SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

PLANO DE GESTÃO DE VULNERABILIDADES

2023

SETIC

GOVERNO DO ESTADO DE RONDÔNIA

Marcos José Rocha dos Santos

Governador

Sérgio Gonçalves da Silva

Vice-Governador

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire

Superintendente

Abdenildo Deividy Sobreira dos Santos

Diretor Técnico

COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva

Coordenador

ELABORAÇÃO

Rosemeire Vidal da Silva

Daltro Barbosa

REVISÃO

Anderson Gomes de Souza

Diego da Silva Oliveira

Ed Carlos Egert Galvão

Eduardo Falkemback Zimmer

Hendrei de Souza Maia

Idan Luiz Souza Santos

Jean Franco Ronconi de Lima

Leonardo Courinos Lima da Silva

Luma Damon de Oliveira Melo

Monike Izzo Martins

Rafael Domingues Cordeiro

Ricardo Fernandes Neto da Silva

Rogério Eduardo Vieira Alvez

Sâmara Ascoli de Queiroz

Tiago Lopes de Aguiar

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	14/03/2023	Rosemeire Vidal e Daltro Barbosa	Elaboração do Plano de Gestão de Vulnerabilidade.

LISTA DE ABREVIATURAS

SETIC	Superintendência Estadual de Tecnologia da Informação e Comunicação;
CAF	Coordenadoria de Administração e Finanças;
CAGD	Coordenadoria de Análise e Gestão de Dados;
COGE	Coordenadoria de Gestão Estratégica;
CODE	Coordenadoria de Desenvolvimento;
COINFRA	Coordenadoria de Infraestrutura e Serviços;
COSEGI	Coordenadoria de Segurança da Informação;
CPSI	Comitê de Privacidade e Segurança da Informação;
CI	Controle Interno;
LGPD	Lei Geral de Proteção de Dados Pessoais; e
GPREV	Gerência de Prevenção e Resposta a Incidentes.

SUMÁRIO

1 INTRODUÇÃO 7
2 OBJETIVO 7
3 PAPÉIS E RESPONSABILIDADES 8
4 INVENTÁRIO DE ATIVOS 9
5 GESTÃO DE VULNERABILIDADES 9
6 FLUXOGRAMA 12
7 REFERÊNCIAS 17
8 ANEXOS 18

1 INTRODUÇÃO

A SETIC utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos em parceria com demais secretarias e melhorando a disponibilidade e integridade das informações e serviços para o cidadão através de sistemas informatizados para apoiar a entrega de produtos e serviços essenciais.

A informação é um dos principais ativos da organização, dessa forma as informações tramitadas através da SETIC, sejam fornecidas ou compartilhadas, obedecem aos requisitos legais, a fim melhorar a proteção das informações através do Programa de Governança em Privacidade (PGP), como prática para ajudar na adequação da Lei Geral de Proteção de Dados Pessoais (LGPD), com intuito de elevar o grau de maturidade, em termos de proteção de dados pessoais e ações de segurança da informação.

As vulnerabilidades, de acordo com a ISO 27000 (ISO da Segurança da Informação) são uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças. A SETIC as trata mediante um ciclo de detecção através de tarefas que suportam testes de vulnerabilidades essenciais. As principais ações são focadas em definir e refinar o escopo após cada análise, preparar as ferramentas e verificar sua integridade, realizando testes e verificando os resultados.

2 OBJETIVO

O objetivo deste documento é apresentar as atividades do processo de gerenciamento de vulnerabilidades da SETIC.

O crescente índice de incidentes de segurança e os danos causados por estes incidentes evidenciam uma necessidade por ações proativas à proteção de segurança das informações.

De acordo com a norma ABNT NBR ISO/IEC 27002, um dos controles que permite apoiar nesse sentido é o Processo de Gestão de Vulnerabilidades Técnicas.

Através da gestão preventiva das vulnerabilidades é possível ter um cenário mais previsível possível e realizar o planejamento das mudanças necessárias. A construção desse processo de gestão é revisada periodicamente, tornando-o flexível, e seguindo a estrutura desta superintendência, refletindo suas necessidades, objetivos e garantindo a melhoria contínua.

A gestão de vulnerabilidades requer um processo de conhecer fraquezas dos ativos, avaliando os riscos aplicados ao negócio, para então definir o tratamento, seja corrigindo e eliminando o risco ou aceitando momentaneamente ou definitivamente.

