Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PROCESSO GESTÃO DE VULNERABILIDADES

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
02/01/2024	1	Elaboração do processo gestão de vulnerabilidades.

1. INTRODUÇÃO

Um processo de gerenciamento de vulnerabilidades é uma abordagem de segurança da informação utilizada para identificar, avaliar, mitigar e monitorar vulnerabilidades em sistemas, softwares, redes e aplicativos (CIS, 2023). Este processo é essencial para identificar, avaliar e mitigar as fraquezas ou falhas nos sistemas, processos ou ativos que possam ser exploradas por ameaças externas ou internas.

O processo de gestão de vulnerabilidades no IFTO abrange a identificação de ativos e recursos, avaliação e priorização de vulnerabilidades, análise de riscos, plano de mitigação das ameaças, implementação de medidas de controles e correção de falhas, testes e validação das correções, monitoramento contínuo de novas ameaças e conscientização sobre segurança cibernética. Este processo trata potenciais ameaças envolvendo diversos ativos de informação que sustentam os serviços do IFTO, tais como: infraestrutura de redes, sistemas, *softwares*, aplicações web, aplicativos móveis, bancos de dados, sistemas de informação, dentro outros.

Dentro deste contexto, este documento apresenta uma breve introdução, definições, gestão de vulnerabilidades, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1. Escopo

O escopo do processo de gestão de vulnerabilidades abrange um conjunto de atividades que visam garantir a segurança da informação e proteger os ativos de informação do IFTO. Faz parte do escopo deste processo: identificação de ativos, inventário de *software* e *hardware*, descoberta de vulnerabilidades, avaliação de riscos, classificação de vulnerabilidades, correção e mitigação, testes de controles de segurança e comunicação e divulgação, acompanhamento contínuo, gestão de *patches* de correções de segurança, treinamento e conscientização e relatórios de auditorias.

1.2. Objetivos

O objetivo geral do processo de gestão de vulnerabilidades é fortalecer a estratégia de gestão de segurança da informação, reduzir o risco de exposição a ameaças e garantir a resiliência contra potenciais ataques cibernéticos. Para isso foram definidos os seguintes objetivos específicos:

a) identificar e catalogar todas as vulnerabilidades presentes nos sistemas, aplicativos, *softwares* e redes do IFTO;

b) avaliar o risco associado a cada vulnerabilidade, considerando fatores como probabilidade de exploração e impacto potencial;

c) priorizar as vulnerabilidades com base em sua criticidade e no risco associado, permitindo a alocação eficiente de recursos para mitigar as ameaças mais críticas; e

d) definir medidas para mitigar ou corrigir vulnerabilidades identificadas, seja por meio de aplicação de patches de correção, configurações de segurança, atualizações de *softwares* ou outras ações.

1.3. Abrangência

O processo de gestão de vulnerabilidades abrange vários aspectos de segurança da informação, tais como: identificação de ativos, avaliação de riscos, varredura e detecção de vulnerabilidades, priorização de correções, mitigação ou correção de vulnerabilidades, testes de segurança pós-mitigação, monitoramento contínuo, treinamento e conscientização, comunicação interna e externa, conformidade legal e regulatória, gestão de incidentes, análise de tendências e relatórios e gestão de fornecedores.

1.4. Benefícios esperados

A execução do processo de gestão de vulnerabilidades acarreta os seguintes benefícios:

a) permite identificar e corrigir vulnerabilidades antes que sejam exploradas por ameaças, reduzindo o potencial de ataques;

b) reduz a exposição a riscos de segurança cibernética, protegendo os sistemas e dados do IFTO;

c) antecipa e mitiga vulnerabilidades reduz o impacto de possíveis incidentes de segurança, minimizando danos financeiros e operacionais;

d) ajuda a atender a padrões e regulamentações de segurança, assegurando conformidade legal e evitando penalidades;

e) melhoria contínua da segurança e aumenta a confiabilidade dos sistemas e serviços oferecidos pelo IFTO;

f) ações proativas para gerenciar vulnerabilidades e demonstrar o compromisso com a segurança, preservando a reputação do IFTO;

