Código: NOR-CENTRAL-009

NP-2

NORMA DE ACESSO REMOTO via VPN

Órgão gestor: SUPTIN
Nº Processo: SEI-100006/001311/2024
Tipo: NOR - Norma
Processo: NORMA DE ACESSO REMOTO via VPN

Órgão aprovador: DIREXE
Data de aprovação: 08/11/2024
Versão: 1.0
Status: Ativo

1. OBJETIVO

Estabelecer diretrizes e procedimentos para o acesso remoto seguro à rede da CENTRAL, utilizando a VPN, a partir de computadores conectados à internet, com vistas a garantir a integridade, a confidencialidade e a disponibilidade dos sistemas e das informações da CENTRAL.

A VPN (Rede Privada Virtual) da Companhia Estadual de Engenharia de Transportes e Logística (CENTRAL) constitui um serviço de acesso remoto ao ambiente corporativo virtual, fornecido, mantido e suportado pela Gerência de Tecnologia da Informação (GERTIN), subordinada à Superintendência de Tecnologia da Informação (SUPTIN), sendo disponibilizado aos usuários conforme as diretrizes desta norma.

A VPN tem como objetivo proporcionar aos usuários a conveniência de acesso à rede corporativa por meio da internet, com a aplicação de requisitos de segurança que protejam os recursos de rede da CENTRAL contra ataques e agentes maliciosos.

Todos os usuários do serviço de VPN devem estar plenamente cientes dos riscos que o uso inadequado do serviço ou de suas credenciais pode representar para a instituição.

2. APLICAÇÃO E ABRANGÊNCIA

Esta norma aplica-se a todos os colaboradores, prestadores de serviço, estagiários, fornecedores, parceiros e quaisquer indivíduos que possuam acesso aos sistemas de informação, redes, serviços ou recursos tecnológicos da CENTRAL por meio da VPN.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

- Lei nº 13.708/18 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Estatuto Social da CENTRAL;
- Regimento Interno da CENTRAL;
- Política de Segurança da Informação da CENTRAL.
- Instrução Normativa PRODERJ/PRE n° 02, de 28 de abril de 2022;
- ABNT NBR ISO/IEC 27001 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação e da Comunicação.

4. DIRETRIZES

4.1. AUTORIZAÇÃO

- O acesso remoto será permitido exclusivamente aos usuários previamente autorizados pela chefia imediata da unidade responsável;
- O acesso remoto sempre deverá atender ao princípio dos acessos mínimos de acordo com a real necessidade e justificativa de acesso; e
- Caso o solicitante não seja o titular da área, a autorização da chefia imediata é obrigatória para a criação ou modificação de contas de acesso.

4.2. CONCESSÃO

- O usuário solicitante deve preencher os seguintes formulários: ***(i)*** o Formulário De Solicitação de Acesso VPN (disponível no Anexo I) e ***(ii)*** o Formulário de Solicitação de Acesso VPN (modelo PRODERJ) (disponível no Anexo II). Ambos devem ser enviados por meio do sistema GLPI, disponível no site da Companhia. **OBSERVAÇÃO: No Anexo II, o usuário deve preencher apenas o item "Usuário do Serviço VPN".**
- A GERTIN encaminha o Formulário de Solicitação de Acesso VPN (Anexo II) para o PRODERJ autorizar o acesso à VPN.
- O PRODERJ enviará aa autorização e a senha de acesso à VPN diretamente ao e-mail do usuário.
- A GERTIN fornecerá ao usuário o manual de acesso à VPN.

4.3. CREDENCIAIS

- As credenciais (login e senha) para autenticação no sistema VPN são distintas das utilizadas para acesso à rede interna da CENTRAL.
- Cada usuário deve utilizar credenciais individuais, que devem ser mantidas em sigilo e não podem ser compartilhadas.
- O acesso à rede da CENTRAL via VPN deve ser exclusivamente para finalidades relacionadas às atividades da Companhia, sendo vedada qualquer utilização que não esteja vinculada ao desempenho das funções do usuário.

