UERJ · Universidade do Estado do Rio de Janeiro
PR6 Pró-reitoria de Planejamento e Gestão
DIRTEC PR6

GUIA ORIENTATIVO · DEPGSI

Guia de Fortalecimento do Perímetro de Rede



PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

DEPGSI
DEPARTAMENTO DE GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO
DIRTEC | PR-6

Produção institucional: UERJ | PR-6 | DIRTEC | DEPGSI
Base técnica: CISC GOV.BR, Guia de Fortalecimento do Perímetro de Rede, versão 1.1 (2026).

SEÇÃO 01

O que é a avaliação do perímetro de rede?

Para a TI da UERJ, avaliar o perímetro é revisar como redes, zonas, equipamentos e serviços se comunicam, verificando se os acessos permanecem necessários, autorizados e protegidos de acordo com os riscos e as necessidades institucionais.

O QUE AVALIAR

- Comunicações entre redes e serviços
- Regras de firewall e acessos externos
- Rotas, zonas e segmentação da rede
- Permissões amplas ou desatualizadas

POR QUE AVALIAR

- Reduzir caminhos possíveis de ataque
- Identificar acessos sem necessidade
- Priorizar correções conforme o risco
- Preservar a operação dos serviços

01 MAPEAR
Redes, fluxos e responsáveis

→

02 VALIDAR
Necessidade, risco e evidências

→

03 TRATAR
Mudanças e revisão periódica

DIRETRIZ | Revisar acessos com evidências, análise de impacto e registro das mudanças.

SEÇÃO 02

Quem deve se envolver?

Na UERJ, a avaliação do perímetro depende da atuação integrada da alta gestão, da PR-6, da DIRTEC, da gestão de TIC, do DEPGSI e do DEPINFRA, para conciliar prioridades institucionais, riscos de segurança e evidências técnicas.

VISÃO ESTRATÉGICA

ALTA GESTÃO · PR-6 · DIRTEC
GESTÃO DE TIC

Define prioridades e orienta decisões sobre os acessos institucionais.

VISÃO DE RISCO

DEPGSI
GOVERNANÇA E SEGURANÇA

Identifica exposições, analisa impactos e orienta o tratamento dos riscos.

VISÃO TÉCNICA

DEPINFRA
REDES E INFRAESTRUTURA

Verifica regras, rotas e segmentação; valida os fluxos e dependências.

VALIDAÇÃO CONJUNTA | As três visões fundamentam decisões sobre acessos e mudanças com evidências.

DIRETRIZ | Validar a necessidade do acesso, os riscos e o impacto antes de qualquer mudança.

SEÇÃO 03

O que deve ser avaliado?

Na TI da UERJ, avaliar o perímetro exige examinar a exposição externa, a segmentação, as regras de acesso, a publicação de serviços, as rotas e a qualidade das configurações, confrontando cada comunicação com sua finalidade institucional e o risco operacional.

01

EXPOSIÇÃO

Portas e serviços acessíveis a partir da Internet.

02

SEGMENTAÇÃO

Fluxos entre zonas, usuários e ambientes críticos.

03

REGRAS DE ACESSO

Origem, destino, protocolo e portas efetivamente liberadas.

04

NAT E PUBLICAÇÃO

Traduções e destinos internos dos serviços publicados.

05

ROTAS E CAMINHOS

Percursos reais do tráfego e possíveis rotas alternativas.

06

QUALIDADE DA CONFIGURAÇÃO

Regras sem efeito, sobreposta ou referências inválidas.

CRITÉRIO COMUM | Confrontar fluxos reais, necessidade de acesso e evidências técnicas.

DIRETRIZ | Registrar escopo, achados e responsáveis antes de propor ajustes no perímetro.

SEÇÃO 03.1

AVALIAÇÃO DO PERÍMETRO DE REDE



Exposição

Quais serviços e portas podem ser alcançados e a partir de quais origens.



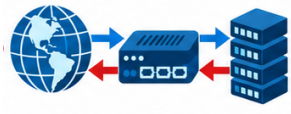
Segmentação

Quais zonas se comunicam e se os fluxos correspondem ao esperado.



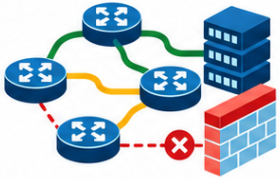
Regras de acesso

Origem, destino, protocolo e porta definidos nas regras que tratam o fluxo.