g) evita custos associados a violações de segurança, como recuperação de dados, multas, perda de clientes e gastos com reparos emergenciais;

h) identifica e corrigi vulnerabilidades que podem levar a um ambiente de TI mais estável e eficiente, contribuindo para a produtividade geral do IFTO;

i) implementa uma estratégia de gestão de vulnerabilidades, tornando o IFTO capaz de antecipar e lidar com ameaças futuras; e

j) estabelece uma cultura de segurança transparente, gerando confiança entre usuários e partes interessadas.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições:

a) alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal;

b) ataque: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

c) evento: Qualquer mudança de estado que tenha significância para o gerenciamento de um serviço de TI ou outro item de configuração. O termo também pode ser usado para significar um alerta ou notificação criada por qualquer serviço de TI, Item de Configuração ou uma ferramenta de monitoramento. Os eventos normalmente exigem que o pessoal de operações de TI tome medidas e muitas vezes levam a incidentes, os quais devem ser registrados;

d) incidente: interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado;

e) informação: qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da empresa ou estar sob sua custódia;

f) resposta a incidentes: medidas tomadas para a preparação, detecção, resposta, contenção e recuperação de um incidente de segurança, além de todas as atividades pós incidente e de conscientização;

g) vulnerabilidade: situação que coloca o IFTO em uma posição mais suscetível a ataques e ações mal-intencionadas. Exemplo: vulnerabilidades de rede, softwares desatualizados e ausência de uma política de segurança da informação bem estruturada; e

h) usuário: qualquer indivíduo com direitos de acesso aprovado.

3. GESTÃO DE VULNERABILIDADES

A gestão de vulnerabilidades é um processo contínuo e sistemático que visa identificar, avaliar, priorizar e mitigar as vulnerabilidades presentes na infraestrutura de redes, sistemas operacionais, *softwares*, sistemas de informação, aplicativos e demais ativos de uma instituição. Esta abordagem envolve:

a) correção ou mitigação de vulnerabilidades: uma vez priorizadas, as vulnerabilidades são corrigidas ou mitigadas. Isso pode incluir aplicar patches de segurança, atualizar *software*, reconfigurar sistemas ou implementar novas políticas de segurança;

b) verificação de vulnerabilidades: após a correção ou mitigação, é essencial verificar se as ações tomadas foram eficazes. Testes de penetração, varreduras de segurança e avaliações

adicionais podem ser realizados para garantir que a vulnerabilidade tenha sido resolvida adequadamente;

c) monitoramento contínuo: a segurança não é um destino final, é um processo contínuo. É crucial monitorar constantemente os sistemas e redes em busca de novas vulnerabilidades, especialmente com as atualizações regulares de *software* e as mudanças no ambiente de ameaças.

d) educação e conscientização: são partes essenciais da gestão de vulnerabilidades. Treinamentos sobre boas práticas de segurança, políticas internas e procedimentos podem ajudar a prevenir muitas vulnerabilidades.

e) documentação e relatórios: manter registros detalhados das vulnerabilidades identificadas, ações tomadas e lições aprendidas é fundamental para melhorar continuamente o processo de gestão de vulnerabilidades. Relatórios periódicos são úteis para avaliar o progresso e identificar áreas que precisam de melhorias.

Com esta abordagem de gestão de vulnerabilidades, o IFTO fortalece sua postura de segurança, reduzindo o risco de ameaças cibernéticas e mantém a integridade, confiabilidade e disponibilidade dos ativos e dados essenciais.

3.1. Processo de gestão de vulnerabilidades

O processo de gestão de vulnerabilidades tem como objetivo reduzir riscos de ataques cibernéticos e proteger a infraestrutura de Tecnologia da Informação. A partir da execução das fases deste processo, o IFTO pode diminuir suas superfícies de ataques cibernéticos, identificar e remover erros de configuração e problemas de segurança que possam ser explorados e gerenciar *patches* de segurança de sistemas e *software*. A figura 1 apresenta as 4 (quatro) fases deste processo que são executadas de forma interativa e incremental.