4.4. DISPOSITIVOS

- Os dispositivos a serem utilizados devem atender aos critérios mínimos estabelecidos pela GERTIN.
- A instalação e configuração dos aplicativos necessários para a conexão VPN são de responsabilidade do próprio usuário, que poderá solicitar suporte da GERTIN/SUPTIN, se necessário.
- O usuário com acesso VPN deve assegurar que informações confidenciais não sejam expostas a terceiros.
- É proibido o uso de qualquer solução de acesso remoto que não seja oficialmente adotada pela CENTRAL.
- O uso da VPN em redes WiFi públicas, abertas (sem criptografia) ou compartilhadas com terceiros não é recomendado.

4.5. EQUIPAMENTOS PESSOAIS

- Os equipamentos pessoais utilizados para acesso remoto são considerados uma extensão da rede da CENTRAL e, como tal, estão sujeitos às mesmas regras, políticas e regulamentações aplicáveis aos equipamentos de propriedade da Companhia. Portanto, os dispositivos pessoais devem ser configurados de acordo com as normas estabelecidas pela Companhia.

4.6. CONFIDENCIALIDADE

- Os usuários são responsáveis por garantir a confidencialidade das informações acessadas remotamente, não permitindo que terceiros não autorizados tenham acesso ou visualizem tais informações.
- É essencial que os usuários assegurem que seu perfil de acesso remoto não seja utilizado por outras pessoas e evitem o uso da VPN em redes não confiáveis ou em computadores compartilhados, minimizando assim os riscos de roubo de credenciais e outras ameaças digitais.

4.7. PROTEÇÃO CONTRA AMEAÇAS

- O usuário é responsável por assegurar que o dispositivo utilizado para acesso remoto esteja protegido contra vírus, malware e outras ameaças, devendo contar com software antivírus atualizado e firewall ativado.

4.8. MONITORAMENTO E AUDITORIA

- Todas as atividades realizadas por meio de acesso remoto poderão ser monitoradas e registradas para fins de auditoria e segurança.
- A CENTRAL reserva-se o direito de revogar o acesso remoto de qualquer usuário que não cumpra esta norma, que represente risco à segurança ou que atue em interesse próprio.

5. RESPONSABILIDADES

a) **USUÁRIOS**

- Manter o sigilo das informações de acesso ao ambiente de rede da CENTRAL e à conexão remota, sendo totalmente responsáveis por qualquer operação realizada por meio de suas credenciais de acesso.
- Comunicar imediatamente à GERTIN/SUPTIN qualquer incidente de segurança relacionado à sua conta de acesso ou aos serviços informatizados da CENTRAL durante a utilização do serviço de VPN.
- Informar à chefia imediata sobre a desnecessidade de acesso remoto para a execução de suas atividades, visando garantir a revogação das credenciais de acesso remoto.
- Zelar pelo fiel cumprimento desta norma, bem como pelos princípios de segurança da informação.

b) SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO – SUPTIN E GERTIN

- Manter a disponibilidade, integridade e confidencialidade em todo o ambiente de rede da CENTRAL.
- Monitorar o ambiente de rede da CENTRAL para identificar ameaças e acessos maliciosos.
- Manter um registro histórico das solicitações de criação e revogação de usuários para fins de controle.
- Orientar sobre os procedimentos de instalação e configuração das VPNs disponíveis no ambiente da CENTRAL, bem como realizar o credenciamento e descredenciamento de usuários mediante solicitação.
- Descredenciar o usuário após sua desvinculação da CENTRAL, em conformidade com as regras, normas e diretrizes vigentes.
- Planejar, implementar e manter as tecnologias de acesso remoto, garantindo a conformidade com esta norma.

c) SUPERINTENDÊNCIA DE GESTÃO DE PESSOAS – SUPGEP

- Informar à SUPTIN sobre a revogação das credenciais de acesso remoto de funcionários que entrarem em licença sem vencimento, forem desligados definitivamente ou desligados temporariamente por decisão judicial.

