MANUAL DE PROCEDIMENTO

MPR/STI-030-R02

SEGURANÇA DE TIC

11/2017

REVISÕES

Revisão	Aprovação	Publicação	Aprovado Por	Modificações da Última Versão
R00	Portaria Nº 2.080, de 22 de Junho de 2017	Não informado	STI	Versão Original
R01	PORTARIA Nº 3.985, DE 30 DE NOVEMBRO DE 2017.	Não informado	STI	1) Processo 'Cadastrar Usuários Administrativos no TACACS' modificado. 2) Processo 'Cadastrar Ativos no TACACS' modificado.
R02	Não Publicado	05/10/2022	STI	1) Processo 'Cadastrar Usuários Administrativos no TACACS' removido. 2) Processo 'Cadastrar Ativos no TACACS' removido. 3) Processo 'Executar Varredura por Vulnerabilidades' inserido. 4) Processo 'Analisar Catálogo de Vulnerabilidades Exploradas' inserido. 5) Processo 'Tratar Incidentes de Segurança da Informação' inserido.

ÍNDICE

PARTICIPAÇÃO NA EXECUÇÃO DOS PROCESSOS

GRUPOS ORGANIZACIONAIS

a) Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais

1) Tratar Incidentes de Segurança da Informação

b) GEIT- Empresa Prestadora de Serviço

1) Analisar Catálogo de Vulnerabilidades Exploradas

2) Executar Varredura por Vulnerabilidades

1. DISPOSIÇÕES PRELIMINARES

1.1 INTRODUÇÃO

Este documento trata sobre as atividade analíticas referentes à manutenção, supervisão eações relativas a segurança de TI.

O MPR estabelece, no âmbito da Superintendência de Tecnologia da Informação - STI, os seguintes processos de trabalho:

a) Tratar Incidentes de Segurança da Informação.

b) Analisar Catálogo de Vulnerabilidades Exploradas.

c) Executar Varredura por Vulnerabilidades.

1.2 REVOGAÇÃO

MPR/STI-030-R01, aprovado na data de 30 de novembro de 2017.

1.3 FUNDAMENTAÇÃO

Resolução nº 381, de 14 de junho de 2016, art. 31 e alterações posteriores

1.4 EXECUTORES DOS PROCESSOS

Os procedimentos contidos neste documento aplicam-se aos servidores integrantes das seguintes áreas organizacionais:

Grupo Organizacional	Descrição
ETIR ANAC	Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais, criado pela portaria de constituição da ETIR n.
GEIT- Empresa Prestadora de Serviço	Empresa contratada de serviços

1.5 ELABORAÇÃO E REVISÃO

O processo que resulta na aprovação ou alteração deste MPR é de responsabilidade da Superintendência de Tecnologia da Informação - STI. Em caso de sugestões de revisão, deve-se procurá-la para que sejam iniciadas as providências cabíveis.

Compete ao Superintendente de Tecnologia da Informação aprovar todas as revisões deste MPR.

1.6 ORGANIZAÇÃO DO DOCUMENTO

O capítulo 2 apresenta as principais definições utilizadas no âmbito deste MPR, e deve ser visto integralmente antes da leitura de capítulos posteriores.

O capítulo 3 apresenta as competências, os artefatos e os sistemas envolvidos na execução dos processos deste manual, em ordem relativamente cronológica.

O capítulo 4 apresenta os processos de trabalho referenciados neste MPR. Estes processos são publicados em outros manuais que não este, mas cuja leitura é essencial para o entendimento dos processos publicados neste manual. O capítulo 4 expõe em quais manuais são localizados cada um dos processos de trabalho referenciados.

O capítulo 5 apresenta os processos de trabalho. Para encontrar um processo específico, deve-se procurar sua respectiva página no índice contido no início do documento. Os processos estão ordenados em etapas. Cada etapa é contida em uma tabela, que possui em si todas as informações necessárias para sua realização. São elas, respectivamente:

a) o título da etapa;

b) a descrição da forma de execução da etapa;

c) as competências necessárias para a execução da etapa;

d) os artefatos necessários para a execução da etapa;

e) os sistemas necessários para a execução da etapa (incluindo, bases de dados em forma de arquivo, se existente);

f) os documentos e processos administrativos que precisam ser elaborados durante a execução da etapa;

g) instruções para as próximas etapas; e

h) as áreas ou grupos organizacionais responsáveis por executar a etapa.

O capítulo 6 apresenta as disposições finais do documento, que trata das ações a serem realizadas em casos não previstos.

