Boletim Pessoal IX
do mês de Março de
2024
Expedido em
14/03/2024

**MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS**
**INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**

# INSTRUÇÃO NORMATIVA/INPI/PR Nº 01, DE 29 DE FEVEREIRO DE 2024

**O PRESIDENTE DO INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI**, no uso das atribuições que lhe conferem o Regimento Interno, aprovado por meio da Portaria do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) nº 11, de 27 de janeiro de 2017, com base no previsto na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 9.637, de 26 de dezembro de 2018, no Decreto nº 10.332, de 29 de abril de 2020 e na Portaria/INPI/PR nº 65, de 01 de setembro de 2022, na Portaria SGD/MGI nº 852, de 28 de março de 2023, na Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, na ABNT/ISO/IEC 27001:2013, assim como o constante nos autos do processo INPI nº 52402.012075/2022-28,

**RESOLVE:**

Art. 1º Aprovar, no âmbito do INPI, a Política de Gestão e Análise de Vulnerabilidade do parque computacional e sistemas de informação, em complemento às diretrizes estabelecidas pelo Capítulo I, Seção XIII, da Política de Segurança da Informação do INPI, PORTARIA/INPI/PR nº 65, de 1° de setembro de 2022.

## CAPÍTULO I
## DAS DISPOSIÇÕES GERAIS

Art. 2º Para efeitos desta norma são estabelecidos os seguintes conceitos e definições:

I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

II - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

III - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

IV - ativo de informação: todo dado ou informação gerado, adquirido, utilizado ou custodiado pelo INPI, assim como qualquer equipamento, **software** ou recurso utilizado para seu processamento ou armazenamento;

V - análise de vulnerabilidades: processo de reconhecimento, análise e classificação de falhas relacionadas à segurança da infraestrutura de tecnologia. A partir desse processo, é possível entender os pontos fracos na cibersegurança, e adotar as medidas necessárias para corrigir as fragilidades de todo o ambiente;

VI - teste de penetração (**Pentest**): metodologia para testar a eficácia e a resiliência dos ativos de informação, através da identificação e exploração de fraquezas nos controles de segurança, e da simulação das ações e objetivos de um atacante; e

VII - CGTI: Coordenação-Geral de Tecnologia da Informação.

## CAPÍTULO II
## DAS COMPETÊNCIAS

Art. 3º Compete ao Gestor de Segurança da Informação:

I - acompanhar a evolução das vulnerabilidades e ameaças referentes ao ambiente computacional e sistemas de informação;

II - realizar ou acompanhar a realização de testes e varreduras nos ativos de informação;

III - comunicar-se com a Equipe Técnica de Resposta a Incidentes de Redes Computacionais (ETIR) e com as áreas da CGTI responsáveis pelos ativos, a fim de fornecer e obter informações acerca de vulnerabilidades e ameaças existentes, bem como sobre o processo de tratamento das mesmas;

IV - elaborar análises de risco de segurança dos ativos de informação, de acordo com as normas de gestão de riscos vigentes;

V - reportar-se ao Comitê de Segurança da Informação do INPI sobre a evolução, os riscos e os achados dos testes e varreduras; e

VI - analisar os riscos e trata-los de acordo com a Política de Gestão de riscos do INPI e com o Manual de Gestão de Riscos do INPI.

Art. 4º Compete às unidades da CGTI responsáveis pelos ativos de informação:

I - providenciar as atualizações de que trata o art. 5º, de acordo com as boas práticas e planejamento;

II - corrigir as vulnerabilidades encontradas em observância à priorização definida pelo Gestor de Segurança da Informação; e

III - implementar medidas para mitigar o risco referente às vulnerabilidades que não puderem ser corrigidas tempestivamente.