d) SUPRINTENDENTES, GERENTES, CHEFES DE ASSESSORIA E EQUIVALENTES

- O desligamento do usuário e/ou a transferência interdepartamental na CENTRAL devem ser informados à SUPTIN.

e) RESPONSÁVEIS PELA GESTÃO E FISCALIZAÇÃO DOS CONTRATOS DE ESTAGIÁRIOS, TERCEIROS/PRESTADORES DE SERVIÇO

- Comunicar imediatamente à SUPTIN sobre o desligamento de estagiários, terceiros e/ou prestadores de serviço da CENTRAL, para que as contas de acesso possam ser revogadas.

f) COMITÊ DE SEGURANÇA DA INFORMAÇÃO – COMISEINF

- Deliberar sobre revisões relativas a esta norma interna e ao processo de controle de acesso.
- Constituir grupos de trabalho para abordar temas e propor soluções específicas sobre controle de acesso.
- Propor diretrizes, competências e responsabilidades para a norma interna e o processo de controle de acesso.

6. REVISÕES E ALTERAÇÕES

Esta norma deverá ser revisada e atualizada periodicamente pela SUPTIN, ou sempre que houver mudanças significativas na infraestrutura ou nas regulamentações aplicáveis.

As alterações devem ser submetidas à aprovação do Comitê de Segurança da Informação e da Diretoria Executiva.

7. DESCRIÇÃO

Procedimento para o usuário solicitar a sua chefia imediata o acesso à VPN.

PASSO	SETOR	AÇÃO A SER TOMADA
01	**Usuário**	O usuário deve encaminhar um chamado por meio do sistema GLPI, solicitando acesso à VPN e anexando os formulários preenchidos que estão nos Anexos I e II. ***É necessária a assinatura da chefia imediata, quando o usuário não for o titular da unidade***.
02	**SUPTIN/GERTIN**	Receber os formulários, preencher os demais campos no Anexo II e encaminhar apenas o Anexo II devidamente preenchido ao PRODERJ.
03	**PRODERJ**	Realizar os trâmites necessários para a criação da conta e enviar diretamente ao e-mail do usuário a autorização e a senha para acesso à VPN.
04	**Usuário**	Informa à SUPTIN/GERTIN o recebimento da autorização e da senha pelo PRODERJ.
05	**SUPTIN/GERTIN**	Fornecer ao usuário o software de acesso à VPN. Encaminhar ao usuário o Manual para Conectar à VPN (Anexo III).
06	**Usuário**	Instalar o software de acesso à VPN no laptop ou desktop pessoal, seguindo as instruções contidas no Manual para Conectar à VPN (Anexo III).

8. ANEXOS

I - FORMULÁRIO DE SOLICITAÇÃO DE ACESSO VPN

II - FORMULÁRIO DE SOLICITAÇÃO DE ACESSO VPN (MODELO PRODERJ)

III - MANUAL PARA CONECTAR À VPN

SUMÁRIO DE REVISÕES		
0	08/11/2024	Emissão Original Procedimento proposto pela SUPTIN, com participação do Comitê de Segurança da Informação - Processo SEI-100006/0001311/2024. Aprovação DIREXE em 08/11/2024 Ata Nº 349/2024.
REVISÕES	**DATA**	**DESCRIÇÃO E/OU ITENS ATINGIDOS**
-	-	-

Documento assinado eletronicamente

DIRETORIA EXECUTIVA

COMPANHIA ESTADUAL DE ENGENHARIA DE TRANSPORTES E LOGÍSTICA - CENTRAL

Distribuição: Geral

Chancela Técnica: Assessoria de Governança, Risco e Compliance - ASSGER

Rio de Janeiro, 13 novembro de 2024

Documento assinado eletronicamente por **Fabricio Abilio Duarte de Moura**, **Diretor-Presidente**, em 14/11/2024, às 13:12, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **87483557** e o código CRC **A2C5A359**.