Por último, é importante comunicar que este documento foi gerado automaticamente. São recuperados dados sobre as etapas e sua sequência, as definições, os grupos, as áreas organizacionais, os artefatos, as competências, os sistemas, entre outros, para os processos de trabalho aqui apresentados, de forma que alguma mecanicidade na apresentação das informações pode ser percebida. O documento sempre apresenta as informações mais atualizadas de nomes e siglas de grupos, áreas, artefatos, termos, sistemas e suas definições, conforme informação disponível na base de dados, independente da data de assinatura do documento. Informações sobre etapas, seu detalhamento, a sequência entre etapas, responsáveis pelas etapas, artefatos, competências e sistemas associados a etapas, assim como seus nomes e os nomes de seus processos têm suas definições idênticas à da data de assinatura do documento.

2. DEFINIÇÕES

A tabela abaixo apresenta as definições necessárias para o entendimento deste Manual de Procedimento.

2.1 Sigla

Definição	Significado
GEIT	Gerência de Infraestrutura Tecnológica

3. ARTEFATOS, COMPETÊNCIAS, SISTEMAS E DOCUMENTOS ADMINISTRATIVOS

Abaixo se encontram as listas dos artefatos, competências, sistemas e documentos administrativos que o executor necessita consultar, preencher, analisar ou elaborar para executar os processos deste MPR. As etapas descritas no capítulo seguinte indicam onde usar cada um deles.

As competências devem ser adquiridas por meio de capacitação ou outros instrumentos e os artefatos se encontram no módulo "Artefatos" do sistema GFT - Gerenciador de Fluxos de Trabalho.

3.1 ARTEFATOS

Nome	Descrição
Lista de Categoria de Incidentes	Lista taxativa de categorias de incidentes

3.2 COMPETÊNCIAS

Para que os processos de trabalho contidos neste MPR possam ser realizados com qualidade e efetividade, é importante que as pessoas que venham a executá-los possuam um determinado conjunto de competências. No capítulo 5, as competências específicas que o executor de cada etapa de cada processo de trabalho deve possuir são apresentadas. A seguir, encontra-se uma lista geral das competências contidas em todos os processos de trabalho deste MPR e a indicação de qual área ou grupo organizacional as necessitam:

Não há competências descritas para a realização deste MPR.

3.3 SISTEMAS

Nome	Descrição	Acesso
Wikianac	A WikiANAC é destinada a facilitar o trabalho dos servidores, melhorando a comunicação e o registro de informações relevantes aos trabalhos do dia a dia.	https://sistemas.anac.gov.br/wiki

3.4 DOCUMENTOS E PROCESSOS ADMINISTRATIVOS ELABORADOS NESTE MANUAL

Não há documentos ou processos administrativos a serem elaborados neste MPR.

4. PROCEDIMENTOS REFERENCIADOS

Procedimentos referenciados são processos de trabalho publicados em outro MPR que têm relação com os processos de trabalho publicados por este manual. Este MPR não possui nenhum processo de trabalho referenciado.

5. PROCEDIMENTOS

Este capítulo apresenta todos os processos de trabalho deste MPR. Para encontrar um processo específico, utilize o índice nas páginas iniciais deste documento. Ao final de cada etapa encontram-se descritas as orientações necessárias à continuidade da execução do processo. O presente MPR também está disponível de forma mais conveniente em versão eletrônica, onde pode(m) ser obtido(s) o(s) artefato(s) e outras informações sobre o processo.

5.1 Tratar Incidentes de Segurança da Informação

Definição do processo para tratamento de incidentes de segurança da informação, em cumprimento à Norma Complementar 5. As atividades do processo poderão ser executadas de forma simultânea, a depender da

criticidade e da complexidade do incidente. O processo segue uma ordenação lógica, não

havendo necessariamente uma ordem temporal ou cronológica para execução das atividades,

podendo inclusive ser feitas de forma iterativa e interativa A detecção e a triagem, por exemplo,

podem ser efetuadas pela mesma pessoa e de forma concomitante, bem como as atividades de

resposta (análise, planejamento e coordenação e tratamento) Particularmente, uma ação de

contenção pode requerer celeridade e urgência já identificada na fase de detecção

O processo contém, ao todo, 7 etapas. A situação que inicia o processo, chamada de evento de início, foi descrita como: "Evento suspeito detectado", portanto, este processo deve ser executado sempre que este evento acontecer. O solicitante deve seguir a seguinte instrução: 'Havendo evento suspeito de ser incidente de segurança da informação, a ETIR ANAC deverá ser comunicada imediatamente Os Canais de Comunicação são:

Para o público interno (servidores e colaboradores da ANAC):

