UNIVERSIDADE FEDERAL DO CEARÁ

PLANO DE TRATAMENTO DE INCIDENTES

CISI Coordenadoria de Infraestrutura e Segurança da Informação

STI Superintendência de Tecnologia da Informação

ORIGEM
Coordenadoria de Infraestrutura e Segurança da Informação – CISI
REFERÊNCIA NORMATIVA
Acórdão Nº 1608/2008 TCU-Plenário. Acórdão Nº 2308/2010 TCU-Plenário. Instrução Normativa GSI Nº 1, de 13 de Junho de 2008. Norma Complementar Nº 05/IN01/DSIC/GSIPR, de 17 de Agosto de 2009. Norma Complementar Nº 08/IN01/DSIC/GSIPR, de 24 de Agosto de 2009. Lei nº 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). POSIC/UFC. Lei Federal nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet) Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais) Guia Orientativo - Tratamento de Dados Pessoais pelo Poder Público. ANPD. Versão 1.0. jan/22.
CAMPO DE APLICAÇÃO
Redes e sistemas computacionais no âmbito da Universidade Federal do Ceará.
INFORMAÇÕES ADICIONAIS
Não há.

gov.br
Documento assinado digitalmente
AMARILDO MAIA ROLIM
Data: 09/02/2023 09:11:11-0300
Verifique em https://verificador.iti.br

Coordenadoria de Infraestrutura e Segurança da Informação
CISI

HISTÓRICO DE MUDANÇAS

Data	Revisão	Responsável	Detalhes
–	00	DSEG	Versão inicial para aprovação.
01/2023	01	CISI	Atualização de normativos; organograma da STI.

Tabela 1. Histórico de mudanças deste documento.

SUMÁRIO

INTRODUÇÃO

A Universidade Federal do Ceará (UFC), através da Superintendência da Tecnologia da Informação (STI), vêm implantando e consolidando redes locais de computadores cada vez mais amplas com a finalidade de suportar o fluxo crescente de informações e permitir o acesso à Internet à sua comunidade.

A Coordenadoria de Infraestrutura e Segurança da Informação (CISI) está encarregada na gestão da garantia de confidencialidade, integridade e disponibilidade de sistemas e recursos de Tecnologia da Informação (TI) oferecidos à comunidade. Dentre as suas atribuições está o tratamento e resposta aos diversos incidentes tentados contra os serviços ofertados pela STI.

1. OBJETIVO

Este documento define o Plano de Tratamento de Incidentes desta Universidade e institui a Equipe de Tratamento de Incidentes de Segurança em Redes de Computadores (ETIR) da STI, definindo sua missão, seus serviços e sua estrutura dentre outros aspectos relacionados, cumprindo com o estabelecido na Política de Tratamento de Incidentes de Segurança em Redes de Computadores (PTIR).

2. CONCEITOS E DEFINIÇÕES

Artefato malicioso: qualquer programa de computador, ou parte dele, construído com a intenção de causar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

Ativo: qualquer bem, material ou não, que tenha valor para a UFC;

Evento: qualquer ocorrência observável em um sistema ou rede de computadores;

Evento adverso: qualquer evento com consequências negativas, por exemplo: quebra de sistemas, inundação de pacotes, acesso não-autorizado, dentre outros;

Gestor do ativo: servidor responsável pelo ativo na instituição;

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou redes de computadores. Nesse documento o termo “incidente” será utilizado com o mesmo significado de “incidente de segurança” aqui definido;

Público-alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma equipe;

Serviços: conjunto de procedimentos, estruturados em um processo bem definido, oferecido ao público-alvo da ETIR;

Vulnerabilidade: qualquer fragilidade dos sistemas e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

3. MISSÃO

A ETIR tem como missão as ações de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança. Seus serviços abrangem a facilitação e coordenação das atividades de tratamento de incidentes de segurança, recuperação de sistemas e análise de ataques e intrusões. Para cumprir com essa missão de maneira otimizada, a ETIR buscará a cooperação com outras equipes e a participação em fóruns nacionais e internacionais, bem como a capacitação e o aperfeiçoamento de seus membros.

4. PÚBLICO ALVO

A ETIR atenderá às notificações oriundas do âmbito da UFC, atingindo a todas as divisões e a todos os usuários dos serviços de TI oferecidos através desta secretaria.

5. COOPERAÇÃO COM ENTIDADES EXTERNAS

A ETIR deve trabalhar em cooperação com outras entidades relacionadas ao tratamento de incidentes de segurança no Brasil. Dentre estas entidades estão:

CTIR Gov: Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (APF). Responsável pelo atendimento aos incidentes em redes de computadores da APF.