Av. Nossa Senhora de Copacabana , 493, 5º andar - Bairro Copacabana, Rio de Janeiro/RJ, CEP 22.031-000
Telefone:

ANEXO I - FORMULÁRIO DE SOLICITAÇÃO DE ACESSO VPN

1. FINALIDADE

CRIAÇÃO DE CONTA ☐	**ALTERAÇÃO DE CONTA** **RENOVAÇÃO** ☐ **RESET DE SENHA** ☐

2. DADOS DO COLABORADOR DA VPN

NOME COMPLETO	
CPF	**MATRÍCULA**
CARGO/FUNÇÃO	**TELEFONE INSTITUCIONAL**
E-MAIL INSTITUCIONAL	

3. JUSTIFICATIVA

DECLARO, para os devidos fins, estar ciente dos procedimentos e políticas vigentes da CENTRAL, incluindo a **NORMA DE ACESSO REMOTO VIA VPN**, referentes ao uso de recursos computacionais e acesso à informação. Comprometo-me a cumpri-las rigorosamente, assumindo total responsabilidade pelos meus atos no uso da VPN e por quaisquer prejuízos decorrentes do seu uso indevido.

Rio de Janeiro, _____ de _____ de _____.

_____ _____

ASSINATURA DO COLABORADOR ***ASSINATURA DA CHEFIA IMEDIATA***

Anexo II - Formulário de Solicitação de Acesso VPN (modelo PRODERJ)

PRODERJ

DIT – Diretoria de Infraestrutura tecnológica

Formulário de Solicitação de Acesso VPN

FINALIDADE

CRIAÇÃO DE CONTA	☐	
ALTERAÇÃO DE CONTA	☐	NOME DA CONTA:
- RENOVAÇÃO	☐	
- RESET DE SENHA	☐	

ÓRGÃO/SECRETARIA

Companhia Estadual de Engenharia de Transportes e Logística - CENTRAL

SOLICITANTE (CONTATO ADMINISTRATIVO)

NOME COMPLETO	
CARGO/FUNÇÃO	TELEFONE
E-MAIL INSTITUCIONAL	

USUARIO DO SERVIÇO VPN (CONTATO TÉCNICO)

NOME COMPLETO	
CPF	MATRÍCULA (Para funcionários)/IDENTIDADE
CARGO/FUNÇÃO	TELEFONE
E-MAIL INSTITUCIONAL	

INFORMAÇÕES TÉCNICAS

SERVIÇO VPN
SERVIDOR/REDE 10.9.5.0./23 e 10.11.92.131
JUSTIFICATIVA PARA O ACESSO

INSTRUÇÕES DE PREENCHIMENTO

- O SOLICITANTE (CONTATO ADMINISTRATIVO), É O RESPONSÁVEL ADMINISTRATIVO DO USUÁRIO DE VPN;
- O USUÁRIO DO SERVIÇO VPN (CONTATO TÉCNICO) , É QUEM FARÁ USO EFETIVO DA CONTA A SER CRIADA;
- EM INFORMAÇÕES TÉCNICAS, NO CAMPO SERVIÇO, INDICAR QUE TIPO DE SERVIÇO SERÁ ACESSADO NA REDE (FTP, HTTP, SSH, ETC);
- EM INFORMAÇÕES TÉCNICAS, NO CAMPO SERVIDOR / REDE INDICAR QUE SERVIDOR, SERVIDORES OU REDE SERÃO ACESSADOS.