- Abertura de chamado através do Portal de Serviços (https://sistemasanacgovbr/portaldeservicos);

- E-mail: portaldeservicos@anacgovbr ou etir@anacgovbr;

- Telefone: 0800-061-7767;

- Correspondências oficiais (memorandos, ofícios), encaminhadas para o Agente Responsável pela ETIR;

- Página da ANAC, através do serviço Fale com a ANAC;

- Pessoalmente;

- Qualquer meio que permita à ETIR ANAC tomar conhecimento do evento tempestivamente

Para o público externo (cidadão, regulados e outros):

- Página da ANAC, através do serviço Fale com a ANAC;

- E-mail: etir@anacgovbr;

- Correspondências oficiais (memorandos, ofícios), encaminhadas para o Agente Responsável pela ETIR

As comunicações deverão conter informações de identificação do usuário e forma de contato, salvo as reportadas de forma anônima É fundamental que seja feita uma descrição detalhada da ocorrência'.

O processo é considerado concluído quando alcança algum de seus eventos de fim. Os eventos de fim descritos para esse processo são:

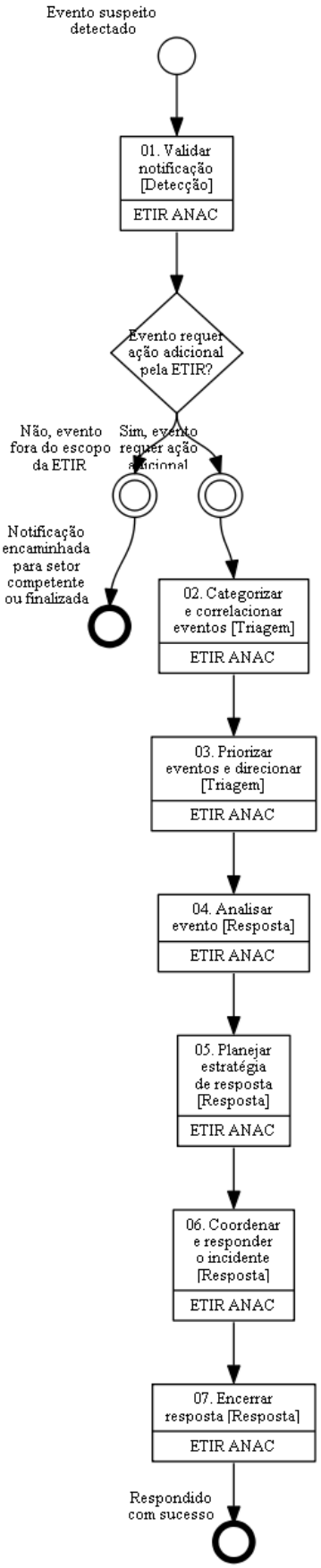
a) Respondido com sucesso.

b) Notificação encaminhada para setor competente ou finalizada.

O grupo envolvido na execução deste processo é: ETIR ANAC.

Para que este processo seja executado de forma apropriada, o executor irá necessitar do seguinte artefato: "Lista de Categoria de Incidentes".

Abaixo se encontra(m) a(s) etapa(s) a ser(em) realizada(s) na execução deste processo e o diagrama do fluxo.


Evento suspeito detectado
01. Validar notificação [Detecção]
ETIR ANAC
Evento requer ação adicional pela ETIR?
Não, evento fora do escopo da ETIR
Sim, evento requer ação adicional
Notificação encaminhada para setor competente ou finalizada
02. Categorizar e correlacionar eventos [Triagem]
ETIR ANAC
03. Priorizar eventos e direcionar [Triagem]
ETIR ANAC
04. Analisar evento [Resposta]
ETIR ANAC
05. Planejar estratégia de resposta [Resposta]
ETIR ANAC
06. Coordenar e responder o incidente [Resposta]
ETIR ANAC
07. Encerrar resposta [Resposta]
ETIR ANAC
Respondido com sucesso