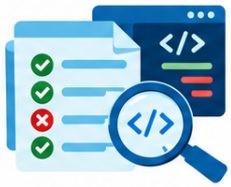
NAT e publicação

Traduções que alteram a origem, o destino ou a forma como o acesso é publicado.



Roteamento e caminhos

Por onde o tráfego pode passar e se existe caminho que evita o controle previsto.



Qualidade da configuração

Referências inválidas, objetos sem uso e regras que não produzem efeito.

SEÇÃO 04

Quais passos devem ser seguidos na avaliação?

A avaliação pode ser conduzida em etapas simples e encadeadas, desde a definição do escopo até a validação dos achados com evidências e contexto.

01

Definir escopo



Firewalls, roteadores, interfaces, redes, enlaces

02

Definir objetivos da avaliação



Portas, serviços, regras, rotas, zonas

03

Elaborar catálogo de verificações



Permissões excessivas, portas críticas expostas, violações de segmentação

04

Coletar e preparar as configurações



Dumps, snapshots, coleta de configurações

05

Executar as verificações



Carregar configurações, consultar regras, gerar relatórios

06

Analisar e classificar os achados



Avaliação dos resultados

07

Validar os achados com evidências e contextos



Confirmação dos achados

SEÇÃO 05

O que verificar na prática?

A avaliação deve partir de perguntas objetivas sobre as configurações coletadas, os acessos permitidos e o comportamento esperado da rede.

TEMA	PERGUNTAS DE VERIFICAÇÃO
Exposição	• Há acesso administrativo exposto à Internet? • A Internet alcança serviços críticos fora da DMZ ou redes internas?
Segmentação	• Usuários alcançam redes de servidores além do necessário? • Homologação ou redes comuns alcançam produção ou administração?
Regras e filtros	• Existem regras amplas do tipo 'any / any / any / permit'? • Há regras sem efeito, sobrepostas ou referências inválidas?
NAT e caminhos	• A publicação aponta para o destino interno esperado? • O caminho passa pelos controles previstos ou existe rota alternativa?
Mudanças	• A mudança abriu comunicação que antes não existia? • Algum caminho ou fluxo esperado mudou ou deixou de funcionar?

Referências públicas do CISC GOV.BR (v1.1) não descrevem ferramentas ou configurações da UERJ. Orientações sobre quaisquer ferramentas a implementar deverão ser verificadas em processo SEI encaminhado ao DEPGSI, com cópia para a DIRTEC. O processo deverá ter nível de acesso 'Restrito', com hipótese legal 'Comprometer Atividades' (art. 23, VIII, da LAI - Lei nº 12.527/2011).

EVOLUÇÃO CONTÍNUA
Catálogo vivo de verificações

É preciso manter um catálogo de verificações adequado ao ambiente, ampliando-o conforme novas necessidades, mudanças ou achados. Sua aplicação deve ocorrer periodicamente e após alterações relevantes, permitindo acompanhar a evolução do perímetro.

SEÇÃO 06

Como verificar?

Depois de definidos os pontos de avaliação, é preciso escolher métodos que produzam evidências e confirmem se a rede funciona conforme os acessos e caminhos esperados.

DEFINIR O ESPERADO

Antes do teste, é preciso definir origem, destino, protocolo, porta e condições do acesso, para comparar o resultado observado com o comportamento esperado.

NO EQUIPAMENTO

É preciso consultar regras e ACLs aplicadas, objetos, zonas, interfaces, NAT e rotas. Contadores e registros podem confirmar o uso real das políticas.

TESTES DE CONEXÃO

É preciso testar a partir de origem autorizada, com o protocolo e a porta do fluxo. As verificações de caminhos e conectividade devem respeitar o escopo definido.

ANÁLISE DE CONFIGURAÇÕES

A análise pode modelar configurações, regras, políticas e caminhos de forma repetível, considerando o alcance e as limitações das ferramentas de referência.

REGISTROS PARA REPETIR

Esperado e evidência

- origem e destino
- protocolo e porta
- ação esperada
- justificativa
- método utilizado
- resultado obtido
- evidência
- data da verificação

REFERÊNCIA TÉCNICA: CISC GOV.BR (v1.1). A UERJ utiliza ferramentas específicas para a avaliação do perímetro de rede. PPSI 2.0: medidas 12.2, 12.4 e 13.4; complementos: CIS Controls v8.1 e NIST SP 800-41 Rev. 1. Orientações para implementar ferramentas devem ser verificadas em processo SEI encaminhado ao DEPGSI, com cópia para a DIRTEC, nível de acesso 'Restrito' e hipótese legal 'Comprometer Atividades' (art. 23, VIII, da LAI - Lei nº 12.527/2011).

