PS_GESI Gerenciar Vulnerabilidades de Segurança da Informação

Bizagi Modeler

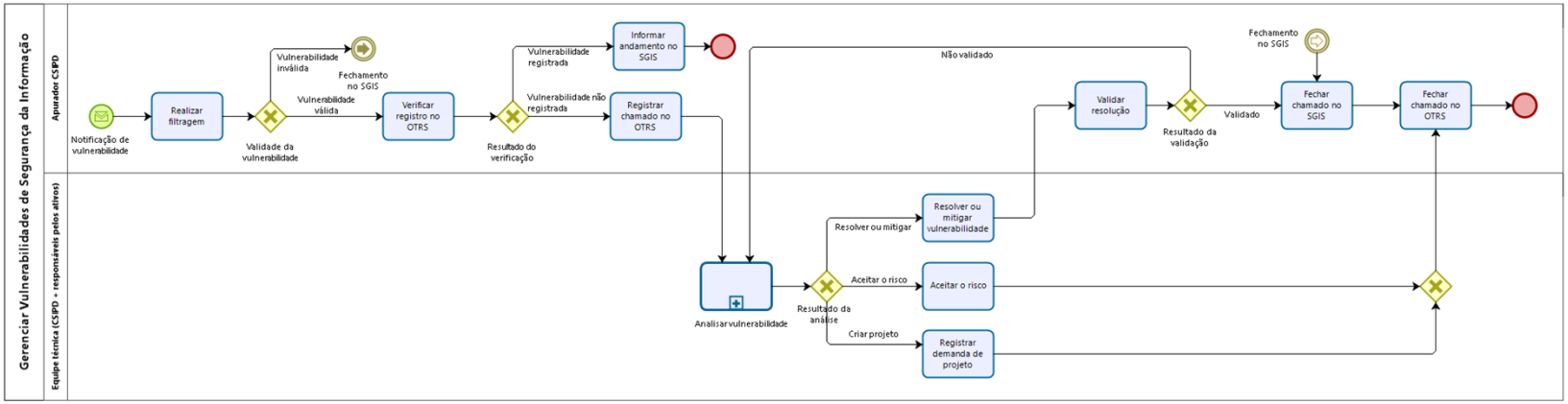
Índice

1 Gerenciar Vulnerabilidades de Segurança da Informação

Gerenciar Vulnerabilidades de Segurança da Informação

Autor: Daniel F. Arcoverde / Revisor: André S. S. Afonso
Versão: 10/09/2021
Descrição: Fluxo que descreve as atividades relacionadas ao recebimento, análise e tratamento das vulnerabilidades de segurança da informação.

UNIVERSIDADE FEDERAL DE PERNAMBUCO



Versão:

10/09/2021

Autor:

Daniel F. Arcoverde / Revisor: André S. S. Afonso

Descrição

Fluxo que descreve as atividades relacionadas ao recebimento, análise e tratamento das vulnerabilidades de segurança da informação.

1.1 Gerenciar Vulnerabilidades de Segurança da Informação

Finalidade

Promover o tratamento das vulnerabilidades de segurança da informação em ativos de TIC da UFPE e prevenir ataques e danos futuros.

Dono do Processo

Coordenador de Segurança da Informação e Proteção de Dados

Termos e definições

Termo / Sigla	Definição
CSIPD	Coordenação de Segurança da Informação e Proteção de Dados.

Atores

Ator	Responsabilidade
Apurador 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.
Equipe técnica (CSIPD + responsáveis pelos ativos)	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.

Indicadores de desempenho

Tipo	Indicador	Descrição	Fórmula de cálculo	Meta	Periodicidade
Indicador de resultado (outcome)	Percentual de resolução de vulnerabilidades de SI identificadas no SGIS	Indicador que mede a capacidade em tratar e resolver as vulnerabilidades relacionadas à Segurança da Informação na UFPE, registradas no SGIS, em um dado período de tempo.	Número de vulnerabilidades de SI resolvidas no período / Número de vulnerabilidades de SI notificadas no período	Consultar https://sgis.rnp.br/	Mensal
Indicador de resultado (outcome)	Número de vulnerabilidades resolvidas no SGIS	Indicador que mede o total de vulnerabilidades registradas como resolvidas no SGIS, em um dado período de tempo.	Número de vulnerabilidades resolvidas no SGIS no período de tempo	Não definida	Mensal
Indicador direcionador (driver)	Percentual de resolução de vulnerabilidades de SI registradas no OTRS	Indicador que mede a capacidade em tratar e resolver as vulnerabilidades relacionadas à Segurança da Informação na UFPE, registradas no OTRS, em um	Número de vulnerabilidades de SI resolvidas no período / Número total de vulnerabilidades de SI notificadas no período.	100%	Mensal

		dado período de tempo.			
Indicador direcionador (driver)	Número de vulnerabilidades notificadas no SGIS	Indicador que mede o total de vulnerabilidades registradas como resolvidas no SGIS, em um dado período de tempo.	Número de vulnerabilidades notificadas no SGIS no período de tempo.	Não definida	Mensal