01. Validar notificação [Detecção]
RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: A detecção envolve qualquer tipo de informação de evento suspeito captada pela ETIR ANAC que possa ocasionar ou indicar um incidente em curso, englobando, mas não se limitando a: - relatórios ou notificações de fontes internas, inclusive chamados de usuários no service desk direcionados para outro fim; - relatórios ou notificações de fontes externas, inclusive os alertas e recomendações do CTIR Gov e o catálogo de vulnerabilidade do CISA; - monitoramento de FW, IDS, IPS, logs de acesso, logs de sistemas, etc. Será dada ênfase na utilização do centralizador de logs para facilitar a visualização e correlação dos eventos. A detecção será efetuada com seguinte abordagem: 1. Continuamente, serão observadas/monitoradas as informações das diversas fontes em busca de sinais de atividades atípicas ou não usuais (o monitoramento contínuo é importante para se estabelecer o baseline); 2. Todo evento suspeito será investigado; 3. Caso o evento suspeito não possa ser explicado por uma atividade legítima ou autorizada (ou requeira investigação adicional), o processo será imediatamente repassado para a triagem: 4. Caso o evento suspeito não corresponda a um incidente de segurança, o processo será finalizado ou encaminhado para outro setor para continuidade do atendimento. Deve ser enfatizado que, em qualquer etapa do processo, caso se conclua que o evento não corresponda a um incidente de segurança, o processo será finalizado ou encaminhado para outro setor para continuidade.
CONTINUIDADE: caso a resposta para a pergunta "Evento requer ação adicional pela ETIR?" seja "não, evento fora do escopo da ETIR", esta etapa finaliza o procedimento. Caso a resposta seja "sim, evento requer ação adicional", deve-se seguir para a etapa "02. Categorizar e correlacionar eventos [Triagem]".

02. Categorizar e correlacionar eventos [Triagem]
RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: Será realizada uma revisão ou apuração das informações coletadas para se definir a categoria do incidente (consultar a Lista de Categoria de Incidentes). Caso o evento não se enquadre em alguma das categorias pré-estabelecidas na lista, uma nova categoria deverá ser criada e a lista deverá ser atualizada. Adicionalmente, mas não menos importante, deverá ser verificado se o evento se correlaciona com um incidente ou evento já em andamento ou finalizado, devendo-se tal fato ser levado em consideração na categorização do incidente e em passos subsequentes do processo.
ARTEFATOS USADOS NESTA ATIVIDADE: Lista de Categoria de Incidentes.

CONTINUIDADE: deve-se seguir para a etapa "03. Priorizar eventos e direcionar [Triagem]".

03. Priorizar eventos e direcionar [Triagem]

RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: Será avaliado o nível de criticidade atribuído ao incidente, conforme os 2 critérios: 1. a relevância do sistema ou informação atingida; ou 2. as ameaças discriminadas na Lista de Categoria de Incidentes já com sua criticidade pré-definida. O CMDB deverá ser consultado para se obter a informação da criticidade do sistema ou da informação atingida. Se qualquer um dos dois critérios for considerado crítico, o incidente será considerado crítico. Caso ambos os critérios não sejam críticos, o incidente será não-crítico. Se um evento isoladamente não se enquadra como incidente crítico, porém esteja correlacionado com outro(s) incidente(s) crítico(s), o conjunto será considerado crítico. A prioridade dos incidentes será estabelecida conforme o nível de criticidade e, dentre os incidentes críticos, conforme discricionariedade do Agente Responsável pela ETIR. Conforme a prioridade, o incidente será direcionado para tratamento (fase de resposta), será incluído em backlog para tratamento posterior, ou direcionado para outra área da organização caso se conclua não se tratar de incidente de segurança.
ARTEFATOS USADOS NESTA ATIVIDADE: Lista de Categoria de Incidentes.
CONTINUIDADE: deve-se seguir para a etapa "04. Analisar evento [Resposta]".

04. Analisar evento [Resposta]

RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: Está é a última etapa onde o evento poderá ser categorizado como incidente. Os fatos deverão ser investigados mais profundamente, incluindo uma breve análise das opções de mitigação e resolução do incidente. Toda informação coletada até o momento será armazenada conforme restrição de acesso apropriada, observando-se particularmente a possibilidade ou não de uso de nuvem. Paralelamente, os meios utilizados para comunicação pelas equipes envolvidas devem levar em consideração o TLP (traffic light protocol, padronizado pelo FIRST) da informação. As evidências consistindo de informações consideradas TLP:RED serão assim controladas: - Todas as permissões de visualização serão registradas; - A possibilidade de edição ou alteração da informação será desabilitada ou, caso não seja possível, as permissões de edição serão registradas;

- Todos os registros (logs) não poderão ser alterados; - Toda informação crítica será duplicada e preservada onsite e offsite em localização segura.
CONTINUIDADE: deve-se seguir para a etapa "05. Planejar estratégia de resposta [Resposta]".