SEÇÃO 07

Como utilizar ferramentas de análise?

O CISC GOV.BR (v1.1) descreve métodos para modelar configurações de diferentes fabricantes e analisar fluxos, regras e caminhos. A verificação depende das evidências coletadas e do escopo definido.

01

COLETA

Configurações

É preciso reunir configurações dos dispositivos que aplicam regras, rotas, ACLs e NAT.



02

MODELAGEM

Carregamento

Os arquivos coletados permitem representar caminhos, políticas e elementos da rede.



03

CONSULTAS

Verificação de regras

As consultas examinam origem, destino, protocolo, portas e caminhos definidos.



04

RESULTADOS

Análise de evidências

É preciso comparar os resultados com o catálogo de verificações e a necessidade institucional.



PERGUNTAS DE VERIFICAÇÃO		TEMA DA CONSULTA
01	Existe algum fluxo SSH permitido da rede de servidores para a Internet?	SSH
02	A Internet consegue alcançar a rede administrativa nas portas 22 ou 3389?	22 / 3389
03	A rede de usuários consegue alcançar servidores pela porta SMB?	SMB / 445

REFERÊNCIA TÉCNICA: CISC GOV.BR (v1.1), seção 7. O guia apresenta exemplos de consultas técnicas, cuja aplicação exige conferência da documentação e análise das evidências. Orientações para implementar ferramentas na UERJ devem ser verificadas em processo SEI ao DEPGSI, com cópia para a DIRTEC, nível 'Restrito', hipótese 'Comprometer Atividades' (art. 23, VIII, da LAI - Lei nº 12.527/2011).

SEÇÃO 08

Como interpretar o resultado da avaliação?

É preciso comparar cada resultado com o fluxo esperado e confirmar a evidência disponível antes de classificá-lo como desvio.

01
COMPARAR
Fluxo esperado

É preciso comparar o fluxo observado ao esperado.



02
IDENTIFICAR
Regra, rota ou NAT

É preciso identificar a regra, a rota e o NAT.



03
CONFIRMAR
Confiabilidade

É preciso conferir a coleta e as limitações da análise.



04
CLASSIFICAR
Resultado e ação

É preciso classificar conforme a evidência.



CLASSIFICAÇÃO DOS RESULTADOS

STATUS	CRITÉRIO PARA CLASSIFICAÇÃO
Conforme	O fluxo está de acordo com o comportamento esperado.
Desvio confirmado	Há acesso indevido, bloqueio indevido ou caminho inesperado confirmado.
Validar	Falta evidência ou permanece dúvida sobre o comportamento esperado.
Limitação	A coleta ou a ferramenta não permite concluir com segurança.

REGISTRO DO RESULTADO — É preciso guardar a evidência, a conclusão e a ação definida para as próximas avaliações.

REFERÊNCIA TÉCNICA: CISC GOV.BR (v1.1), seção 8. A UERJ utiliza ferramentas específicas para a avaliação do perímetro de sua rede.

SEÇÃO 09

O que priorizar após a avaliação?



É preciso priorizar os desvios que expõem áreas sensíveis ou rompem a segmentação prevista.

PRIORIDADE ALTA	É preciso priorizar desvios que exponham áreas sensíveis, quebrem a segmentação, permitam acesso administrativo indevido ou contornem controles.
CORREÇÃO PLANEJADA	É preciso planejar a correção quando a mudança depender de testes, janela de manutenção, avaliação de impacto ou ajustes em outros componentes.
VALIDAR ANTES DE ALTERAR	É preciso confirmar o comportamento esperado, as dependências, a necessidade do acesso e a cobertura da avaliação antes de alterar regras.

PERGUNTAS DE TRIAGEM

CRITÉRIO	PERGUNTA OBJETIVA
Origem	O acesso parte da Internet, de parceiro ou de rede com menor confiança?
Destino	O fluxo alcança administração, dados sensíveis, infraestrutura ou serviço crítico?
Amplitude	A regra permite mais origens, destinos, protocolos ou portas do que o necessário?
Persistência	O desvio existe no caminho principal e também em rotas alternativas?
Mudança	A correção é compreendida, testável e reversível?
FECHAMENTO DO ACHADO	É preciso repetir o teste após a correção e verificar que o desvio cessou sem afetar acessos necessários.

REFERÊNCIA TÉCNICA: CISC GOV.BR (v1.1), seção 9. A UERJ utiliza ferramentas específicas para avaliar o perímetro de sua rede.