3 PAPÉIS E RESPONSABILIDADES

. **Gerência de Prevenção de Incidentes - GPREV**: responsável por monitorar, identificar, analisar, notificar e apoiar no tratamento de vulnerabilidades de segurança da informação nos serviços e recursos de TIC no âmbito da Instituição, bem como gerar relatórios e estatísticas para acompanhamento.

. **Comitê de Privacidade e Segurança da Informação - CPSI** - responsável por aprovar este plano de gestão de vulnerabilidades e sugerir alterações em casos julgados necessários devido a mudança de cenário ou mudanças na gestão das vulnerabilidades.

. **Fornecedores** - Responsável por corrigir vulnerabilidades em ambientes e ferramentas de terceiros adquiridas pela SETIC, sendo os mesmos responsáveis pelos ativos licenciados. Além de apoiar as equipes internas na definição de boas práticas de configuração segura ou configuração de correção de vulnerabilidade identificada pelo fornecedor ou pela equipe que utiliza.

4 INVENTÁRIO DE ATIVOS

O inventário foi construído de forma a demonstrar o cenário da SETIC na atuação das ações de varreduras preventivas de identificação de vulnerabilidades.

O inventário está propiciado de forma a demonstrar todos os ativos disponíveis de hardware e de software, organizados de forma a atender a estratégia de monitoramento, varredura e tratamento, conforme disponibilizado no Anexo I.

5 GESTÃO DE VULNERABILIDADES

A abrangência deste plano compreende a SETIC e seus ativos, bem como os ativos de sua responsabilidade. As vulnerabilidades identificadas serão registradas no sistema GLPI.

O processo de gestão das vulnerabilidades será realizado em todos os ativos relacionados no Anexo I, através da identificação de alguma vulnerabilidade, validação das informações, devidas medidas de correção e/ou comunicação às partes envolvidas.

Os ciclos consistem em análise diária, semanal e mensal realizando um escaneamento em um grupo de ativos definidos e concomitantemente também é feito o monitoramento de alertas relacionados à segurança da informação gerados por sistemas de segurança da SETIC. A partir disso são abertos tickets via GLPI, Email e SEI de acordo com a necessidade da demanda para que as devidas vulnerabilidades ou notificações de alertas sejam corrigidas e ou verificadas pelo responsável do ativo.

A natureza cíclica do gerenciamento de vulnerabilidades provoca a melhoria contínua do processo realizado.

A mitigação das vulnerabilidades é feita pelo responsável do ativo, que deve estabelecer a melhor forma de tratar os problemas identificados, levando em consideração o nível do risco atrelado a cada vulnerabilidade encontrada, podendo:

Aceitar o risco - havendo impossibilidade de implementar ações para corrigir a vulnerabilidade. O risco deve ser aceito formalmente pelo responsável do ativo;

Mitigar o risco - Evitar o risco através dos controles e soluções direcionado pela equipe de tratamento, a fim de diminuir o nível de risco; e

Transferir - acionar fornecedor responsável por corrigir vulnerabilidades em ambientes externos, garantida através de contrato.

As varreduras são realizadas em intervalo de tempo necessário a ser concluído o tratamento e mitigação da varredura anterior e em concomitante a equipe de tratamento realiza o acompanhamento de todas as entradas de comunicados externos à SETIC. Os responsáveis pelos ativos notificados necessitam comunicar à equipe a ação a ser realizada, como: aceitar, mitigar ou informar se irá transferir o risco, formalmente.

Em seguida ao tratamento realizado, a equipe pode ser notificada para que uma nova varredura seja realizada no ambiente, a fim de avaliar a implementação ocorrida.

As informações de identificação, validação e classificação até o encerramento do tratamento das vulnerabilidades, farão parte do relatório trimestral da COSEGI.

5.1 MATRIZ DE PRIORIZAÇÃO/CLASSIFICAÇÃO

A classificação de vulnerabilidades é feita de forma automática pela ferramenta de análise de vulnerabilidades utilizada na SETIC, utilizando a pontuação CVSS (Common Vulnerability Scoring System), padrão este, criado pelo Forum for Incident Response and Security Team (FIRST).

As vulnerabilidades são classificadas em:

CLASSIFICAÇÃO DAS VULNERABILIDADES

Padrão criado pelo Forum for Incident Response and Security Team (FIRST).