Documentos reguladores

Documento/normativo	Descrição
Resolução N 01/2017 POSIC/UFPE	Política de Segurança da Informação e Comunicações da UFPE
	Plano de Gestão de Vulnerabilidades de Ativos de TIC
NC 08/IN01/DSIC/GSIPR	Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

Equipe de elaboração

Integrantes
André Souto Soares Afonso
Daniel de França Arcoverde
Maria Betânia Martins da Silva

Pedro Correa de Araújo Neto
Xerxes Lins

1.1.1 Elementos do processo

1.1.1.1 *Notificação de vulnerabilidade*

Descrição

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**.

1.1.1.2 *Realizar filtragem*

Descrição

No caso de 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.

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.

1.1.1.3 *Validade da vulnerabilidade*

Portões

Vulnerabilidade válida

Vulnerabilidade inválida

1.1.1.4 *Verificar registro no OTRS*

Descrição

Uma vez que a vulnerabilidade identificada seja válida, deve-se consultar o sistema de abertura de chamados (OTRS) de modo a verificar se o chamado para a referida vulnerabilidade foi reportado.

1.1.1.5 *Resultado do verificação*

Portões

Vulnerabilidade registrada

Vulnerabilidade não registrada

1.1.1.6 *Registrar chamado no OTRS*

Descrição

Caso a vulnerabilidade identificada não tenha sido reportada 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;

1.1.1.7 *Analisar vulnerabilidade*

Descrição

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. Em caso de resolução/mitigação da vulnerabilidade, a equipe de tratamento pode resolver ou mitigar a vulnerabilidade de forma diferente da recomendada pelo SGIS, quando considerar necessário.

Caso não seja possível resolver/mitigar 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:

- Registrar a situação, justificando em nota os encaminhamentos, no OTRS;

- Consultar os diretores e o Superintendente 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".

1.1.1.8 ◇*Resultado da análise*

Portões

Aceitar o risco

Resolver ou mitigar

Criar projeto

1.1.1.9 ☐*Resolver ou mitigar vulnerabilidade*

Descrição

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

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 tarefa “Validar resolução”.

• No caso da vulnerabilidade identificada ter sido mitigada, o agente responsável pela ETISI deverá validar essa resolução conforme descrito na tarefa "Validar resolução" e fechar o chamado conforme descrito nas tarefas "Fechar chamado no SGIS" e "Fechar chamado no OTRS".

1.1.1.10 ☐ *Validar resolução*

Descrição

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 na tarefa "Fechar chamado no SGIS" e "Fechar chamado no OTRS".

• Caso a vulnerabilidade persista o chamado deve ir para o estado de "Em atendimento (triagem)" e o processo volta para "Análise".

1.1.1.11 ◇ *Resultado da validação*

Portões

Validado

Não validado

1.1.1.12 ☐ *Aceitar o risco*

Descrição

Em caso de aceitação do risco, a equipe deverá registrar formalmente a decisão por e-mail à CSIPD (csipd.sti@ufpe.br) com cópia para o agente responsável pela ETISI, para as diretorias relacionadas, e para o Superintendente.

1.1.1.13 ☐ *Registrar demanda de projeto*

Descrição

No caso de criação de projeto, o agente responsável pela ETISI deverá registrar a demanda de projeto e comunicar formalmente aos envolvidos. E registrar no chamado os e-mails formalizando a decisão pela criação do projeto, bem como o número do registro da demanda do projeto.

O chamado deve mudar o estado para “resolvido sem sucesso" e seguir para a parte “fechar chamado no OTRS”.

1.1.1.14 *Gateway exclusivo*

Portões

Fechar chamado no OTRS

1.1.1.15 *Informar andamento no SGIS*

Descrição

Caso a vulnerabilidade já tenha sido reportada, o apurador não deve tomar nenhuma ação adicional, visto que a vulnerabilidade identificada já foi registrada para tratamento.

1.1.1.16 *Nenhum final*

1.1.1.17 *Fechamento no SGIS*

Descrição

Caso a vulnerabilidade identificada não seja 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).

1.1.1.18 *Fechamento no SGIS*

1.1.1.19 *Fechar chamado no SGIS*

Descrição

O agente responsável pela 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”.

1.1.1.20 *Fechar chamado no OTRS*

Descrição

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 ser assumido.

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

1.1.1.21 *Nenhum final*

1.1.1.22 *Apurador CSIPD*

1.1.1.23 *Equipe técnica (CSIPD + responsáveis pelos ativos)*