades e eventos de segurança e sua divulgação e conscientização como processo educacional;
- Estabelecer canais de comunicação desses eventos de maneira a permitir a tomada de ações em tempo hábil;
- Gerenciar os incidentes de segurança de maneira que a solução aplicada seja consistente e efetiva. A gestão inclui, dentre outras ações:
    - Definir as estratégias de monitoramento de sistemas, alertas e vulnerabilidades;
    - Definir procedimentos para manusear os diferentes tipos de incidentes de segurança (trilhas de auditoria, responsabilidades, dentre outros.);
    - Definir procedimentos para receber e tratar notificações internas ou externas, com o objetivo de detectar ou identificar de fato a existência de um incidente de segurança;
    - Levantar os impactos e determinação do diagnóstico preliminar que possa guiar as ações de solução do problema;
    - Estabelecer planos de contingência; e
    - Documentar as ações como processo de realimentação educacional.

Em particular, no que se refere a recursos de TIC, este tratamento deve incluir estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido:

- Falhas de sistemas de informação e perda de serviços;
- Ataques cibernéticos;
- Violações de confidencialidade e integridade; e
- Sinistros (inundações, incêndios, dentre outros).

Todo o tratamento de incidentes de segurança está sob a responsabilidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação.

Os temas relativos à modelo, responsabilidade e autonomia da equipe deve ser abordado no documento de criação da ETIR.

1. CRIAÇÃO DA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR)

1.1 MISSÃO

Garantir o cumprimento da missão institucional da Universidade Federal do Espírito Santo por meio da prevenção, tratamento e resposta a incidentes de segurança cibernética, além de disseminar práticas para o uso seguro das Tecnologias de Informação e Comunicação.

1.2 PÚBLICO-ALVO

O público-alvo da ETIR da Ufes é formado pelos membros da comunidade acadêmica e por todos os usuários dos serviços de Tecnologia da Informação e Comunicação da Universidade.

1.3 MODELO DE IMPLEMENTAÇÃO

O modelo de implementação adotado no estabelecimento da ETIR da Ufes segue o estabelecido no Modelo 1, da Norma Complementar nº 05/IN01/DSIC/GSIPR, homologada pela Portaria GSI/PR nº 38, de 14 de agosto de 2009, sendo formada por membros da Superintendência de Tecnologia da Informação (STI), preferencialmente servidores efetivos e estáveis, que desempenharão atividades de forma proativa e reativa ao tratamento e resposta

a incidentes de segurança em redes computacionais.

1.4 ESTRUTURA ORGANIZACIONAL

A ETIR será formada por quatro integrantes, todos pertencentes a STI. Ao ocupante do cargo de Diretor de Infraestrutura e Suporte (DIS/STI) é designado o posto de Agente Responsável, que deve criar os procedimentos internos, gerenciar as atividades, distribuir tarefas da ETIR e intermediar a comunicação com outras ETIRs da Administração Pública Federal durante o tratamento de incidentes de segurança da informação oriundos por notificações externas.

Os integrantes da ETIR são designados pelo Gestor de Segurança da Informação, sendo que para cada integrante deverá ser indicado um suplente.

Extraordinariamente, o Agente Responsável poderá convocar outros membros da STI ou de outros setores da Universidade para atuar no tratamento e resposta de determinado incidente de segurança.

Sempre que preciso, as atividades da ETIR, proativas ou reativas, terão precedência sobre as demais atividades realizadas pelos seus integrantes.

1.5 AUTONOMIA DA ETIR

Durante o tratamento de incidentes, a ETIR tem autonomia completa para tomar as medidas técnicas necessárias para o restabelecimento dos serviços e/ou recuperação de dados.

1.6 SERVIÇOS DA ETIR

Os serviços prestados pela ETIR são:

- Tratamento de incidentes de segurança em redes computacionais.
- Resposta a notificações externas de outras ETIR.
- Análise de Vulnerabilidade da rede UFES.
- Melhorias de segurança de acesso à rede UFES.