05. Planejar estratégia de resposta [Resposta]

RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: Poderão fazer parte do planejamento as seguintes atividades: - Contenção de qualquer atividade maliciosa em andamento, com o objetivo de: remover acesso a sistemas comprometidos, limitar a extensão dos danos incorridos aos sistemas, e prevenir a ocorrência de dano adicional. Os passos específicos dependem do tipo de incidente (intrusão, vírus, furto, etc) e se o incidente está em andamento (p.ex. intrusão) ou finalizado (p.ex. furto de equipamento). Podem consistir em: temporariamente desligar sistema, desabilitar serviços, desconectar da rede os sistemas afetados, alterar configurações de segurança, alterar password, desabilitar contas, alterar mecanismos de acesso físico, instalar patches ou atualizações em sistemas vulneráveis, filtrar portas, serviços, IPs ou pacotes no FW, IPS, servidores de e-mail, roteadores ou outros dispositivos. - Resolução ou mitigação do incidente através da análise da causa raiz e das respectivas ações corretivas e preventivas, podendo incluir: erradicação ou exclusão de processos e arquivos maliciosos; ajuste ou melhoria de mecanismos de deteção, proteção e prevenção (tais como IDS, IPS e FW); mudanças de procedimentos de reporte; melhoria dos controles de acesso físico ou lógico; conscientização, treinamento, notificação, alerta ou outra forma de comunicação; alteração de política ou procedimentos. - Recuperação, restauração ou reparo de sistemas afetados, retornando a operação à normalidade. Idealmente a recuperação será iniciada somente após a resolução ou mitigação do incidente, para prevenir sua recorrência ou pelo menos para permitir uma deteção mais efetiva. Caso contrário, o risco de uma recuperação sem a resolução ou mitigação do incidente, particularmente num incidente crítico, deverá ser aceito formalmente pelo O STI. A recuperação incluirá os seguintes passos: 1. usar o último backup confiável para restaurar os dados, que serão revisados pelos respectivos curadores para verificação da sua integridade; 2. habilitar sistema e serviços requeridos pelos usuários; 3. reconectar o sistema restaurado à rede, e validar por meio de testes pré-determinados; 4. monitorar o sistema em busca de recorrência, pois sistema anteriormente comprometido é comumente alvo de ataque. - Comunicações requeridas, tanto interna como externamente. Para comunicações em massa ao público interno, será dada preferência por disparo de e-mail, por intermédio da ASCOM (comunica@anac.gov.br); comunicações pontuais (com poucas pessoas) serão feitas diretamente, através do meio que se julgar mais apropriado. Comunicações externas deverão seguir procedimento diferenciado, a depender do público alvo: a página da ETIR ANAC na Wikianac será consultada para contatos com CTIR Gov, DPF, SGD, ou fornecedores de ativos de rede ou segurança, caso necessário, enquanto que informe à sociedade será intermediada pela ASCOM com auxílio da ETIR ANAC. Caso haja indícios de ilícito penal ou

infração administrativa, os órgãos competentes também serão notificados conforme a competência para o caso. Serão considerados, especialmente nos incidentes críticos: - Os níveis de risco aceitáveis dos processos de negócio e a infraestrutura que os suporta, e em que extensão tais processos e infraestrutura devem permanecer operacional mesmo durante um incidente de segurança grave; - Métodos para avaliar rapidamente o estado global da situação atual (escopo, impacto, dano, ameaça, etc); - Determinar se os usuários serão imediatamente informados da ocorrência do incidente e dos impactos nas suas atividades de trabalho; - A possibilidade de as ações de contenção destruírem ou invalidarem informações potencialmente fontes de evidências; - A possibilidade de as ações de contenção alertarem o atacante, ocasionando o acionamento de medidas contradefensivas ou ofensivas por parte do atacante; - Quando e para quem escalar nas decisões mais sensíveis; - A definição do responsável ou quem desempenhará cada tarefa. A coordenação dos incidentes críticos será exercida pelo Agente Responsável pela ETIR, com a participação dos gestores da GEIT, GESI e GTPP e dO STI na tomada de decisão, enquanto a dos incidentes não críticos poderá ser exercida pela própria ETIR ANAC sem a participação direta do Agente Responsável pela ETIR. A operacionalização das atividades envolverá necessariamente os colaboradores da contratada. Poderão ser envolvidas outras torres no auxílio à resposta, a critério da coordenação. Os incidentes críticos serão tratados por estratégias específicas, especialmente desenvolvidas para o caso, além de serem notificados ao CTIR Gov e outras autoridades caso necessário. Também será identificada a necessidade de se acionar o Plano de Continuidade de Serviços de TI – PCSTI, o Plano de Recuperação de Serviços de TI – PRSTI, no âmbito da ASCOM, ou mesmo o Comitê de Crise e o Plano de Comunicação de Crise, em âmbito mais amplo.
SISTEMAS USADOS NESTA ATIVIDADE: Wikianac.
CONTINUIDADE: deve-se seguir para a etapa "06. Coordenar e responder o incidente [Resposta]".