SEÇÃO 10

Quando repetir a avaliação?

A avaliação do perímetro deve acompanhar as mudanças da rede. É preciso repetir as verificações em ciclos definidos e quando alterações puderem modificar caminhos, regras ou exposições.

IDEIA PRINCIPAL
REAVALIAÇÃO PROPORCIONAL

Mudanças locais podem alterar apenas um fluxo; alterações estruturais podem afetar vários caminhos. A reavaliação deve acompanhar o impacto e confirmar o comportamento esperado.

QUANDO VALE REPETIR

01
CICLOS DEFINIDOS
Periodicidade

A periodicidade das verificações acompanha a criticidade e o ritmo das mudanças, mesmo quando não houver alteração específica.

02
MUDANÇAS NA REDE
Fluxos afetados

É preciso rever os fluxos após mudanças em firewalls, rotas, NAT, VPN, segmentação, novas redes, publicações ou integrações.

03
APÓS CORREÇÃO
Validar resultado

É preciso repetir o teste que apontou o desvio, para comprovar a correção e a disponibilidade dos acessos necessários.

04
NOVAS SITUAÇÕES
Atualizar catálogo

Incidentes, novas exposições e necessidades de acesso devem integrar o catálogo e orientar verificações adicionais.

ATÉ ONDE REVISAR?

MUDANÇA LOCALIZADA
Repetir apenas o necessário
Quando a mudança estiver delimitada, a verificação deve concentrar-se nos fluxos, regras, equipamentos ou redes afetados.

MUDANÇA ESTRUTURAL
Ampliar a avaliação
Arquitetura, segmentação, roteamento ou comunicação entre ambientes alterados exigem avaliação ampliada e eventual revisão do catálogo.

HISTÓRICO DAS AVALIAÇÕES

Registrar data, escopo, alterações e resultados permite comparar avaliações e acompanhar a evolução do perímetro.

REFERÊNCIA TÉCNICA: CISC GOV.BR (v1.1), seção 10. A UERJ utiliza ferramentas específicas para a avaliação do perímetro de sua rede.

REFERÊNCIAS TÉCNICAS

Onde aprofundar?

A avaliação do perímetro pode ser aprofundada por referências públicas sobre configuração segura, arquitetura, segmentação, filtragem e monitoramento de rede.

REFERENCIAL FEDERAL
PPSI 2.0

As medidas do framework apoiam a análise técnica do perímetro, sem descrever controles, ferramentas ou configurações da UERJ.

MEDIDAS DE REFERÊNCIA DO PPSI 2.0

01

CONFIGURAÇÃO SEGURA

MEDIDA 4.2
Configuração segura da infraestrutura e dos dispositivos de rede.

MEDIDAS 12.3 E 12.6
Gestão segura da infraestrutura e protocolos de comunicação.

02

ARQUITETURA E ACESSO

MEDIDAS 12.2 E 12.4
Arquitetura segura, segmentação e diagramas de rede atualizados.

MEDIDAS 12.7 E 12.8
VPN e AAA para acesso remoto; recursos administrativos segregados.

03

FILTRAGEM E VISIBILIDADE

MEDIDA 13.4
Filtragem de tráfego entre segmentos, quando apropriada.

MEDIDA 13.6
Coleta de registros de fluxo para investigar comportamentos suspeitos.

OUTROS MATERIAIS PARA CONSULTA

CIS CONTROLS
Controles 12 e 13: gestão da infraestrutura, monitoramento e defesa de rede.

NIST SP 800-41 REV. 1
Diretrizes para arquitetura, políticas e administração de firewalls.

DOCUMENTAÇÃO TÉCNICA
Fontes públicas para conferir consultas, alcance e limitações dos métodos de avaliação.

BASES PÚBLICAS: CISC GOV.BR (v1.1); Guia do PPSI 2.0 (v1.2); CIS Controls (v8.1); NIST SP 800-41 (Rev. 1).

UERJ — Universidade do Estado do Rio de Janeiro

PR6 Pró-reitoria de Planejamento e Gestão

DIRTEC PR6

GUIA ORIENTATIVO • DEPGSI

Fortalecimento do Perímetro de Rede



VERSÃO 1.0 • NOVEMBRO DE 2026

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

DEPGSI
DEPARTAMENTO DE GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO
DIRTEC | PR-6

Produção institucional: UERJ | PR-6 | DIRTEC | DEPGSI

Base técnica: CISC GOV.BR, Guia de Fortalecimento do Perímetro de Rede, versão 1.1 (2026).