Crítica
Alta
Média
Baixa
Informativa

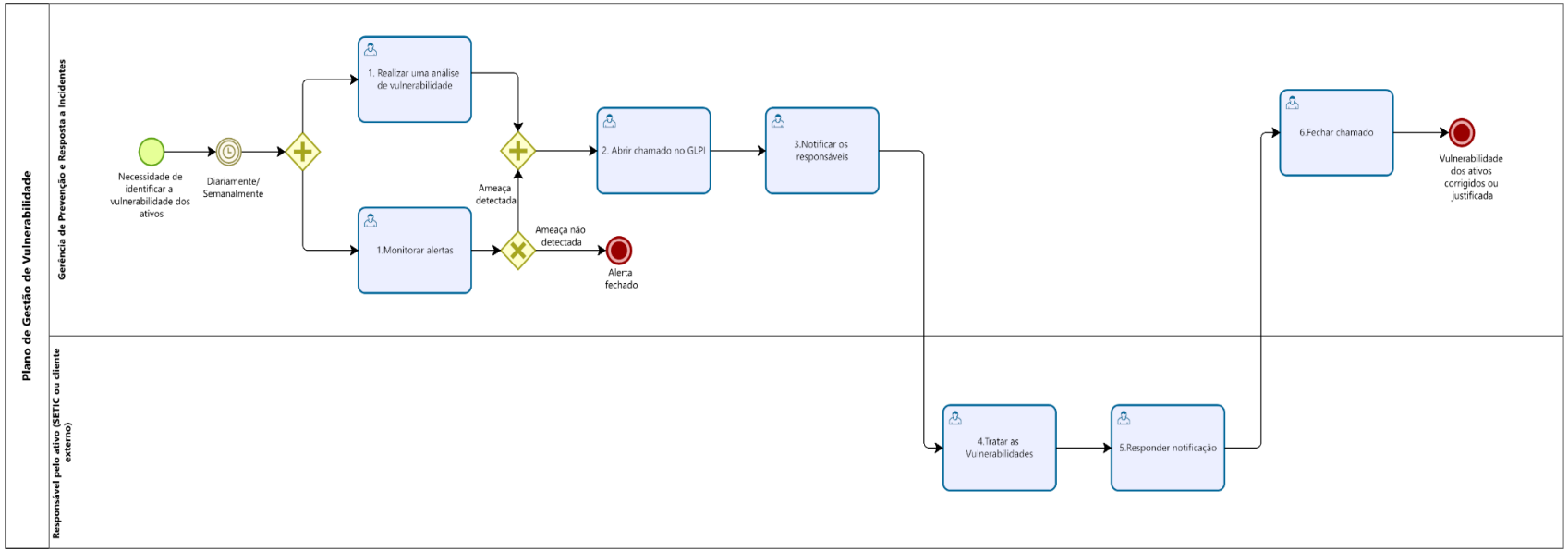
6 FLUXOGRAMA

Plano de Gestão de Vulnerabilidade

Autor: Usuário

Versão: 1.0

Descrição: Este processo tem como escopo as atividades de identificação da Vulnerabilidade, desde a entrada da necessidade de identificar a vulnerabilidade dos ativos, até o término dos procedimentos de recuperação estabelecidos.



Powered by bizagi Modeler

6.1 FASES DO FLUXOGRAMA

6.1.1 Realizar Análise de Vulnerabilidades

O processo de análise de vulnerabilidades será executado, em base periódica, conforme definido pela equipe de segurança, em um escopo pré-determinado de ativos da SETIC.

Cabe ressaltar que para ativos considerados importantes, todas as equipes envolvidas no processo de análise de vulnerabilidades serão notificadas com antecedência. Isso se deve ao fato da possibilidade de degradação na performance dos ativos envolvidos (enlace, roteadores, servidores, aplicações) durante a análise.

Também poderá ser solicitado, via email, GLPI ou SEI, uma análise de vulnerabilidade sob demanda, em um determinado ativo, antes da entrada de uma aplicação em produção ou disponível para a web e também nos casos de incidentes de segurança da informação, por exemplo.

Com as vulnerabilidades identificadas, é gerado um relatório automático pela ferramenta que contém as seguintes colunas citadas abaixo:

IDENTIFICAÇÃO DAS VULNERABILIDADES
ID da Vulnerabilidade;
Serviço / Porta;
Severidade (Crítica / Alta / Média / Baixa / Informativa);

Conforme exemplo abaixo, dentro da coluna **Nome da Vulnerabilidade (Microsoft SQL Server Multiple Vulnerabilities 3199641)**, também podem ser encontrados os campos: sumário, softwares afetados, impacto, solução e referências.