06. Coordenar e responder o incidente [Resposta]
RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.
DETALHAMENTO: A resposta será executada conforme o plano estabelecido, envolvendo as pessoas necessárias para o tratamento e as comunicações internas ou externas.
SISTEMAS USADOS NESTA ATIVIDADE: Wikianac.
CONTINUIDADE: deve-se seguir para a etapa "07. Encerrar resposta [Resposta]".

07. Encerrar resposta [Resposta]
RESPONSÁVEL PELA EXECUÇÃO: Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais.

DETALHAMENTO: Todas as informações relevantes serão armazenadas no Microsoft Teams (Equipe "ETIR - ANAC" | Canal "INCIDENTES"), restrito à ETIR ANAC, para futura auditoria e melhoria do processo, e conterão no mínimo o seguinte: - Descrição da notificação recebida; - Tipo de ataque; - Êxito do ataque: [Não | Parcial | Sim]; - Se houve danos e quais; - Ações executadas; Os stakeholders serão comunicados conforme requerido sobre o resultado do incidente, conforme o planejamento.
CONTINUIDADE: esta etapa finaliza o procedimento.

5.2 Analisar Catálogo de Vulnerabilidades Exploradas

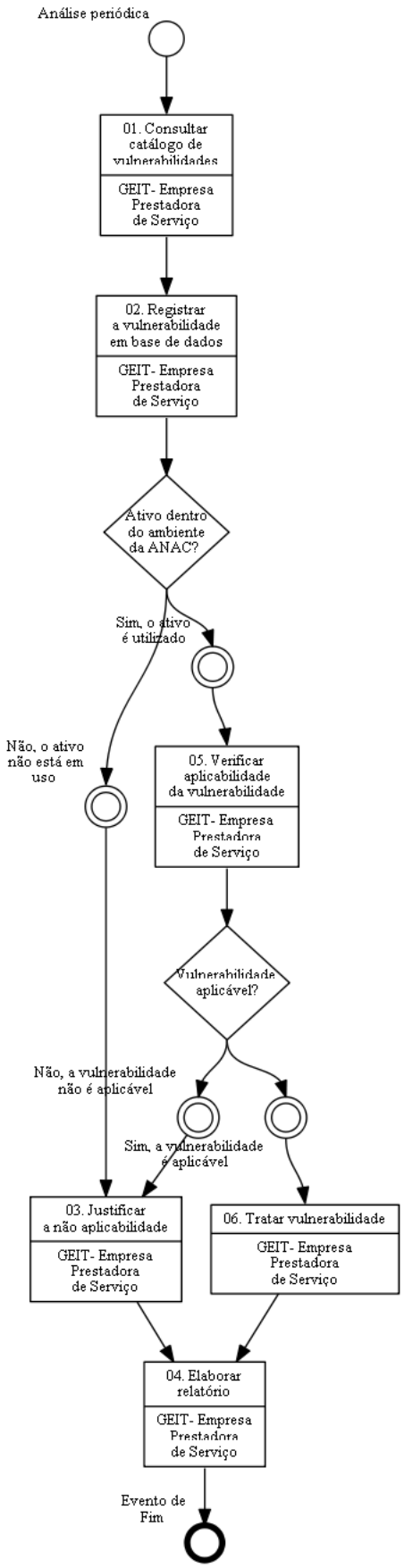
Analisar, avaliar e tratar as vulnerabilidades catalogadas pelo CISA e CTIR-BR nos ativos de infraestrutura tecnológica da ANAC.

O processo contém, ao todo, 6 etapas. A situação que inicia o processo, chamada de evento de início, foi descrita como: "Análise periódica", portanto, este processo deve ser executado sempre que este evento acontecer. O solicitante deve seguir a seguinte instrução: 'A contratada deve consultar semanalmente o catálogo publicado pelo CISA (https://wwwcisagov/known-exploited-vulnerabilities-catalog) para verificação de novas vulnerabilidades adicionadas ("Date Added to Catalog")'.

O processo é considerado concluído quando alcança seu evento de fim. O evento de fim descrito para esse processo é: "Evento de Fim.

O grupo envolvido na execução deste processo é: GEIT- Empresa Prestadora de Serviço.

Abaixo se encontra(m) a(s) etapa(s) a ser(em) realizada(s) na execução deste processo e o diagrama do fluxo.