## CAPÍTULO III
## DOS PROCEDIMENTOS

Art. 5º Devem ser implementadas ações preventivas, de acordo com as melhores práticas de Segurança da Informação, para, no mínimo:

I - atualizar e manter atualizados os sistemas operacionais e aplicativos instalados em estações de trabalho e dispositivos móveis do INPI;

II - atualizar e manter atualizados os sistemas operacionais de servidores, sejam estes físicos ou virtuais;

III - atualizar e manter atualizados os servidores de aplicação (**middleware**);

IV - atualizar e manter atualizados os Sistemas Gerenciadores de Bancos de Dados (SGBDs);

V - atualizar e manter atualizada a infraestrutura de virtualização;

VI - atualizar e manter atualizados os sistemas e aplicações **web**;

VII - atualizar e manter atualizados sistemas de IOT (**Internet of Things**, ou “Internet das Coisas”) e de comunicação;

VIII - testar novos sistemas de informação antes de sua entrada em produção; e

IX - manter atualizada a base de ativos de informação.

Parágrafo único. Todas as atualizações devem ser previamente avaliadas e testadas, preferencialmente em ambiente de homologação e testes, antes de serem implementadas em ambiente de produção, reduzindo assim o risco de incompatibilidades que possam produzir incidentes e perturbações indesejáveis no ambiente de TI do INPI.

Art. 6º Devem ser realizadas varreduras e testes periódicos em todos os ativos de informação inventariados e conectados à rede do INPI, em busca de vulnerabilidades.

Art. 7º As atividades de varreduras e testes devem ser feitas preferencialmente de forma automatizada, utilizando ferramenta apropriada e reconhecida na Divisão de Segurança da Informação (DISEG), do INPI, que possua base de vulnerabilidades e **plug-ins** de verificação continuamente atualizados.

Parágrafo único. A ferramenta deve ter a capacidade de análise e verificação do ambiente para adequação do mesmo de acordo com as melhores práticas de entidades relevantes no cenário de Segurança da Informação.

Art. 8º As varreduras a serem realizadas devem contemplar testes para todas as vulnerabilidades conhecidas de aplicativos da **Web**, sistemas operacionais e redes.

Art. 9º As vulnerabilidades encontradas nas varreduras e testes serão classificadas de acordo com o nível de criticidade, devendo a ferramenta que realiza a varredura contemplar essa classificação por criticidade.

Art. 10. As vulnerabilidades de maior criticidade deverão ser tratadas no menor tempo possível.

Art. 11. No caso de impossibilidade de tratamento de alguma vulnerabilidade classificada como crítica, o Gestor de Segurança da Informação deverá ser imediatamente comunicado pela área técnica responsável pelo tratamento.

Art. 12. A área responsável pelo ativo de informação cuja vulnerabilidade for encontrada, deve atuar para diminuir a exposição ao risco a um nível aceitável, de acordo com o nível de criticidade do ativo.

Art. 13. Os processos de correção de vulnerabilidade de criticidade alta em ativos definidos como prioritários ao negócio, devem ter suas atividades priorizadas em relação às demais atividades rotineiras das unidades técnicas.

Art. 14. Caso um ativo de informação vulnerável tenha sido desenvolvido ou seja mantido por outro órgão público, este deverá ser comunicado.

Art. 15. O teste de penetração (**Pentest**) deve ser realizado conforme critério de necessidade do INPI, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as

informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal do Instituto.

## CAPÍTULO IV
## DISPOSIÇÕES FINAIS

Art. 16. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela CGTI, podendo ser levados em caso de necessidade ao Comitê de Segurança da Informação do INPI.

Art. 17. Esta Instrução Normativa entra em vigor em 01 de abril de 2024 e sua publicação se dará no Boletim de Pessoal, do INPI

**JÚLIO CESAR CASTELO BRANCO REIS MOREIRA**
Presidente


Documento assinado eletronicamente por **JULIO CESAR CASTELO BRANCO REIS MOREIRA**, **Presidente**, em 14/03/2024, às 15:34, 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.inpi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0977785** e o código CRC **8CC0D39D**.