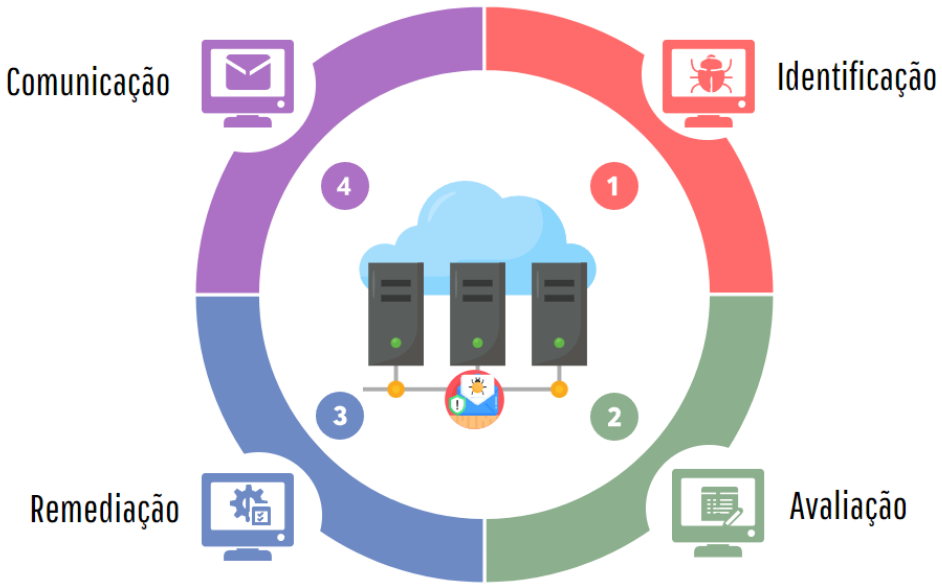


Figura 1 - Processo de gestão de vulnerabilidades

O processo de gestão de vulnerabilidades é caracterizado por sua natureza flexível e adaptável, permitindo ajustes, melhorias e refinamentos contínuos ao longo do tempo. As fases do processo de gestão de vulnerabilidades serão detalhadas na tabela 1.

Tabela 1 - Detalhamento do processo de gerenciamento de vulnerabilidades

Processo de gerenciamento de vulnerabilidades	
Entrada	- logs de sistemas, softwares e dispositivos.
Fases	1. Identificação. 2. Avaliação. 3. Remediação. 4. Comunicação.
Saída	- Relatórios de gestão de vulnerabilidades.

3.1.1. Identificação

Fase responsável por realizar o levantamento e a análise minuciosa dos sistemas, aplicativos, *softwares*, redes e processos para identificar possíveis falhas ou pontos fracos que possam ser explorados por ameaças. Nesta fase o escopo é definido e avaliado. Ela envolve a execução das seguintes atividades:

a) preparar as ferramentas necessárias e verificar sua integridade;

b) verificar os ativos de TI do IFTO para encontrar vulnerabilidades conhecidas e potenciais ameaças;

c) realizar testes de vulnerabilidades e os resultados obtidos; e

d) monitorar regularmente os registros de *logs* para identificar quaisquer tentativas de exploração de vulnerabilidades.

3.1.2. Avaliação

Fase responsável por compreender o impacto e a criticidade das vulnerabilidades identificadas, priorizando as ações necessárias para mitigá-las. Ela envolve a execução das seguintes atividades:

a) coletar e analisar as informações disponíveis sobre vulnerabilidades, incluindo *logs* e outros registros gerados pelos recursos, sistemas e serviços de TI;

b) realizar varreduras automatizadas de vulnerabilidade de ativos corporativos internos trimestralmente ou com maior frequência. Realizar varreduras autenticadas e não autenticadas, usando uma ferramenta de varredura de vulnerabilidade compatível com SCAP;

c) executar varreduras de vulnerabilidade automatizadas de ativos corporativos expostos externamente usando uma ferramenta de varredura de vulnerabilidade;

d) avaliar a integridade do resultado de detecção de vulnerabilidades;

e) identificar a existência de outros eventos e alertas relacionados com o vulnerabilidade em questão;

f) identificar que tipo de informação e processos podem ser afetados com a vulnerabilidade;

g) avaliar a relevância e o impacto da vulnerabilidade, a fim de definir quais medidas devem ser tomadas para a remediação; e

h) classificar/categorizar a severidade das vulnerabilidades identificadas e atribuir a elas um nível de prioridade de acordo com a gravidade e o risco real.

