Plano de Gestão de Vulnerabilidade de Ativos de TIC

Diretoria de Governança e Gestão de TIC
Coordenação de Segurança da Informação e Proteção de Dados

Dezembro/2021

UNIVERSIDADE FEDERAL DE PERNAMBUCO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DE PERNAMBUCO
SUPERINTENDENCIA DE TECNOLOGIA DA INFORMAÇÃO – STI
DIRETORIA DE GOVERNANÇA E GESTÃO DE TIC - DGGTIC

Equipe de Colaboradores do Plano de Gestão de vulnerabilidades de ativos de TIC

André Souto Soares Afonso

John Ewerton dos Santos Paiva - CIn

Pedro Corrêa de Araújo Neto

Rosângela Saraiva Carvalho

Aprovação

Marco Aurélio Benedetti Rodrigues
Superintendente de Tecnologia da Informação - STI

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR (ES)	APROVADO POR
01/12/2021	1.0	Criação do plano de gestão de vulnerabilidades de ativos de TIC.	Equipe de colaboradores do Plano de Gestão de Incidentes de Segurança da Informação	STI

Sumário

1. Objetivo

Pode-se compreender vulnerabilidade como uma fragilidade que se explorada, é capaz de gerar um incidente de segurança da informação. Nesse contexto, os principais objetivos deste plano são:

- Corrigir ou mitigar as vulnerabilidades que venham a ser identificadas, reduzindo assim, as brechas que possam acarretar em incidente de segurança;
- Prover o tratamento das vulnerabilidades identificadas de forma sistemática e eficiente;
- Buscar que as partes responsáveis tenham um claro entendimento sobre suas atribuições na correção ou mitigação das vulnerabilidades identificadas;
- Prevenir ataques e danos futuros.

2. Escopo

O plano de gestão de vulnerabilidade, sob responsabilidade da Coordenação de Segurança da Informação e Proteção de Dados (CSIPD), está restrito a vulnerabilidades de SI em ativos de TIC da UFPE identificadas pela CSIPD, pelo Sistema de Gestão de Incidentes de Segurança da Informação – SGIS da Rede Nacional de Pesquisa – RNP ou por órgãos ou grupos externos.

4. Papéis e responsabilidades

- **Apurador da CSIPD**: servidor técnico, lotado na CSIPD/STI, responsável pelo recebimento das notificações de vulnerabilidades, por validar a referida notificação e por abrir o chamado no sistema de registro de chamados (OTRS), quando for o caso.

- **Agente responsável da ETISI**: responsável por acompanhar as atividades de resolução da vulnerabilidade identificada, verificar se a vulnerabilidade foi resolvida ou mitigada pela equipe de tratamento, e, ao final, fechar as notificações no OTRS, e quando for o caso no SGIS. Responsável também por filtrar notificações de **órgãos ou grupos externos** de segurança da informação parceiros (CERT e outras equipes de tratamento de incidentes de segurança (ETIR's)), assim como da própria **CSIPD**.

- **Equipe de tratamento**: grupo (multidisciplinar) criado com o objetivo de realizar o tratamento de uma determinada vulnerabilidade, executando ações de análise, correção ou mitigação. Este grupo deve reportar-se ao agente responsável pela ETISI sobre as ações executadas. No caso, de vulnerabilidades de SI ocorridos nos campi Caruaru e Vitória, CIn e HC, o grupo deve reportar-se ao respectivo representante da ETISI que comunicará ao agente responsável.

- **ETISI**: equipe responsável por coordenar os trabalhos no tratamento das vulnerabilidades de SI identificadas. Responsável por analisar a solução proposta pela equipe de tratamento, e quando for o caso, propor a aceitação do risco.

- **NATI** (Núcleo de Apoio a Tecnologia da Informação): responsável por apoiar o tratamento da vulnerabilidade identificada quando solicitado por algum membro da ETISI, fazendo, assim, parte da equipe de tratamento, no respectivo centro acadêmico ou órgão de atuação.

- **Relator da vulnerabilidade**: responsável pela notificação de uma vulnerabilidade. O relator da vulnerabilidade pode ser:

    - **Órgãos ou grupos externos**: órgãos/grupos de segurança da informação parceiros (CERT e outras Equipes de Tratamento de Incidentes de segurança (ETIR's)).

- **CAIS/RNP:** responsável por identificar vulnerabilidades na rede gerenciada pela UFPE e notificar a partir da ferramenta SGIS/RNP.
- **CSIPD**: coordenação de segurança da informação e proteção de dados.

5. Processo de tratamento

5.1 Notificação

Qualquer vulnerabilidade relativa a ativo de TIC da UFPE deve ser notificada à ETISI, por intermédio do sistema de abertura de chamados (OTRS).