PARA USO DO PRODERJ

TEMPORÁRIO? ( ) SIM ( ) NÃO

PERÍODO DE USO DA CONTA: ____/____/_____ A ____/____/_____

OBSERVAÇÕES

Rio de Janeiro, ____ de _____ de _____

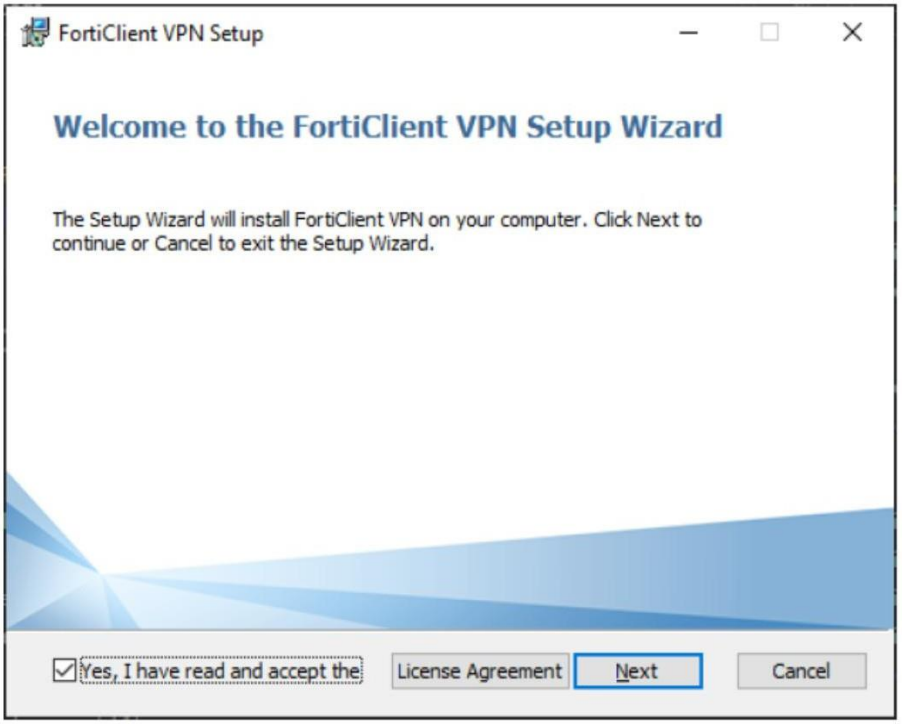
_____

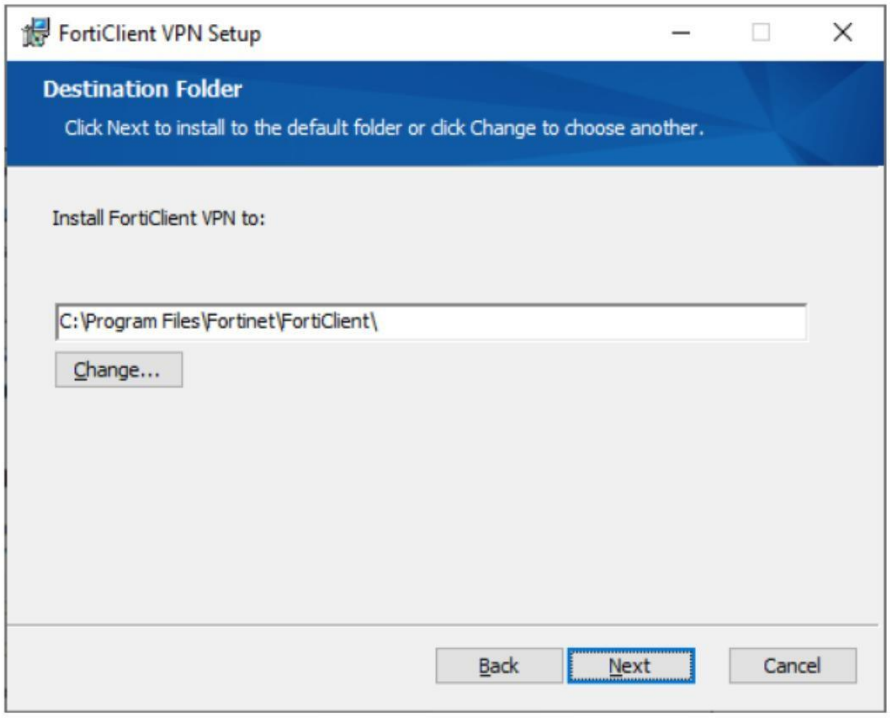
Assinatura do Solicitante