3.1.3. Remediação

Esta fase responsável por corrigir as vulnerabilidades encontradas. Nesta fase ações são tomadas para corrigir ou mitigar as vulnerabilidades identificadas e avaliadas. Ela envolve a execução das seguintes atividades:

a) estabelecer e manter uma estratégia de remediação baseada em risco documentada com revisões mensais ou mais frequentes;

b) executar atualizações do sistema operacional em ativos corporativos por meio do gerenciamento automatizado de *patches* mensalmente ou com maior frequência;

c) realizar atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de *patches* mensalmente ou com maior frequência de formar a corrigir as vulnerabilidades;

d) tratar vulnerabilidades com base na priorização realizada a partir da classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio; e

e) corrigir as vulnerabilidades detectadas no *software* por meio de processos e ferramentas em uma base mensal, ou mais frequente, com base no processo de correção.

3.1.4. Comunicação

Fase responsável por garantir que todas as partes interessadas estejam cientes das vulnerabilidades identificadas, das medidas de remediação tomadas e das ações realizadas. Ela envolve a execução das seguintes atividades:

a) caracterizar o conjunto de lições aprendidas de modo a aprimorar os procedimentos e processos existentes;

b) identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe;

c) prover estatísticas e métricas relativas ao processo de resposta a incidentes;

d) obter informações que podem ser utilizadas em processos legais;

e) confirmar o restabelecimento da normalidade dos recursos computacionais;

f) registrar as ações realizadas durante o processo de remediação, incluindo as vulnerabilidades identificadas, as soluções aplicadas e os resultados dos testes;

g) registrar lições aprendidas e *feedback* com usuário; e

h) atualizar políticas e procedimentos.

4. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Os papéis e responsabilidades dos envolvidos no processo de gestão de vulnerabilidades são:

4.1. Alta Administração

Representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal. Cabe ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de gestão de vulnerabilidades, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) garantir os recursos (humanos, tecnológicos e financeiros) para a execução da gestão de vulnerabilidades no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

Grupo de pessoas que representam áreas finalísticas do IFTO. Cabe a este grupo de pessoas as seguintes responsabilidades:

a) avaliar e aprovar a política, norma interna complementar e o processo de gestão de vulnerabilidades; e

b) propor melhorias para a política, norma interna complementar e o processo de gestão de vulnerabilidades.

4.3. Gestor de Segurança da Informação

Servidor designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) elaborar e coordenar o processo de gestão de vulnerabilidades; e

b) realizar ajustes no processo de gestão de vulnerabilidades com a finalidade de estar em conformidade com a legislação vigente no âmbito da administração pública federal.

4.4. Equipe de Tratamento e Resposta à Incidentes Cibernéticos - ETIR

Grupo de pessoas composto por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades dessa equipe. Compete à estas pessoas a seguinte responsabilidade:

a) avaliar a política ou norma interna complementar e o processo de gestão de vulnerabilidades, bem como as medidas de controle adotadas para o processo.

4.5. Setor de TI (Diretoria de Tecnologia da Informação e demais Setores de TI das unidades do IFTO)

Agente responsável pela gestão de vulnerabilidades. Cabe ao setor as seguintes responsabilidades:

a) designar um agente responsável pela execução das atividades referentes ao processo de gestão de vulnerabilidades, dentre os servidores efetivos do IFTO;

b) identificar e classificar as vulnerabilidades por nível de criticidade;

c) avaliar as vulnerabilidades de acordo com o nível de criticidade;

d) realizar as correções de vulnerabilidades de acordo com os controle de segurança da informação utilizados pelo IFTO; e

e) comunicar os resultados obtidos com a execução do processo de gestão de vulnerabilidades à alta administração, ETIR e CSI.