A ETISI receberá notificações internas provenientes do **apurador da CSIPD**, que é o responsável pelo recebimento das notificações de **órgãos ou grupos externos** de segurança da informação parceiros (CERT e outras equipes de tratamento de incidentes de segurança (ETIR's)), do **CAIS/RNP**, assim como da própria **CSIPD**.

5.2 Filtragem

Para as notificações feitas pelo **CAIS/RNP**:

Cabe ao **apurador da CSIPD** realizar a filtragem da vulnerabilidade e, após análise, abrir chamado para tratamento da referida vulnerabilidade no OTRS, se necessário. Para tanto, deve consultar as notificações presentes no SGIS, verificar se a vulnerabilidade identificada é válida.

a) Se a vulnerabilidade identificada for válida, consultar o sistema de abertura de chamados (OTRS) de modo a verificar se o chamado para a referida vulnerabilidade já foi reportado. E observar, no caso:

   - De o chamado já ter sido reportado: o apurador não deve tomar nenhuma ação adicional, visto que a vulnerabilidade identificada já foi registrada para tratamento.
   - Caso a vulnerabilidade identificada não tenha sido reportada no OTRS: o apurador deve seguir para a fase de notificação no OTRS.

b) Se, a vulnerabilidade identificada não for válida, o apurador deverá seguir para a etapa de fechamento do chamado do SGIS (apenas nesses casos o apurador fará o fechamento do chamado no SGIS).

Nos casos das notificações de **órgãos ou grupos externos** de segurança da informação parceiros (CERT e outras equipes de tratamento de incidentes de segurança (ETIR's)), assim como da própria **CSIPD**, a filtragem da vulnerabilidade deve ser feita pelo agente responsável pela ETISI, que, após análise, abrirá chamado para tratamento da vulnerabilidade identificada no OTRS, quando for o caso.

5.3 Registro no OTRS

O apurador da CSIPD ou o agente responsável pela ETISI deverá abrir chamado no OTRS preenchendo os campos da seguinte forma:

- **Tipo**: Requisição de Serviços;
- **Usuário Cliente**: Agente ETISI;
- **Fila**: A depender da fila que irá atendê-lo;
- **Serviço**: Vulnerabilidade;
- **Assunto**: Deve conter o número da notificação no SGIS e o texto presente no título da notificação do SGIS, caso não venha do SGIS deve conter a origem da notificação, ou seja o "**órgãos ou grupos externo"** ou **"CSIPD".**
- **Descrição**: Deve conter:
  - Texto explicando a vulnerabilidade;
  - Endereço IP da máquina afetada;
  - Evidências da vulnerabilidade presente;
  - Formas de mitigação informadas no SGIS.
- **Canal de solicitação**: Analista Nível 2;

- **Ramal de Contato**: o ramal da CSIPD;
- **Unidade solicitante**: De acordo com o mapeamento da rede;

5.4 Análise

A equipe de tratamento deverá analisar o chamado verificando a possibilidade de resolução da vulnerabilidade identificada ou sua mitigação, considerando, para tanto, o impacto e o esforço necessário. A equipe de tratamento pode resolver ou mitigar a vulnerabilidade de forma diferente da recomenda pelo SGIS, quando considerar necessário.

Caso não seja possível resolver a vulnerabilidade identificada ou a solução demande a criação de um projeto específico para tal, o representante da ETISI responsável pela fila que responde o chamado deverá seguir as orientações do tópico "**Aceitação do Risco**".

Importa ressaltar, que os diretores das áreas afetadas e o(a) superintendente deverão ser consultados acerca da aceitação do risco.

5.5 Resolução

A equipe de tratamento deve escolher a melhor forma de resolução para a vulnerabilidade identificada, observando as sugestões apontadas pelo SGIS, bem como, as especificidades e características da universidade.

Ao término do tratamento da vulnerabilidade identificada, o representante da ETISI responsável pela fila que responde o chamado deverá registrar no chamado aberto no OTRS, as ações realizadas para o seu tratamento e encaminhar o chamado para a fila "segurança da informação" informando se a vulnerabilidade foi resolvida, mitigada ou o risco foi aceito.

No caso:

- Da vulnerabilidade identificada ter sido resolvida, o agente responsável pela ETISI deverá validar essa resolução conforme descrito no tópico "**Validação**".
- Da vulnerabilidade identificada ter sido mitigada, o agente responsável pela ETISI deverá: validar essa resolução conforme descrito no tópico "**Validação**" fechar o chamado conforme descrito nos tópicos "**Fechamento do chamado no SGIS**" e "**Fechamento do chamado no OTRS**".
- Do risco ter sido aceito, o agente responsável pela ETISI deverá seguir as recomendações do tópico "**Aceitação do Risco**".

