INSTRUÇÃO NORMATIVA 1/2025/REIT - CGAB/REIT

PROCESSO SEI Nº 23243.004192/2024-51

DOCUMENTO SEI Nº 2521035

Estabelece a Política de Gestão de Vulnerabilidades no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Rondônia (IFRO).

Instrução Normativa aprovada na 79ª Reunião Ordinária do Colégio de Dirigentes (CODIR) do Instituto Federal de Educação, Ciência e Tecnologia do Rondônia (IFRO), realizada nos dias 18 e 19 de dezembro de 2024, em formato híbrido. Processo SEI nº 23243.007386/2024-17.

CAPÍTULO I

DO ESCOPO

Art. 1º A Política de Gerenciamento de Vulnerabilidades tem o objetivo de estabelecer diretrizes, competências e responsabilidades para um processo contínuo e estruturado de identificação, avaliação, documentação, priorização, mitigação, remediação e comunicação de vulnerabilidades relacionadas a recursos, sistemas operacionais, *softwares*, infraestrutura, sistemas de informação e serviços de TI de forma a protegê-los contra potenciais ameaças cibernéticas, minimizando o risco de exploração de vulnerabilidades.

Art. 2º Esta política se aplica aos ativos de TI, incluindo recursos, infraestrutura de redes, sistemas operacionais, bancos de dados, sistemas de informação, aplicações, *softwares* e serviços de TI, funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem esses ativos.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins de compreensão dos termos utilizados neste documento serão utilizados os seguintes conceitos e definições:

I. ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

II. atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzam ou suportem um ou mais produtos ou serviços;

III. ativo: tudo que tenha valor para a organização, material ou não;

IV. ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

V. banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VI. Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

VII. Equipe de Tratamento e Resposta à Incidentes Cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade.

VIII. evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

IX. *firewall*: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de *hardware* ou *software*, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

X. *host*: um computador ou dispositivo de TI (por exemplo, roteador, *switch*, *gateway*, *firewall*);

XI. gerenciamento de vulnerabilidade: processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;

XII. gestor de segurança da informação: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

XIII. *log* (registro de auditoria): registro de eventos relevantes em um dispositivo ou sistema computacional;

XIV. *patch*: uma parte de código adicional desenvolvido para resolver um problema ou falha em um *software* existente;

XV. risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

XVI. teste de invasão: metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante;

XVII. teste de penetração (PENTEST): também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos *softwares* que estão sendo utilizados pelo IFRO;

XVIII. vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha; e

XIX. usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º Esta política considera os seguintes princípios:

I. respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a Administração Pública Federal;

II. garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFRO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III. alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV. responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V. conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5º As diretrizes gerais constituem os pilares da gestão de segurança da informação no IFRO, norteando a elaboração de normas, planos, procedimentos, metodologias, ações e controles que garantem que os princípios de segurança da informação definidos nesta PSI sejam atingidos.

§ 1º A política deve estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura organizacional do IFRO, bem como ao Plano Diretor de Tecnologia da Informação.

§ 2º A equipe de TI, servidores, estudantes e prestadores de serviço, fornecedores e partes interessadas devem ser conscientizados sobre as melhores práticas de segurança, incluindo a identificação e mitigação de vulnerabilidades.

§ 3º O IFRO deve monitorar continuamente os sistemas em busca de novas vulnerabilidades e garantir que as correções aplicadas sejam eficazes.

§ 4º Usuários devem ser conscientizados sobre boas práticas de segurança cibernética para reduzir a probabilidade de exploração de vulnerabilidades por meio de ações não intencionais ou falhas de segurança.

CAPÍTULO V

DA GESTÃO DE VULNERABILIDADES

Art. 6º O gerenciamento de vulnerabilidades consiste em identificar, avaliar, remediar e comunicar vulnerabilidades em recursos, sistemas operacionais, infraestrutura de redes, banco de dados, sistemas de informação, *softwares* e serviços de TI de forma a garantir que os ativos institucionais tenham condições seguras de uso.

§ 1º Um processo de gestão de vulnerabilidades deve ser estabelecido pela Equipe de Tratamento e Resposta de Incidentes Cibernéticos, documentado e atualizado continuamente para proteger ativos críticos de TI contra ameaças cibernéticas e garantir a continuidade dos negócios e a confiança dos usuários.