4.6. Usuários

Pessoa que pode tornar os ativos institucionais vulneráveis. Cabe à esta pessoa:

a) respeitar os princípios da finalidade e uso de ativos de TI estabelecido nas políticas e normas de segurança da informação do IFTO;

b) utilizar os ativos de informação no IFTO prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade; e

c) não entregar os computadores, componentes internos, como HDs, e equipamentos em geral a pessoas sem autorização.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 2 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed*.

a) responsible (responsável): pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo; representa quem irá, de fato executar a tarefa; deve haver ao menos um por tarefa;

b) accountable (responsabilizado): dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *accountable*; define quem será responsável pelo sucesso da atividade; fica encarregado de verificar se a atividade foi realizada com sucesso e dentro do prazo; deve haver um, e apenas um, por atividade;

c) consulted (consultado): pessoa que deve ser consultada durante a execução da atividade; ss informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; geralmente exercem papel de conselho na tomada de decisões;

d) ***informed (informado):*** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Fase	CSI	GSI	ETIR	STI	U
Detecção	A	C	C	R	I
Avaliação	A	C	C	R	I
Remediação	A	C	C	R	I
Comunicação	A	C	C	R	I

Legenda:

AA: Alta Administração

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta à Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação

U: Usuário

6. INDICADOR DE DESEMPENHO

O processo de gerenciamento de vulnerabilidades deve ser monitorado e avaliado periodicamente através de indicador de desempenho de forma a realizar eventuais ajustes necessários. Esse monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 3 apresenta o indicador de desempenho do processo.

Tabela 3 - Indicador de Desempenho

Indicador	Vulnerabilidades corrigidas durante o ano.
Descrição	Número de vulnerabilidades corrigidas durante o ano.
Objetivo	Medir o percentual de vulnerabilidades corrigidas durante o ano.
Periodicidade	Anual
Fonte	Diretoria de Tecnologia da Informação
Fórmula	Total de vulnerabilidades corrigidas durante o ano.
Meta	Monitorar a quantidade de vulnerabilidades corrigidas a cada ano.

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o processo de gestão de vulnerabilidades está interligado à outros processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 2 apresenta estes processos.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

As práticas recomendadas para o processo de gestão de vulnerabilidades incluem:

1. Uma política ou norma interna complementar deve ser estabelecida e mantida atualizada, contendo diretrizes, competências e responsabilidades para a gestão de vulnerabilidades, a fim de prevenir ataques cibernéticos.

2. O processo de gestão de vulnerabilidades deve ser revisado e atualizado anualmente ou quando ocorrerem mudanças significativas no IFTO.

3. Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas e a exposição do IFTO a tais vulnerabilidades deve ser avaliada, tomando medidas adequadas.

4. Um inventário atualizado de ativos institucionais deve ser mantido e atualizado regularmente de forma a identificar vulnerabilidades presentes em sistemas operacionais, *softwares*, aplicativos, sistemas de informação e serviços de TI, utilizando ferramentas de escaneamento e testes de segurança.

5. As vulnerabilidades identificadas devem ser classificadas e priorizadas com base no seu impacto potencial e na probabilidade de exploração, focando nas mais críticas e urgentes.

6. Sistemas e *softwares* devem ser mantidos atualizados com as últimas correções de segurança e atualizações de *software*, aplicando patches regularmente para fechar brechas conhecidas.

7. Políticas e práticas de gerenciamento de acesso devem ser estabelecidas controlando quem tem acesso a sistemas e dados sensíveis, reduzindo as chances de exploração por meio de acesso não autorizado.

8. Ferramentas de monitoramento de segurança da informação devem ser implementadas para fornecer alertas em tempo real sobre atividades suspeitas ou vulnerabilidades emergentes.

9. Testes de invasão devem ser realizados regularmente e simulações de ataques devem ser feitas para avaliar a resistência dos sistemas e identificar possíveis brechas não detectadas.

10. Um plano de resposta a incidentes deve ser desenvolvido, documentando os procedimentos a serem seguidos em caso de violações de segurança, garantindo uma resposta rápida e eficaz.