Microsoft SQL Server Multiple Vulnerabilities (3199641)	809096	ms-sql-s (1433/tcp)	Medium
Vulnerability Detection Result: Vulnerable range: 13.0.1000.0 - 13.0.1721.0 **CVSS Base Vector:** AV:N/AC:L/Au:S/C:P/I:P/A:P **Summary:** This host is missing an important security update according to Microsoft Bulletin MS16-136. **Insight:** Multiple flaws exist due to: - The Microsoft SQL Server improperly handles pointer casting. - The SQL Server MDS does not properly validate a request parameter on the SQL Server site. - An improper check of 'FILESTREAM' path. - The SQL Server Agent incorrectly check ACLs on atxcore.dll. **Affected Software/OS:** - Microsoft SQL Server 2012 x86/x64 Edition Service Pack 2 and prior - Microsoft SQL Server 2012 x86/x64 Edition Service Pack 3 and prior - Microsoft SQL Server 2014 x86/x64 Edition Service Pack 1 and prior - Microsoft SQL Server 2014 x86/x64 Edition Service Pack 2 and prior - Microsoft SQL Server 2016 x64 Edition **Impact:** Successful exploitation will allow remote attackers to gain elevated privileges that could be used to view, change, or delete data, or create new accounts, also can gain additional database and file information and to spoof content, disclose information, or take any action that the user could take on the site on behalf of the targeted user. **Solution:** The vendor has released updates. Please see the references for more information. **Vulnerability Detection Method:** Checks if a vulnerable version is present on the target host. **References:** URL:https://technet.microsoft.com/library/security/MS16-136 URL:http://www.securityfocus.com/bid/94037 URL:http://www.securityfocus.com/bid/94060 URL:http://www.securityfocus.com/bid/94043 URL:http://www.securityfocus.com/bid/94050 URL:http://www.securityfocus.com/bid/94061	**Family name:** Windows : Microsoft Bulletins **Category:** infos **Created:** 2016-11-14T10:00:37Z **Modified:** 2022-04-13T13:17:10Z **CVEs:** CVE-2016-7249, CVE-2016-7250, CVE-2016-7251, CVE-2016-7252, CVE-2016-7253, CVE-2016-7254		

6.1.2 Abrir chamado no canal de atendimento de chamados oficial da SETIC

Para cada relatório produzido pelo scanner de vulnerabilidades será aberto um chamado no canal de atendimento oficial, anexado o relatório e encaminhado para a equipe responsável pelo ativo. Também será aberto um chamado pela equipe da GPREV, caso algum alerta identificado seja apontado na monitoração de aletas divulgados pelos desenvolvedores/fabricantes.

É altamente recomendável que sejam utilizadas ferramentas que consolidam os resultados das varreduras em um único local, produzindo *dashboards* que facilitem a gestão das vulnerabilidades encontradas.

6.1.3 Notificar Responsáveis

Diante do relatório de vulnerabilidade produzido, será gerado chamado pela equipe da GPREV via canal de atendimento de chamados oficial da

SETIC e encaminhado ao responsável do ativo para que proceda com as correções de vulnerabilidades encontradas.

Diante dos casos em que a SETIC não seja responsável pela administração do ativo, o relatório será encaminhado via SEI para o órgão responsável dar prosseguimento das correções de vulnerabilidades apontadas no relatório.

6.1.4 Tratar as Vulnerabilidades

A etapa de mitigação é uma das mais importantes e consequentemente a que demanda mais tempo das equipes responsáveis pelos ativos analisados, que devem identificar a melhor forma de tratar os problemas reportados levando em consideração o nível de risco ou pontuação (score) atrelado a cada uma das vulnerabilidades.

Diversos fatores devem ser considerados na escolha do tratamento a ser utilizado em uma vulnerabilidade, como por exemplo, a falta de suporte do fabricante, recursos para o tratamento (financeiros ou humanos), e até mesmo onde o controle sugerido para a correção da vulnerabilidade impacta no funcionamento de sistemas legados, podendo levar a uma aceitação do risco.

A SETIC recomenda observar as boas práticas disponibilizadas na ABNT NBR ISO/IEC 27002:2013, em “Gestão de Vulnerabilidades Técnicas” e de acordo com recomendação da Coordenadoria de Segurança da SETIC (COSEGI), o responsável pelo ativo deverá realizar as correções de vulnerabilidades apontadas no relatório de acordo com o quadro da Matriz de Escalonamento. Caso não seja possível a correção das mesmas, deverá ser apresentada uma solução de contorno ou justificar a não correção das vulnerabilidades.

A GPREVI será responsável por acompanhar o prazo para a correção das vulnerabilidades informadas. É importante que os gestores tenham conhecimento dos relatórios e fragilidades do ambiente.