Análise periódica
01. Consultar catálogo de vulnerabilidades
GEIT- Empresa Prestadora de Serviço
02. Registrar a vulnerabilidade em base de dados
GEIT- Empresa Prestadora de Serviço
Ativo dentro do ambiente da ANAC?
Sim, o ativo é utilizado
Não, o ativo não está em uso
05. Verificar aplicabilidade da vulnerabilidade
GEIT- Empresa Prestadora de Serviço
Vulnerabilidade aplicável?
Não, a vulnerabilidade não é aplicável
Sim, a vulnerabilidade é aplicável
03. Justificar a não aplicabilidade
GEIT- Empresa Prestadora de Serviço
06. Tratar vulnerabilidade
GEIT- Empresa Prestadora de Serviço
04. Elaborar relatório
GEIT- Empresa Prestadora de Serviço
Evento de Fim

01. Consultar catálogo de vulnerabilidades
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve consultar semanalmente o catálogo publicado pelo CISA (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) para verificação de novas vulnerabilidades adicionadas ("Date Added to Catalog"). A contratada também deve consultar os alertas e recomendações acerca de vulnerabilidades encaminhados pelo CTIR-GOV, no site (CTIR Gov — Português (Brasil) (www.gov.br)) e/ou por e-mail.
CONTINUIDADE: deve-se seguir para a etapa "02. Registrar a vulnerabilidade em base de dados".

02. Registrar a vulnerabilidade em base de dados
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: Ainda que o produto não exista na ANAC ou não esteja em uso, registrar a vulnerabilidade em planilha de registro de incidentes (CVEs), informando tal situação no devido campo. A planilha deverá ser preenchida contendo minimamente os seguintes campos: CVE ID, Vendor / Project, Product, Vulnerability Name, Date Added to Catalog, Short Description, Required Action, Due Date. A planilha estará localizada dentro da equipe “Infra-GEIT/GW”, canal “Segurança”, na aba arquivos, pasta “Catálogo CISA”
CONTINUIDADE: caso a resposta para a pergunta "Ativo dentro do ambiente da ANAC?" seja "sim, o ativo é utilizado", deve-se seguir para a etapa "05. Verificar aplicabilidade da vulnerabilidade". Caso a resposta seja "não, o ativo não está em uso", deve-se seguir para a etapa "03. Justificar a não aplicabilidade".

03. Justificar a não aplicabilidade
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve justificar a não aplicabilidade, mesmo que por motivo de inexistência do produto no ambiente da ANAC; de versão não atingida pela vulnerabilidade; ou por já ter sido executada a remediação. Deve ser registrado na planilha de incidentes os campos: Aplicável = “Não” e Ação tomada / Justificativa, Data de conclusão.
CONTINUIDADE: deve-se seguir para a etapa "04. Elaborar relatório".

04. Elaborar relatório
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.

DETALHAMENTO: A contratada deve apresentar as informações relevantes no relatório operacional mensal da torre de segurança.
CONTINUIDADE: esta etapa finaliza o procedimento.

05. Verificar aplicabilidade da vulnerabilidade
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: Caso o produto faça parte do ambiente da ANAC, a contratada deve verificar a aplicabilidade da vulnerabilidade à ANAC; caso não aplicável, deve justificar a não aplicabilidade; caso aplicável, deve incluir à base de dados informações mais detalhadas da vulnerabilidade.
CONTINUIDADE: caso a resposta para a pergunta "Vulnerabilidade aplicável?" seja "sim, a vulnerabilidade é aplicável", deve-se seguir para a etapa "06. Tratar vulnerabilidade". Caso a resposta seja "não, a vulnerabilidade não é aplicável", deve-se seguir para a etapa "03. Justificar a não aplicabilidade".

06. Tratar vulnerabilidade
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve, com um mínimo de planejamento e análise de risco, coordenar com as torres afetadas o tratamento das vulnerabilidades até a Due Date. Caso o tratamento seja por atualização/patch, deve verificar o cronograma de atualização acordado com a ANAC e, se o cronograma for posterior à Due Date, avaliar os riscos de se aguardar ou de se adiantar a atualização, e documentar as medidas de mitigação eventualmente adotadas (em função da análise e avaliação dos riscos). Todas as ações de tratamento deverão ser executadas por meio de registro de chamados, conforme processo de cumprimento de requisição. Deve ser registrado na planilha de incidentes os campos: Aplicável = “Sim” , Ação tomada / Justificativa, Chamados e Data de conclusão.
CONTINUIDADE: deve-se seguir para a etapa "04. Elaborar relatório".

5.3 Executar Varredura por Vulnerabilidades

Execução de varredura automática (scanner de vulnerabilidades) nos sistemas de TI da ANAC em busca por vulnerabilidades.