11. Os usuários devem ser conscientizados sobre as boas práticas de segurança cibernética, pois muitas vulnerabilidades surgem de ações humanas inadvertidas.

12. Uma comunicação clara e eficiente entre as equipes de segurança, TI, desenvolvimento e outras partes interessadas devem ser mantidas para garantir ações coordenadas na gestão de vulnerabilidades.

13. Procedimentos e tecnologias de segurança devem ser revisadas regularmente com base nas novas ameaças e vulnerabilidades identificadas, buscando constantemente aprimorar a postura de segurança do IFTO.

14. O IFTO deve realizar quando possível varreduras automatizadas de vulnerabilidade em ativos institucionais internos.

15. O IFTO deve realizar quando possível varreduras automatizadas de vulnerabilidade em ativos institucionais expostos externamente.

16. O IFTO deve realizar quando possível atualizações do sistema operacional em ativos institucionais por meio da gestão automatizada de *patches* mensalmente ou com mais frequência.

17. O IFTO deve realizar quando possível atualizações de aplicações em ativos institucionais por meio da gestão automatizada de patches mensalmente ou com mais frequência.

18. O IFTO deve estabelecer uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.

19. O IFTO deve corrigir as vulnerabilidades detectadas no *software* por meio de processos e ferramentas mensalmente, ou com mais frequentemente, com base no processo de correção.

9. **REFERÊNCIAS**

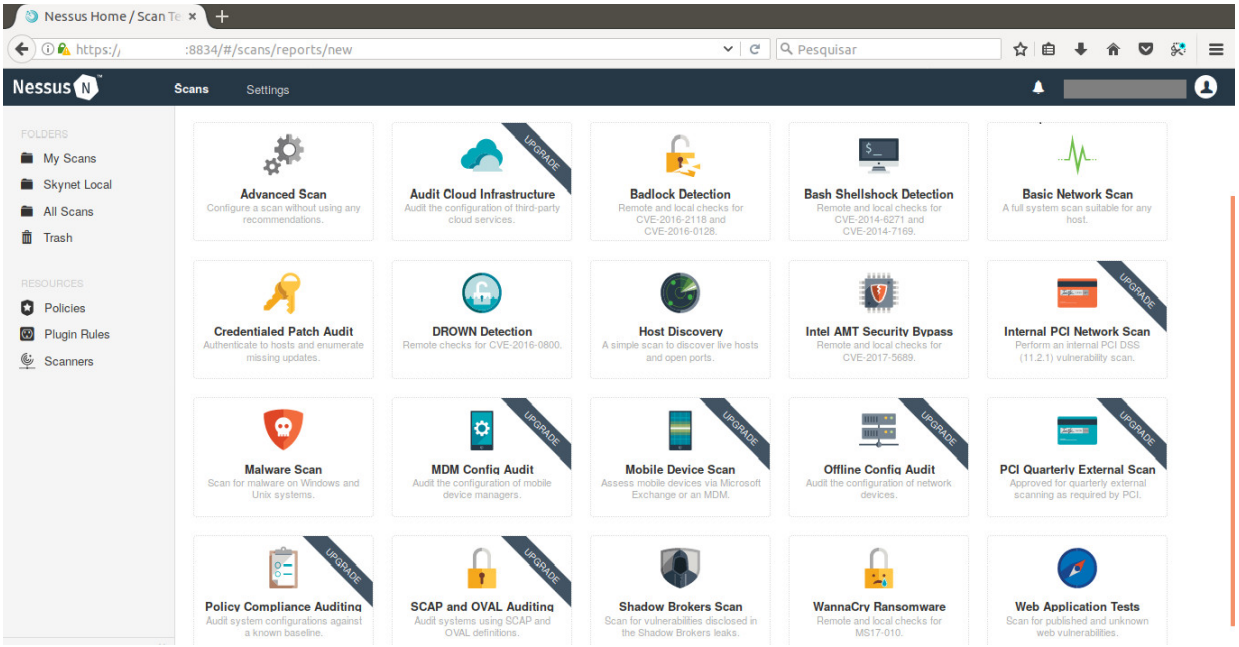
BRASIL. Ministério da Gestão e da Inovação em Serviços Pũblicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 852, de 28 de março de 2023: dispõe o Programa de Privacidade e Segurança da Informação. Disponível em:** https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908 Acessp em: 11 dez. 2023.