Score / Nível de Risco	Prazo de Correção	Notificar	Prazo de Correção	Notificar	Prazo de Correção	Notificar
Crítica	7 dias	Responsável pelo Ativo	15 dias	Gerente	30 dias	Diretor
Alta	15 dias		30 dias		60 dias	
Média	30 dias		60 dias		120 dias	
Baixa	60 dias		120 dias		240 dias	

Matriz de Escalonamento

Nos casos em que a SETIC não seja o administrador do ativo, caberá o solicitante ou órgão responsável pelo ativo a correção das vulnerabilidades, conforme portaria n° 18 (0023889794) de 8 de fevereiro de 2022, que define requisitos mínimos para a criação de máquina virtual no ambiente de infraestrutura da rede de computadores da Superintendência Estadual de Tecnologia da Informação e Comunicação do Estado de Rondônia - SETIC/RO e dá outras providências.

6.1.5 Responder Notificação

O responsável pelo ativo deverá responder as notificações geradas, informando quais vulnerabilidades foram corrigidas, e justificando aquelas que não possam ser corrigidas.

6.1.6 Fechar Chamado

Após a remediação das vulnerabilidades ou a justificativa daquelas que não possam ser corrigidas, o chamado deverá ser encerrado.

7 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: 2013;

BRASIL. Guia de Gerenciamento de Vulnerabilidades da Secretaria de Governo Digital;

BRASIL. Guia para Implementação do Processo Gestão de Vulnerabilidades Técnicas da RNP (Rede Nacional de Ensino e Pesquisa);

BRASIL. Processo de vulnerabilidades de segurança da UFBA;

RONDÔNIA. Portaria nº 97/2021/SETIC. Política de Segurança da Informação - PSI da SETIC. Disponível em: http://wiki.setic.ro.gov.br/lib/exe/fetch.php?media=start:docs:psi_setic_-_versao_1.0.pdf; e

SETIC/Governo de Rondônia. RELATÓRIO DE ANÁLISE DE RISCOS;

8 ANEXOS

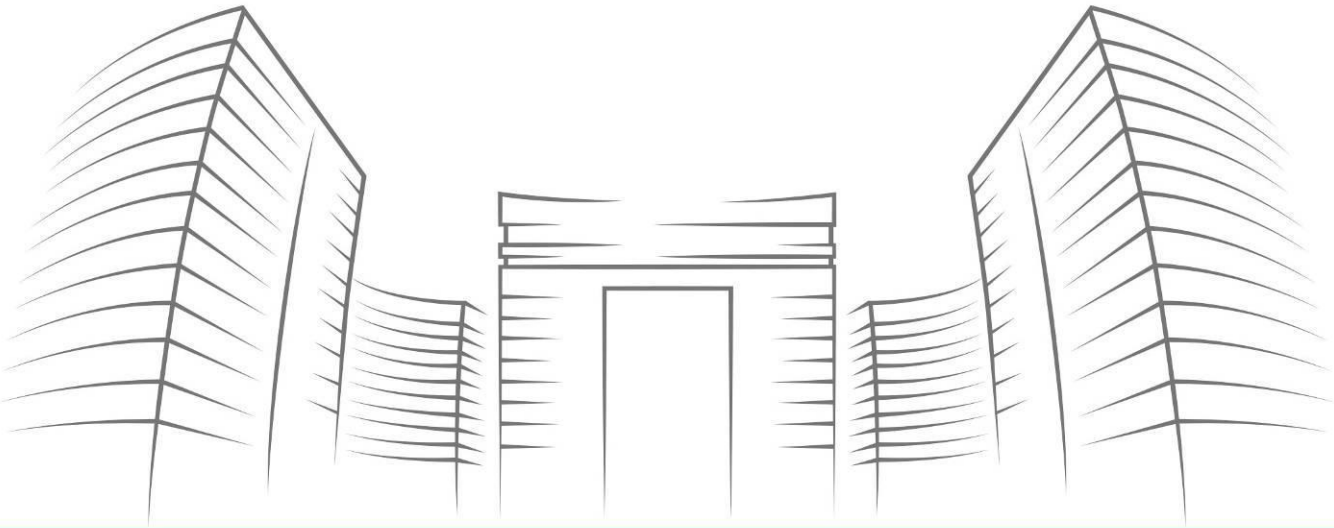
O Anexo está disponível no seguinte endereço: https://wiki.setic.ro.gov.br/home/Base-Conhecimento/ativos_sistemas (link da intranet).

Apontamentos do Abdenildo

SETIC
Superintendência Estadual de
Tecnologia da Informação e Comunicação

Governo do Estado de
RONDÔNIA

Wiki.SETIC | *Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC*
wiki.setic.ro.gov.br



setic.ro.gov.br
@setic.rondonia
Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470