O processo contém, ao todo, 5 etapas. A situação que inicia o processo, chamada de evento de início, foi descrita como: "Varredura periódica", portanto, este processo deve ser executado sempre que este evento acontecer. O solicitante deve seguir a seguinte instrução: 'A contratada deve fazer a varredura com OpenVAS pelo menos uma vez por mês nos sistemas expostos à internet das unidades de BSB, RJ, SP e SJC'.

O processo é considerado concluído quando alcança seu evento de fim. O evento de fim descrito para esse processo é: "Varredura concluída.

Os grupos envolvidos na execução deste processo são: GEIT- Empresa Prestadora de Serviço, STI - Empresa de Apoio.

Abaixo se encontra(m) a(s) etapa(s) a ser(em) realizada(s) na execução deste processo e o diagrama do fluxo.


Varredura periódica
01. Avaliar riscos de impacto
GEIT- Empresa Prestadora de Serviço
02. Executar varredura
GEIT- Empresa Prestadora de Serviço
03. Priorizar as vulnerabilidades
GEIT- Empresa Prestadora de Serviço
04. Tratar as vulnerabilidades
GEIT- Empresa Prestadora de Serviço
05. Registrar
GEIT- Empresa Prestadora de Serviço
Varredura concluída

01. Avaliar riscos de impacto
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve manter gestão/controle de acesso às informações resultantes da varredura e gestão/controle de acesso (inclusive log) às máquinas com o OpenVAS. A varredura deve ser precedida de uma avaliação (registrada) do risco de impacto nos sistemas escaneados, e preferencialmente ocorrer fora do horário comercial.
CONTINUIDADE: deve-se seguir para a etapa "02. Executar varredura".

02. Executar varredura
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: Executar varreduras externas nos sistemas publicados da ANAC, além de outros sistemas e soluções a serem definidos, mensalmente, junto à equipe da ANAC, utilizando a ferramenta OpenVAS ou outros recursos disponíveis. Os recursos administrativos e usuários privilegiados utilizados para a varredura deverão ser desativados imediatamente após a conclusão da atividade.
CONTINUIDADE: deve-se seguir para a etapa "03. Priorizar as vulnerabilidades".

03. Priorizar as vulnerabilidades
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve preferencialmente priorizar o tratamento das vulnerabilidades conforme os seguintes critérios e nesta ordem: 1. a criticidade do ativo envolvido; 2. a severidade do CVE (CVSS).
CONTINUIDADE: deve-se seguir para a etapa "04. Tratar as vulnerabilidades".

04. Tratar as vulnerabilidades
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve coordenar com as torres afetadas, e, dentro de 15 dias corridos, elaborar e entregar um planejamento para o tratamento das vulnerabilidades, contendo uma análise simplificada dos riscos envolvidos e os prazos para tratamento. Caso a complexidade para a remediação (correção definitiva) e o risco envolvido sejam considerados elevados, a empresa deve propor medidas de mitigação apropriadas para reduzir o risco a níveis aceitáveis, até que a remediação seja possível. Dentro do planejamento, deve ser realizada a comunicação com as áreas responsáveis e/ou gestoras dos sistemas e soluções, as quais deverão aprovar as datas e horários em que serão aplicadas as correções ou ajustes necessários.
CONTINUIDADE: deve-se seguir para a etapa "05. Registrar".

05. Registrar
RESPONSÁVEL PELA EXECUÇÃO: GEIT- Empresa Prestadora de Serviço.
DETALHAMENTO: A contratada deve registrar as informações das vulnerabilidades encontradas na ferramenta de ITSM (Citsmart), para fins de rastreabilidade e auditoria. O registro deve ser feito no item de catálogo: Portal > Demandas Internas GlobalWeb > Suporte a Ativos de Segurança de Redes > Tratar notificação de vulnerabilidade de TI. Os anexos, evidências e relatórios produzidos devem ser anexados ao mesmo chamado registrado. A varredura, avaliação de risco, priorização, tratamento e outras observações relevantes devem ser documentadas e incluídas no relatório operacional mensal da torre de segurança, o qual deverá conter como anexo o relatório automático obtido do OpenVAS. A contratada deve apresentar, periodicamente, sugestões de melhorias para o aprimoramento deste processo, bem como manter o ambiente devidamente atualizado.
CONTINUIDADE: esta etapa finaliza o procedimento.

6. DISPOSIÇÕES FINAIS

Em caso de identificação de erros e omissões neste manual pelo executor do processo, a STI deve ser contatada. Cópias eletrônicas deste manual, do fluxo e dos artefatos usados podem ser encontradas em sistema.