CERT.br: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Grupo de resposta a incidentes de segurança, mantido pelo Núcleo de Informação e Coordenação do ponto BR (NIC.br), responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

CAIS: Centro de Atendimento a Incidentes de Segurança. Responsável pela detecção, resolução e prevenção de incidentes de segurança da Rede Nacional de Ensino e Pesquisa (RNP).

ANPD: Autoridade Nacional de Proteção de Dados. Órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

Essa cooperação será feita de acordo com os procedimentos instituídos pelas próprias entidades para permitir o desenvolvimento de soluções integradas e a geração de estatísticas respeitando a classificação das informações trocadas.

Esse intercâmbio científico-tecnológico sobre o tratamento de incidentes de segurança entre a ETIR e as entidades supracitadas auxiliarão a equipe na otimização de suas atividades.

6. MODELO DE IMPLEMENTAÇÃO

A ETIR adota o modelo de implementação misto. Sendo assim, é composta por uma equipe central e por equipes distribuídas pela organização.

A equipe central é responsável por criar as estratégias, gerenciar e distribuir as atividades relacionadas ao tratamento de incidentes às equipes distribuídas. As equipes distribuídas são responsáveis pela implementação das estratégias e execução das atividades de tratamento de incidentes em suas respectivas áreas de responsabilidade.

Os membros da ETIR deverão dedicar um período de seu expediente às atividades de tratamento de incidentes para as quais forem designados. Recomenda-se que esse período seja ajustado de tal forma que membros de uma determinada tarefa dediquem o mesmo período para a realização da tarefa. Em casos onde haja dificuldade na determinação desse período, tal decisão será tomada pelo Agente Responsável.

7. AUTONOMIA

A ETIR adota o modelo de autonomia compartilhada. Assim sendo, a equipe participará do processo de tomada de decisões quanto ao tratamento de incidentes, recomendando os procedimentos ou as medidas de reparo e recuperação de incidentes e discutirá as ações a serem tomadas, ou as repercussões caso as recomendações não sejam seguidas.

A equipe será representada no processo decisório pelo Agente Responsável ou por algum outro membro da equipe indicado pelo mesmo.

8. ESTRUTURA ORGANIZACIONAL

8.1 Posição na estrutura organizacional da UFC

A ETIR faz parte da CISI, e é composta por uma equipe central e auxiliada por equipes distribuídas pela instituição. Eventualmente, será feita a indicação de substitutos para que a equipe possa garantir a execução de suas atividades.

i. Equipe central

A equipe central é composta pelo Agente Responsável, um representante da gestão de riscos, um representante da gestão de continuidade de negócio e demais membros da CISI indicados pelo Agente Responsável.

O dimensionamento da equipe deve estar adequado à demanda de seus serviços e aos recursos humanos disponíveis.

ii. Equipes distribuídas

As equipes distribuídas serão compostas por colaboradores externos, de outros setores ou divisões da instituição. A indicação desses membros ocorrerá diante de solicitação por parte do Agente Responsável ao gestor do colaborador externo, que indicará o(s) servidor(es) que ficará(ão) encarregado(s) de engajar(em)-se nas atividades de tratamento de incidentes que lhe forem

atribuídas.

As equipes distribuídas deverão conter pelo menos um colaborador externo das seguintes áreas: infraestrutura, redes de computadores, suporte e sistemas. Sempre que necessário, o Agente Responsável poderá solicitar a cooperação de membros de outros setores ou divisões para compor equipes distribuídas complementares.

8.2 Competências e responsabilidades

i. Agente Responsável

O Agente Responsável é o servidor da STI e membro da CISI, designado pelo Coordenador da CISI e está responsável por:

- Compor a equipe central e as equipes distribuídas;
- Indicar os substitutos dos membros da equipe;
- Criar procedimentos internos;
- Gerenciar as atividades;
- Atribuir tarefas;
- Buscar solução para eventuais dificuldades encontradas pela equipe na execução de suas atividades;
- Participar na tomada de decisões quanto ao tratamento de incidentes de segurança na STI;
- Intermediar e viabilizar a cooperação da equipe e as demais divisões sempre que necessário;
- Intermediar a capacitação e o aperfeiçoamento técnico-científico dos membros da equipe;
- Intermediar o provimento da infraestrutura necessária para a execução das atividades da equipe;
- Ponto de contato (Point-of-Contact - PoC) entre a STI com o CTIR Gov e demais entidades com as quais a equipe mantenha relacionamento.

ii. Membros

Os membros da equipe central são servidores da DSEG e têm como responsabilidade:

- Engajar-se nas atividades de tratamento a incidentes de segurança;
- Realizar as tarefas de tratamento a incidentes de segurança;
- Informar ao Agente Responsável o estado das atividades a qual foi designado;
- Informar ao Agente Responsável as eventuais dificuldades encontradas durante a realização de suas atividades;
- Manter-se atualizado quanto às tecnologias e soluções relacionadas à Segurança da Informação e Comunicações.

iii. Substitutos

Para garantir a atuação contínua da ETIR, devem ser indicados, pelo Agente Responsável, substitutos para os membros que se ausentarem de sua função por qualquer razão. A indicação do substituto do Agente Responsável deve ser feita pelo Coordenador da CISI.