CENTER FOR INTERNET SECURITY. **Controle 7: gestão de vulnerabilidades.** Disponível em: https://www.cisecurity.org/ Acesso em: 5 dez. 2023.

UNIVERSIDADE FEDERAL DE LAVRAS. **Plano de Gestão de Incidentes de Segurança da Informação e Privacidade.** UFLA, 2021. Disponível em: https://dgti.ufla.br/images/politicas-e-normas/Plano_Gestao_Incidentes_v12_assinado.pdf Acesso em: 21 dez. 2021.

ANEXO I

MONITORAMENTO DE VUNERABILIDADES



ANEXO II
PLANO DE TRATAMENTO DE VULNERABILIDADES

O Plano de Gestão de Vulnerabilidades estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de potenciais ameaças, orientando o funcionamento do processo, de forma que este seja tratado adequadamente, reduzindo ao máximo os impactos para o negócio.

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pelo IFTO. A tabela 1 apresenta as atividades e tarefas que compõem o plano de ação de gestão de vulnerabilidades.

Tabela 1 - Ações para resposta e tratamento de vulnerabilidades

Fase	Atividade	Responsável
Identificação	Estabelecer sistemas e ferramentas de detecção de incidentes, como sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS).	CRSI
	Monitorar constantemente as atividades de rede e sistema em busca de indicadores de comprometimento (IOCs) e comportamentos suspeitos.	CRSI
Avaliação	Realizar uma análise detalhada de potenciais ameaças para entender como ocorre e quais sistemas podem ser afetados.	DTI
	Desenvolver critérios para classificar e priorizar as vulnerabilidades com base em sua gravidade, impacto e probabilidade.	CRSI
	Alocar recursos de forma eficiente para as vulnerabilidades mais críticas.	DTI
	Determinar a extensão do comprometimento e identifique a origem da vulnerabilidade.	CRSI

Remediação	Isolar sistemas ou redes afetados para evitar a propagação da ameaça.	CRSI
	Preservar e coletar evidências relevantes para a investigação posterior.	CRSI
	Desenvolver e implementar medidas para mitigar o impacto da vulnerabilidade e restaurar a operação normal.	CRSI
	Certificar-se de que as vulnerabilidades exploradas sejam corrigidas e de que as medidas de segurança sejam reforçadas.	CRSI
Comunicação	Estabelecer um plano de comunicação interna e externa para manter as partes interessadas informadas sobre vulnerabilidades.	DTI
	Comunicar-se com as autoridades competentes, se necessário, dependendo da natureza da vulnerabilidades.	DTI
	Após a resolução da vulnerabilidade, realizar uma análise pós-remediação para identificar o que funcionou bem e o que pode ser melhorado no processo de resposta.	CRSI
	Aplicar as lições aprendidas para atualizar o plano de resposta a vulnerabilidades e fortalecer a postura de segurança.	CRSI
	Treinar regularmente os usuários em como identificar e lidar com vulnerabilidades.	GSI
	Realizar simulações de invasão para testar a eficácia do plano de resposta e identificar vulnerabilidades.	GSI
	Manter registros detalhados de todos as vulnerabilidades, ações tomadas e resultados da investigação.	CRSI

ANEXO III
CONTATO PARA NOTIFICAÇÃO DE VULNERABILIDADES

Equipe de Tratamento e Resposta a Incidentes Cibernéticos
Telefone: (63) 2229-2200
E-mail: etir@ifto.edu.br
Endereço:
Prédio da Reitoria
Avenida Joaquim Teotônio Segurado, Quadra 202 sul, ACSU-SE 20, Conjunto 1, Lote 8.

Palmas-Tocantins

CEP 77020-450

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 02/01/2024, às 16:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2218385** e o código CRC **34979F50**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.022952/2023-21 SEI nº 2218385