§ 2º A gestão de vulnerabilidades deve permitir a implementação de mecanismos para obter informações oportunas sobre potenciais ameaças a infraestrutura, sistemas e ativos de informação, a avaliação da exposição do IFRO a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.

§ 3º A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

SEÇÃO I

DA IDENTIFICAÇÃO

Art. 7º Um inventário atualizado de todos os ativos de TI, incluindo *hardware*, *software*, sistemas, banco de dados, sistemas de informação e dados, deve ser estabelecido, documentado e mantido continuamente para uma melhor compreensão do que precisa ser protegido.

§ 1º O mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades para determinar qual marca, modelo e versão de equipamento de *hardware*, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de *software* são

usados no IFRO.

§ 2º A identificação de vulnerabilidades deve envolver a busca ativa por falhas de segurança conhecidas em sistemas, infraestrutura de TI, redes e aplicativos.

§ 3º As varreduras de vulnerabilidades devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.

§ 4º As ferramentas utilizadas nas varreduras de vulnerabilidades devem ser ajustadas continuamente, de forma a evitar erros no mapeamento de brechas de segurança da informação.

§ 5º A varredura de vulnerabilidades pode ser feita por meio de scanners de vulnerabilidades, testes de penetração e acompanhamento de alertas de segurança.

§ 6º Sempre que possível a varredura de vulnerabilidades deve ser realizada de forma automatizada.

SEÇÃO II

DA AVALIAÇÃO

Art. 8º Avaliações periódicas de vulnerabilidades usando scanners, testes de penetração e auditorias de segurança devem ser realizadas para identificar e entender as vulnerabilidades existentes.

§ 1º Na medida do possível, testes de invasão ou penetração (PENTEST) devem ser realizados para fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal do IFRO.

§ 2º As vulnerabilidades identificadas devem ser avaliadas para determinar seu impacto potencial e a probabilidade de serem exploradas, devendo ser classificadas com base na gravidade, alcance e risco que representam para o IFRO.

§ 3º Sempre que possível, deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de *software*, que precisam ser aplicadas aos sistemas e ativos informacionais do IFRO.

§ 4º As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

§ 5º Vulnerabilidades devem ser priorizadas com a finalidade de direcionar recursos para as mais críticas e urgentes. Fatores como a criticidade do sistema afetado, a facilidade de exploração e a disponibilidade de patches ou soluções devem ser considerados na priorização.

§ 6º A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

SEÇÃO III

DA REMEDIAÇÃO

Art. 9º A mitigação e remediação deve envolver a aplicação de correções, patches de segurança, atualizações de *software* ou implementação de contramedidas para reduzir ou eliminar as vulnerabilidades.

§ 1º O tratamento de vulnerabilidades deve ser priorizado com base em sua 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 do IFRO.

§ 2º As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados pela ETIR.

2º As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados pela Equipe de Tratamento e Resposta de Incidentes Cibernéticos.

§ 3º Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

§ 4º Mecanismos para obter atualizações de *softwares* devem ser estabelecidos, quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como: sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

§ 5º Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

§ 6º As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de logs.

§ 7º Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de *software*.

§ 8º Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do processo de gestão de mudanças para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

§ 9º As correções bem-sucedidas de falhas ou brechas de segurança da informação poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (PENTEST) e verificação das definições de configuração.

SEÇÃO IV

DA COMUNICAÇÃO

Art. 10 O IFRO deve comunicar os resultados das avaliações de vulnerabilidades, as ações tomadas e os riscos residuais para as partes interessadas.

§ 1º As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.

§ 2º A equipe de gerenciamento de vulnerabilidades deve elaborar relatórios após cada ciclo de detecção para auxiliar o IFRO a entender e mensurar as vulnerabilidades existentes.

§ 3º Os relatórios de vulnerabilidades devem ser compartilhados com o gestor de segurança de informação e ETIR.