5.6 Aceitação do Risco

Caso não seja possível resolver a vulnerabilidade identificada ou a solução demande a criação de um projeto específico para tal, o representante da ETISI responsável pela fila que responde o chamado junto com a equipe de tratamento deve:

- Consultar os diretores e o Superintendente da STI para avaliar pela aceitação do risco ou pela criação de um projeto específico que solucione a vulnerabilidade.
  - ✓ Em caso de aceitação do risco, executar a atividade "**Aceitar o risco**";
  - ✓ Em caso de criação de projeto, executar a atividade "**Oficializar demanda de projeto**".

Aceitar o risco

- Registrar a situação, justificando em nota, no OTRS, e mover o chamado para a fila da Segurança da informação;

- Reportar formalmente (email) a decisão para a CSIPD (csipd.sti@ufpe.br) com cópia para o agente responsável pela ETISI (agente.etisi@ufpe.br), para as diretorias relacionadas, e para o Superintendente da STI

O agente responsável deverá anexar devidamente as evidencias da decisão da aceitação do risco pela alta gestão no OTRS e mudar o estado do referido chamado para "Fechado sem êxito".

Oficializar demanda de projeto

- No caso de criação de projeto, o agente responsável pela ETISI deverá:

a. Registrar a demanda de projeto no OTRS;

b. Comunicar formalmente aos envolvidos do registro da demanda do projeto;

c. Registrar no chamado da vulnerabilidade (OTRS) os e-mails formalizando a decisão pela criação do projeto, bem como o número do registro da demanda do projeto aberto;

d. Mudar o estado do chamado para "resolvido sem sucesso", e

e. Seguir para a parte "**Fechar chamado no OTRS**".

5.7 Validação

O agente responsável pela ETISI deverá reproduzir o teste de vulnerabilidade apontado pelo relator da vulnerabilidade, podendo utilizar-se das ferramentas disponibilizadas pelo CAIS com vistas a verificar se a vulnerabilidade foi sanada.

- Caso a vulnerabilidade tenha sido resolvida, o agente responsável pela ETISI deverá fechar o chamado conforme descrito nos tópicos "**Fechamento do chamado no SGIS**" e "**Fechamento do chamado no OTRS**".
- Caso a vulnerabilidade persista o chamado deve ir para o estado de "Em atendimento (triagem)" e o processo volta para "**Análise**".

5.8 Fechamento do chamado no SGIS

O Agente responsável da ETISI deverá validar a solução ou mitigação aplicada à vulnerabilidade e fechar todas as notificações citadas no sistema SGIS referente ao mesmo endereço IP informando a ação tomada para a resolução ou mitigação da vulnerabilidade.

Em seguida o Agente responsável pela ETISI deverá seguir o processo para o "**Fechamento do chamado no OTRS**".

5.9 Fechamento do chamado no OTRS

Ao final do processo do tratamento da vulnerabilidade identificada, o agente responsável pela ETISI deverá mudar o estado do referido chamado no OTRS conforme as anotações registradas no chamado para:

- "Fechado com êxito", no caso, da vulnerabilidade identificada ter sido resolvida.
- "Fechado com contorno", quando a vulnerabilidade identificada tiver sido mitigada.
- "Fechado sem êxito", quando não for possível resolver a vulnerabilidade e o risco for assumido.

Importa ressaltar que se a notificação da vulnerabilidade identificada for proveniente do SGIS/RNP, o agente responsável da ETISI deverá, primeiramente, fechar o chamado no SGIS, conforme descrito no tópico “**Fechamento do chamado no SGIS**”.

6 Revisão do documento

Este plano deverá ser revisado e atualizado a cada dois anos, a contar da sua vigência ou quando a CSIPD ou a ETISI considerar necessário.

Emitido em 18/01/2023

ANEXOS Nº 326/2023 - CSIPD STI (11.29.23)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 20/01/2023 17:38)
MARCO AURELIO BENEDETTI RODRIGUES
SUPERINTENDENTE - TITULAR
STI (11.29)
Matrícula: 1512338

(Assinado digitalmente em 19/01/2023 14:39)
ROSANGELA SARAIVA CARVALHO
DIRETOR - TITULAR
DGGTIC-STI (11.29.20)
Matrícula: 1133617

Para verificar a autenticidade deste documento entre em http://sipac.ufpe.br/documentos/ informando seu número: **326**, ano: **2023**, tipo: **ANEXOS**, data de emissão: **18/01/2023** e o código de verificação: **85e42ca057**