Aquele que for indicado como substituto de um membro da equipe passa a ter as mesmas responsabilidades do membro ao qual está substituindo pelo período que se der a substituição.

iv. Colaboradores externos

Membros de outras divisões indicados pela chefia imediata da respectiva unidade, mediante solicitação do Agente Responsável, para compor uma das equipes distribuídas da ETIR.

Dentre suas responsabilidades estão:

- Auxiliar à equipe na execução da atividade a qual coopera;
- Informar ao Agente Responsável o estado das atividades a qual foi designado;
- Informar ao Agente Responsável as eventuais dificuldades encontradas durante a realização da atividade em questão.

9. SERVIÇOS

Abaixo está a lista dos serviços atualmente oferecidos pela ETIR.

- **Triagem:** recepção, classificação e registro de incidentes de segurança ocorridos no âmbito da STI;
- **Análise de incidentes:** análise dos incidentes reportados e identificação de medidas para a mitigação dos incidentes analisados;
- **Suporte à resposta a incidentes:** auxílio na recuperação de um incidente de segurança;

Uma descrição mais detalhada dos serviços é encontrada no Anexo I deste documento.

ANEXO I

Descrição dos serviços oferecidos pela ETIR

Triagem

Através deste serviço, a equipe recebe notificações e faz a abertura, o registro e o encaminhamento para a análise de incidentes de segurança ocorridos no âmbito da STI.

A ETIR possui as seguintes entradas para os relatos incidentes:

- Formulário online disponível no Portal da UFC, no banner "Solicitações de Serviços de TI" (link: *https://appsti.ufc.br/ticket/seguranca*).
    - Após realizar o login, o usuário deverá marcar a opção "Relatar incidentes de Segurança da Informação" e preencher o formulário com as informações solicitadas.
- Sistema de criação de chamados, RT, disponível em servicos.sti.ufc.br.
    - Abrir um chamado na fila "relatos de incidentes".
- Endereço de e-mail *etir@sti.ufc.br*.
- Central de Relacionamento
    - Contato através do telefone (85) 3366-9999.

Ao relatar um incidente, o usuário deverá informar:

- se o evento ainda está em andamento;
- se envolve o vazamento de dados pessoais;
- descrição do incidente/situação percebida;
- capturas de tela ou arquivos relacionados.

Os incidentes reportados deverão ser repassados para uma ferramenta de gerenciamento de incidentes, para que possam ser feitas a classificação e o registro dos incidentes reportados, bem como a atribuição da ocorrência a um membro da ETIR. Esta ferramenta deverá, também, permitir a interação com um sistema de banco de dados tal que, todo incidente reportado seja devidamente registrado e armazenado para fins de histórico e controle, obtenção de estatísticas, evidência legal e colaboração com outras entidades relacionadas ao tratamento de incidentes.

Os registros devem ser mantidos respeitando as exigências legais e regulatórias quanto ao armazenamento de informações na instituição.

Análise de incidentes

Neste serviço, é feita a análise dos incidentes reportados para que possam ser identificadas as medidas para a mitigação do incidente.

O processo de análise abrange:

- análise das informações recebidas com a notificação do incidente;
- identificação do escopo;
- identificação dos responsáveis pelos ativos afetados;
- identificação da natureza do incidente;
- identificação de medidas para mitigar o incidente.

Toda a atividade de análise deve ser registrada em um relatório contendo:

- informações do registro do incidente;
- descrição das evidências encontradas;
- os danos causados e;
- sugestão de medidas a serem tomadas.

Os incidentes envolvendo dados pessoais serão informados ao encarregado pelo tratamento de dados pessoais da UFC para execução das medidas relacionadas à LGPD.

Suporte à resposta a incidentes

Neste serviço, a equipe presta auxílio ao usuário na recuperação de um incidente de segurança e coordena as ações de resposta a incidentes de segurança.

O atendimento é feito através da comunicação com o responsável pelos ativos afetados, contendo as medidas de reparo e recuperação sugeridas pelo processo de análise.

A equipe deverá monitorar se as medidas sugeridas foram devidamente tomadas pelo gestor do(s) ativo(s) afetado(s). Caso não tenham sido tomadas, a equipe deverá entrar em contato com o gestor do(s) ativo(s) afetado(s) para averiguar porque as medidas sugeridas pela equipe não foram tomadas e tomar as ações necessárias para a contenção do incidente.

A equipe também deverá monitorar o sucesso da execução das medidas sugeridas. Em caso de sucesso da solução indicada, o incidente será considerado encerrado.