CRISI – Definições Gerais

SUTIC/UFERSA

1. APRESENTAÇÃO

O objetivo deste documento é registrar as definições acerca dos elementos básicos da equipe de resposta a incidente da Universidade Federal Rural do Semi-Árido. Estas definições incluem missão, visão, estrutura e modelo organizacional e autonomia da equipe.

2. DEFINIÇÕES

2.1 NOME DA EQUIPE

Comitê de Resposta a Incidentes de Segurança da Informação - CRISI

Comentários: Comitê de caráter eminentemente técnico/executivo, constituído por profissionais efetivos da Universidade com conhecimento e experiência capazes de tratar a ocorrência de incidentes de segurança da informação e realizar ações de mitigação bem como se antever à ocorrência destes incidentes.

2.2. MISSÃO

Proteger a integridade da Instituição, da comunidade que a constitui, do capital intelectual e do conhecimento gerado na organização pela diminuição dos riscos e tratamento de incidentes de segurança da informação.

Comentários: A Universidade é reconhecida pela sociedade como uma referência no crescimento intelectual das pessoas e da sociedade e isso se dá pelo conhecimento gerado. Este conhecimento deve ser protegido da ação de malfeitores assim como as pessoas que fomentam o crescimento e divulgação deste conhecimento. Complementarmente, para a continuidade do negócio da Universidade faz-necessário ainda que as ações de gestão sejam protegidas e interferências externas e internas.

2.3. VISÃO

Ser a referência organizacional para violações de dados, atuando na resposta a incidentes de segurança da informação em redes de computadores para a comunidade técnica interna e instituições externas, buscando fortalecer a prevenção e detecção de incidentes de segurança da informação.

Comentários: Tempo entre incidentes é um parâmetro que deixa claro que o risco sempre existirá, não importa o esforço dispendido, mas que se este esforço for bem realizado os incidentes ocorrerão com menos frequência, à medida em que isso ocorra queremos que o setor não se torne invisível, mas que seja visto como referência no tema.

2.4. PÚBLICO ALVO

A comunidade acadêmica da Universidade, através dos ativos de informação, serviços e meio de comunicação digitais.

Comentários: Os riscos e incidentes observados devem cobrir os meios pelo qual as informações e dados gerenciais e acadêmicos da Universidade são manipulados, armazenados e transmitidos.

2.5. SERVIÇOS

TRATAMENTO DE INCIDENTES	
Objetivo	Tratar as ocorrências de incidentes de segurança da informação e responder aos envolvidos sobre as ações realizadas.
Disponibilidade	8 x 5
SLA	48 horas uteis
Solicitação	Alunos e servidores, técnico-administrativos e docentes, da UFERSA

GERENCIAMENTO DE VULNERABILIDADES	
Objetivo	Identificar falhas de segurança em ativos, serviços e sistemas, analisando, em conjunto com as unidades, as vulnerabilidades e orientando sua mitigação antes da exploração por agentes maliciosos
Disponibilidade	8 x 5
SLA	48 horas uteis
Solicitação	Alunos e servidores, técnico-administrativos e docentes, da UFERSA

DISSEMINAÇÃO DA CULTURA EM SEGURANÇA DA INFORMAÇÃO	
Objetivo	Promover uma disseminação da cultura de segurança da informação
Disponibilidade	8 x 5
SLA	Determinado pelo projeto de disseminação e pela urgência da ação
Solicitação	Comitê de Governança Digital (CGD/UFERSA) ou Superintendência de Tecnologia da Informação e Comunicação (STIC/UFERSA)

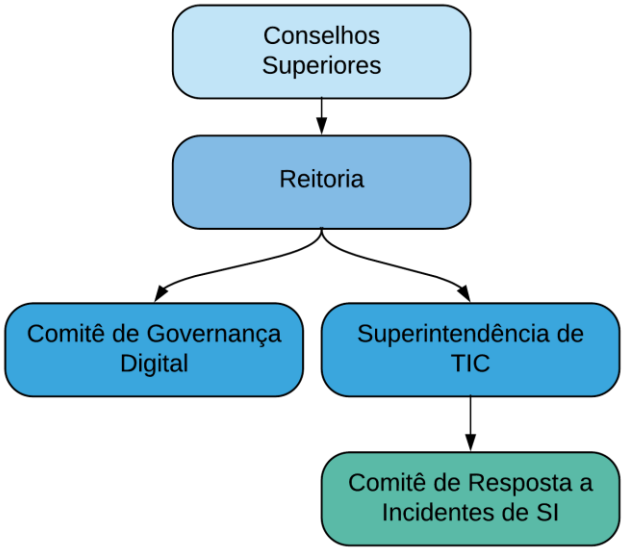
2.6. MODELO ORGANIZACIONAL

Os membros do Crisi são servidores da SUTIC que incluirão dentre suas atribuições naturais, as atribuições do Comitê.

Comentários: A instituição possui uma estrutura de TI muito enxuta em termos de volume de profissionais, e a expertise da equipe já instalada é essencial para a formalização da equipe de tratamento de incidentes.

2.7. ESTRUTURA ORGANIZACIONAL

2.7.1. ORGANOGRAMA



Comentário: Apesar de estar operacionalmente conectado diretamente à SUTIC, o Crisi responde também ao CGD em demandas específicas.

2.7.2. ORGANOGRAMA INTERNO DO CSIRT

O CRISI apesar de possuir um presidente como todo Comitê da Universidade, este deve exercer um papel de gerir a comunicação com os demais entes da Universidade e gerenciar os projetos de longo prazo, mas não exerce papel de chefia ou de poder de ação. Todos os membros são iguais mediante a necessidade de resposta a incidentes.

Comentário: o amadurecimento da Instituição e do Comitê poderá promover mudanças e necessidade de constituição de uma hierarquia mais categorizada e dividida por tipos de ação. Esta estrutura deve ser revisada bianualmente.

2.7.3 EQUIPE DO CSIRT (MEMBROS)

Presidente/Agente responsável

- Chefe da Divisão de Segurança da Informação da Universidade

MEMBROS

- Membro da Divisão de Segurança
- Membro da Divisão de Infraestrutura
- Membro da Divisão de Serviços
- Membro da Divisão de sistemas

2.8. AUTONOMIA DO CSIRT

O CRISI tem autonomia de ação, mas realiza reports periódicos e sistemáticos à SUTIC e CGD.

Comentário: O CRISI deve possuir autonomia de ação pois os incidentes não podem esperar uma decisão de um órgão superior, mas todas as ações devem ser tomadas solidariamente por todos os membros presentes durante o tratamento do incidente.