NORMATIVA SOBRE ANÁLISE DE VULNERABILIDADES

SUMÁRIO:

1. OBJETIVO 4
2. APLICABILIDADE 4
3. ACRÔNICOS E ABREVIATURAS 4
4. DO PERÍMETRO 5
   - **4.1. Perímetro interno** 5
   - **4.2. Perímetro Externo** 5
   - **4.3. Perímetro Gerência** 5
5. DOS PROCEDIMENTOS 5
   - **5.1. Perímetro interno** 5
     - **5.1.1. Servidores** 5
     - **5.1.2. Roteadores** 6
   - **5.2. Perímetro Externo** 6
   - **5.3. Perímetro Gerência** 6
6. DOS PROCESSOS PÓS ANÁLISE 6
7. OBSERVAÇÕES 7
8. COMPOSIÇÃO DO COMITÊ DE SEGURANÇA DA FIBRASIL 7
9. APROVAÇÃO 7
10. DOCUMENTOS RELACIONADOS 7
11. VIGÊNCIA 8

RESPONSÁVEL E APROVADORES:

Área Responsável	Governança CTIO
Aprovadores	Infraestrutura e Segurança de TI, NOC, Site Management

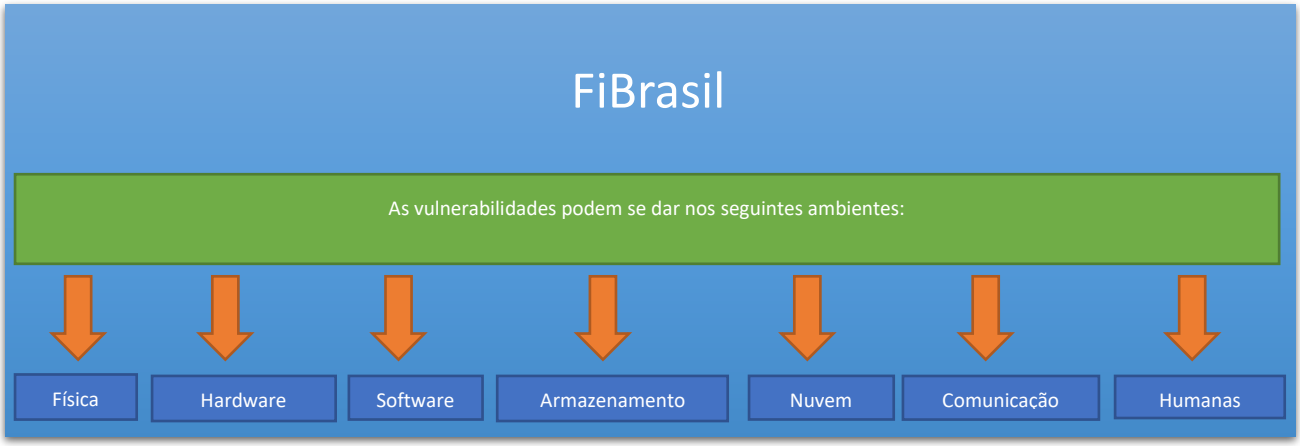
1. OBJETIVO

Entende-se como vulnerabilidade o conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Com a evolução da rede da FiBrasil fez-se necessária a adoção de processos e procedimentos para realização de constantes análises da exposição dos elementos suscetíveis a intervenções não autorizadas.

Essa análise se dará utilizando-se de ferramentas apropriadas para tal fim, deverá ser efetuado de diversos pontos de acesso denominados perímetros, definidos logo mais nesse documento.

A normativa de Análise de Vulnerabilidades estabelece as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para evitar-se que vulnerabilidades estejam presentes nos ativos da organização. Sendo um processo contínuo, proativo, automatizado ou não, que mantém os sistemas de computação, as redes e aplicativos corporativos protegidos contra-ataques cibernéticos e violações de dados.



2. APLICABILIDADE

Aplica-se aos empregados, aos clientes e aos fornecedores da FIBRASIL.

3. ACRÔNICOS E ABREVIATURAS

As siglas e acrônimos aqui utilizados seguem a Portaria Número nº 93, de 26 de setembro de 2019 (Glossário de Segurança da Informação).

4. DO PERÍMETRO

A análise de Vulnerabilidade será feita a cada 2 (dois) meses e são definidos os seguintes pontos de análise:

4.1. PERÍMETRO INTERNO

Define-se como PERÍMETRO INTERNO todo o acesso efetuado dentro da Rede da FiBrasil. Visa simular um ataque através de um agente interno.

4.2. PERÍMETRO EXTERNO

Deve-se entender como PERÍMETRO EXTERNO o acesso efetuado fora da Rede da FiBrasil, ou seja, da INTERNET. Essa análise simula o ataque proveniente de qualquer lugar.

4.3. PERÍMETRO GERÊNCIA

Como a Rede da FiBrasil tem uma Rede própria e isolada para a sua Gerência, é necessário simular um ataque como se um hacker a tivesse invadido.

5. DOS PROCEDIMENTOS

Para cada um dos Perímetros descritos acima, deve ser seguido um procedimento publicado e aprovado.

5.1. PERÍMETRO INTERNO

Utiliza-se a ferramenta de análise de vulnerabilidade a qual está configurada para fazer uma análise dos endereços IPs dos elementos de rede.