CAPÍTULO VI

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

SEÇÃO I

DA ALTA ADMINISTRAÇÃO

Art. 11 Compete à alta administração:

I. prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

II. destinar recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas à gestão de vulnerabilidades no âmbito do IFRO.

SEÇÃO II

DO GESTOR DE TECNOLOGIA DA INFORMAÇÃO

Art. 12 Compete ao Gestor de Tecnologia da Informação:

I. planejar, implementar e melhorar continuamente os controles de vulnerabilidades em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

SEÇÃO III

DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 13 Compete ao Gestor de Segurança da Informação:

Compete ao Gestor de Segurança da Informação:

I. coordenar a elaboração e a revisão da Política de Gestão de Vulnerabilidades e da norma interna complementar, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República.

II. assessorar a alta administração na implantação da Política de Gestão de Vulnerabilidades;

III. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à vulnerabilidades;

IV. propor recursos necessários às ações de gestão de vulnerabilidades;

V. verificar os resultados dos trabalhos de auditoria sobre a gestão de vulnerabilidades; e

VI. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de vulnerabilidades.

SEÇÃO IV

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 14 Compete ao Comitê de Segurança da Informação:

I. planejar, implementar e melhorar continuamente os controles de vulnerabilidades em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

II. deliberar sobre a política e norma interna complementar sobre gestão de vulnerabilidades;

III. assessorar a implementação das ações de gestão de vulnerabilidades; e

IV. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre gestão de vulnerabilidades.

SEÇÃO V

DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS

Art. 15 Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I. deliberar sobre procedimentos internos para gestão de vulnerabilidades;

II. receber, analisar e responder às notificações e atividades relacionadas a gestão de vulnerabilidades;

III. desenvolver as atividades de prevenção, tratamento e resposta a incidentes relacionados à vulnerabilidades em sistemas, aplicações, sistemas de informação e serviços de TI; e

IV. propor diretrizes e responsabilidades para a política e norma interna complementar sobre gestão de vulnerabilidades.

SEÇÃO VI

DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E DEMAIS SETORES DE TI NAS UNIDADES DO IFRO

Art. 16 Compete à Diretoria de Gestão de Tecnologia da Informação e demais setores de TI nas suas respectivas unidades do IFRO:

I. pesquisar, implantar e manter soluções para gestão de vulnerabilidades no âmbito do IFRO;

II. propor e gerenciar procedimentos de gestão de vulnerabilidades;

III. implantar, configurar, gerenciar e monitorar a estrutura de mitigação de vulnerabilidades; e

IV. propor diretrizes e responsabilidades para a política e norma interna complementar sobre gestão de vulnerabilidades.

SEÇÃO VII

DOS USUÁRIOS

Art. 17 Compete aos usuários:

I. atender aos princípios e diretrizes contidos nesta política, incluindo norma interna complementar e procedimentos complementares destinados à segurança da informação e comunicação; e

II. guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

CAPÍTULO VII

DAS PENALIDADES

Art. 18 Ações que violem esta política, norma interna complementar, processo, procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Parágrafo único. Casos omissos não tratados neste documento serão submetidos, analisados, tratados e decididos pelo Comitê de Segurança da Informação.

CAPÍTULO VIII

DA REVISÃO E ATUALIZAÇÃO

Art. 19 Esta política bem como norma interna complementar e os documentos gerados a partir dela deverão ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas normativas do IFRO e quando considerada necessária pelo Comitê de Segurança da Informação.

CAPÍTULO IX

DAS DIRETRIZES FINAIS

Art. 20 As regras, procedimentos, medidas e controles de gestão de vulnerabilidades serão apresentadas em norma interna complementar, que detalharão suas particularidades e procedimentos relativos à segurança da informação alinhados às diretrizes emanadas pelo Comitê de Segurança da Informação e aos

respectivos planos institucionais e estrutura organizacional do IFRO.

Art. 21 Esta política e suas atualizações, bem como norma interna complementar, devem ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 22 Esta Instrução Normativa entra em vigor na data de sua assinatura.

MOISÉS JOSÉ ROSA SOUZA
Reitor
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO)

Documento assinado eletronicamente por **Moisés José Rosa Souza**, **Reitor(a)**, em 25/02/2025, às 18:54, 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 https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2521035** e o código CRC **3778D5BE**.

Referência: Processo nº 23243.004192/2024-51 SEI nº 2521035