5.1.1. SERVIDORES

São monitorados:

- Sistema Operacional
- Aplicações
- Portas
- Serviços

5.1.2. ROTEADORES

São monitorados:

- Portas
- Serviços
- Protocolos

5.2. PERÍMETRO EXTERNO

São utilizados ferramentas e scripts para varredura dos pontos de extremidade onde são gerenciadas ameaças de vulnerabilidades.

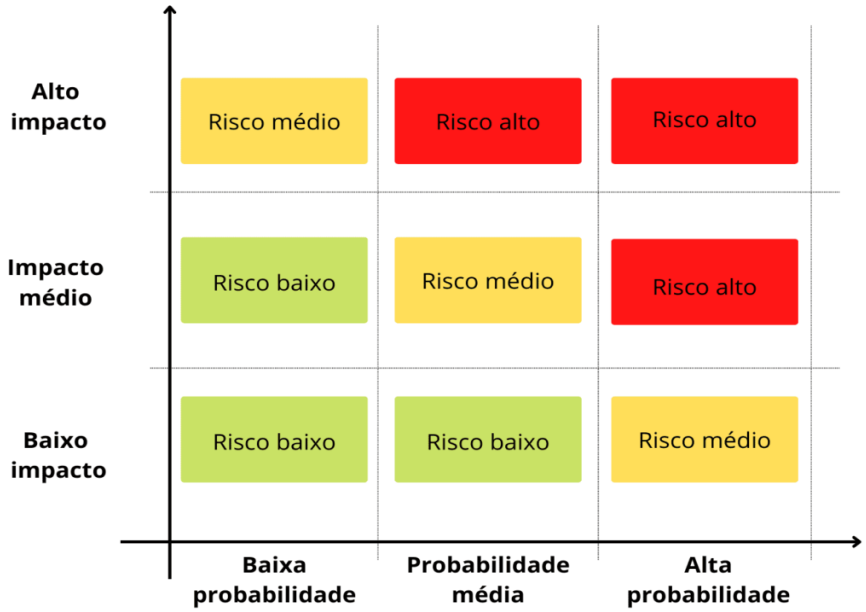
5.3. PERÍMETRO GERÊNCIA

Seguem os mesmos procedimentos do perímetro interno.

6. DOS PROCESSOS PÓS ANÁLISE

Uma vez efetuada a Análise de Vulnerabilidade, seja qual for o perímetro, deverá ser emitido o Relatório de Análise de Vulnerabilidade.

Esse relatório classificará a Vulnerabilidade conforme a figura abaixo, denominada MATRIZ DE RISCO:



Probabilidade

- **Baixo Impacto / Baixa Probabilidade**: os riscos neste quadrante do gráfico são tanto de baixo impacto quanto de baixa probabilidade.
- **Baixo Impacto / Alta Probabilidade**: esse tipo de risco representa uma ameaça moderada às operações.
- **Alto Impacto / Baixa Probabilidade**: Este tipo de evento terá um alto impacto nas operações, mas a probabilidade de sua concretização é improvável.
- **Alto Impacto / Alta Probabilidade**: os riscos nesta categoria são os de maior prioridade porque têm uma alta probabilidade de ocorrer e teriam um efeito gravemente negativo nas operações.

O Comitê de Segurança, ao identificar a vulnerabilidade, deverá comunicar a área custodiante e está deverá fazer uma avaliação e apresentar a resolução, contendo prazos, responsáveis e descrição quando aplicável.

Caso não seja apontada a resolução, o Comitê de Segurança emitirá uma Carta de Risco, conforme matriz acima, a qual deverá ser assinada pelo gestor da área custodiante da vulnerabilidade.

7. OBSERVAÇÕES

Quaisquer comentários, sugestões, críticas, contribuições ou informações relacionadas à presente publicação deverão ser dirigidos ao Comitê de Segurança da FiBrasil.

8. COMPOSIÇÃO DO COMITÊ DE SEGURANÇA DA FIBRASIL

O Comitê de Segurança da Fibrasil será composto por um representante de cada uma das seguintes áreas: Gerência de Operações, Gerência *Site Management* e Gerência de Infraestrutura e Segurança de TI. A indicação deverá ser aprovada em Reunião de Diretoria.

9. APROVAÇÃO

Esse documento foi aprovado pelas áreas de Infraestrutura e Segurança em TI, NOC – Operações e Site Management - Engenharia em 06/02/23 e entra em vigor nessa data.

10. DOCUMENTOS RELACIONADOS

Sem prejuízo das demais normas relacionadas ao tema, destacam-se:

- Normativa de Segurança da Informação FiBrasil
- Normativa de Segurança Cibernética
- Normativa de Respostas a Incidentes
- Diretrizes e Bases Rede IP – FiBrasil
- Diretrizes e Bases Segurança – FiBrasil
- Política de Segurança de Elementos de Rede – FiBrasil
- Framework CIS Controls V8
- Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados
- Resolução nº 740/2020 da ANATEL – Regulamento de Segurança Cibernética

11. VIGÊNCIA

A presente normativa terá validade a partir da data de sua aprovação e permanecerá em vigor até sua expressa revogação.