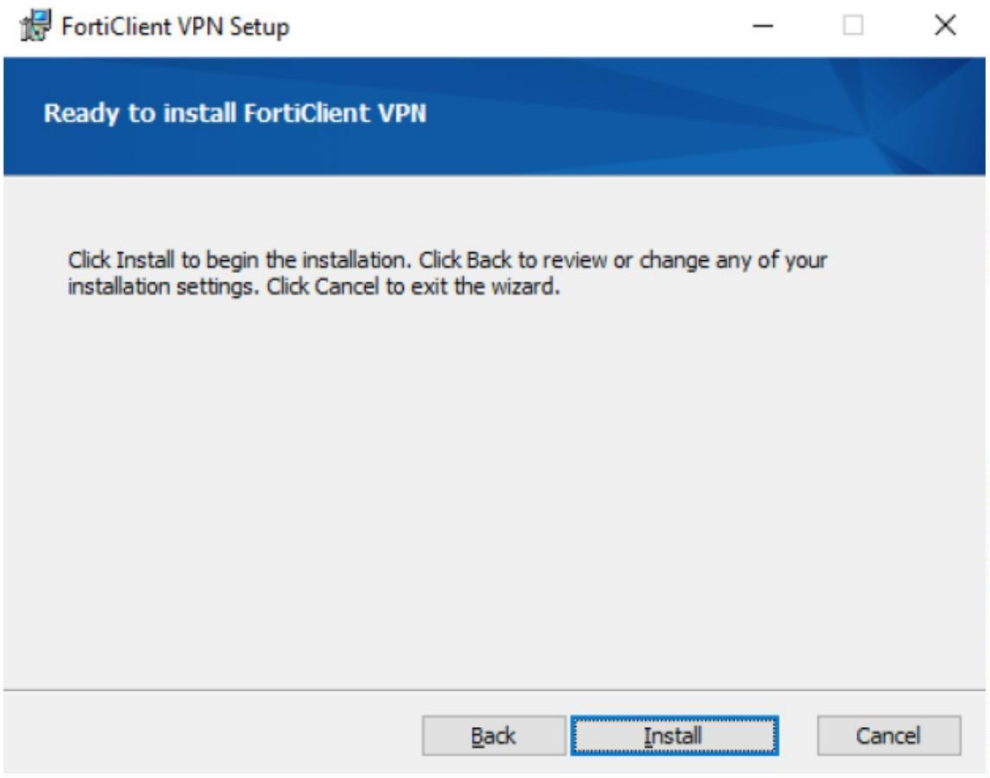
Anexo III - Manual para Conectar à VPN

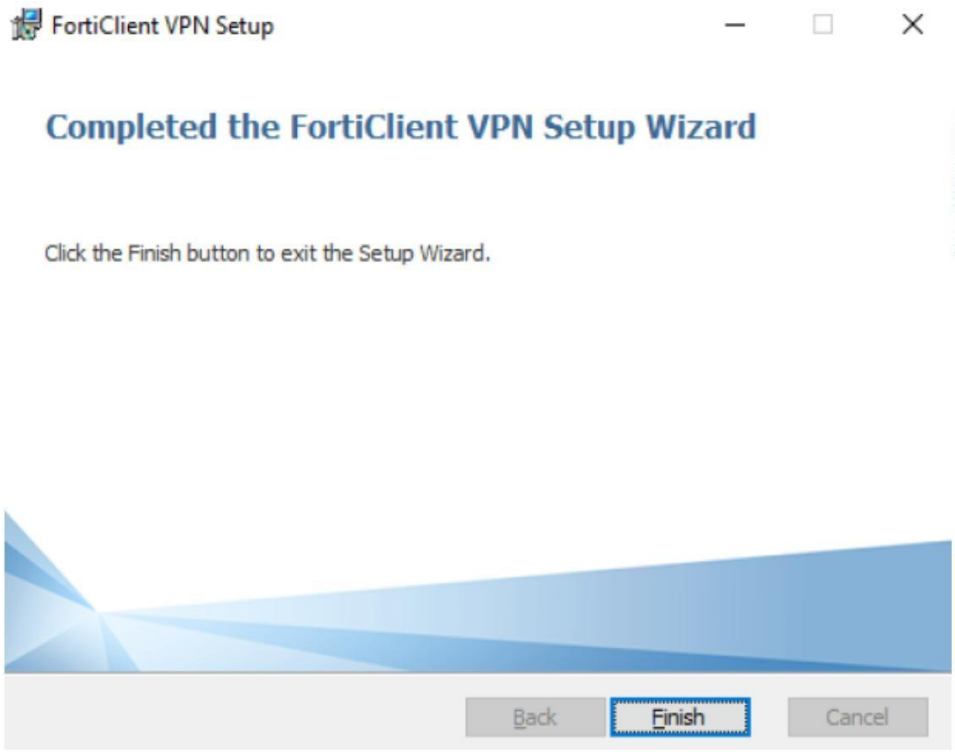
MANUAL PARA CONECTAR À VPN

No arquivo de instalação, clicar duas vezes para começar a instalação:





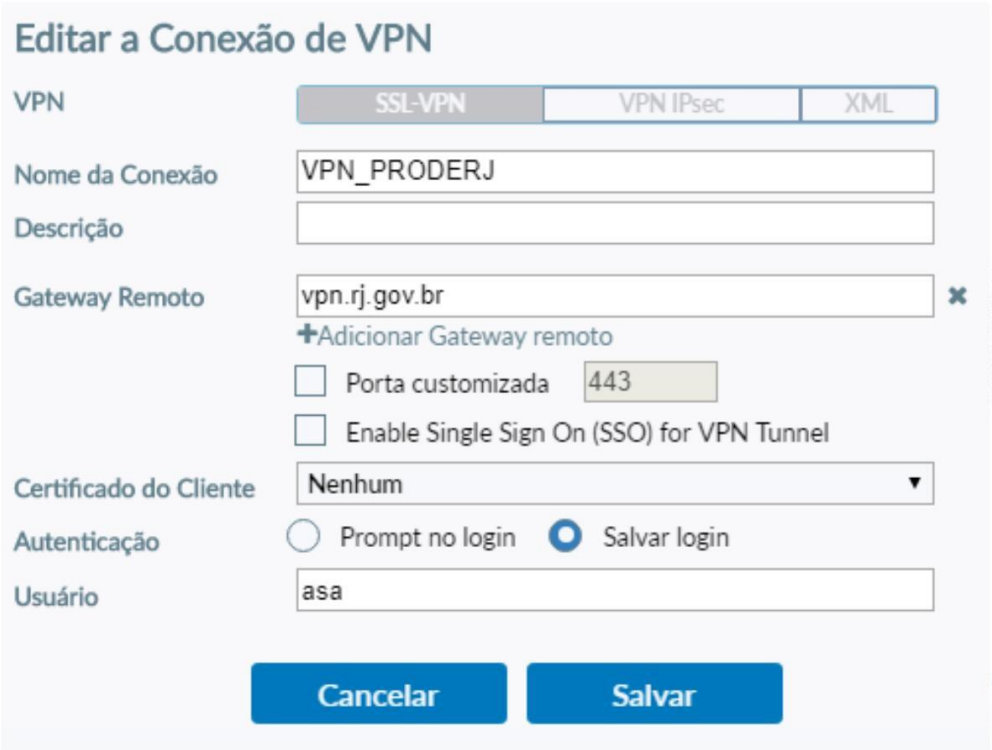

FortiClient VPN Setup
Ready to install FortiClient VPN
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel


FortiClient VPN Setup
Completed the FortiClient VPN Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

Configurar a VPN

Clicar em "Configurar a VPN"

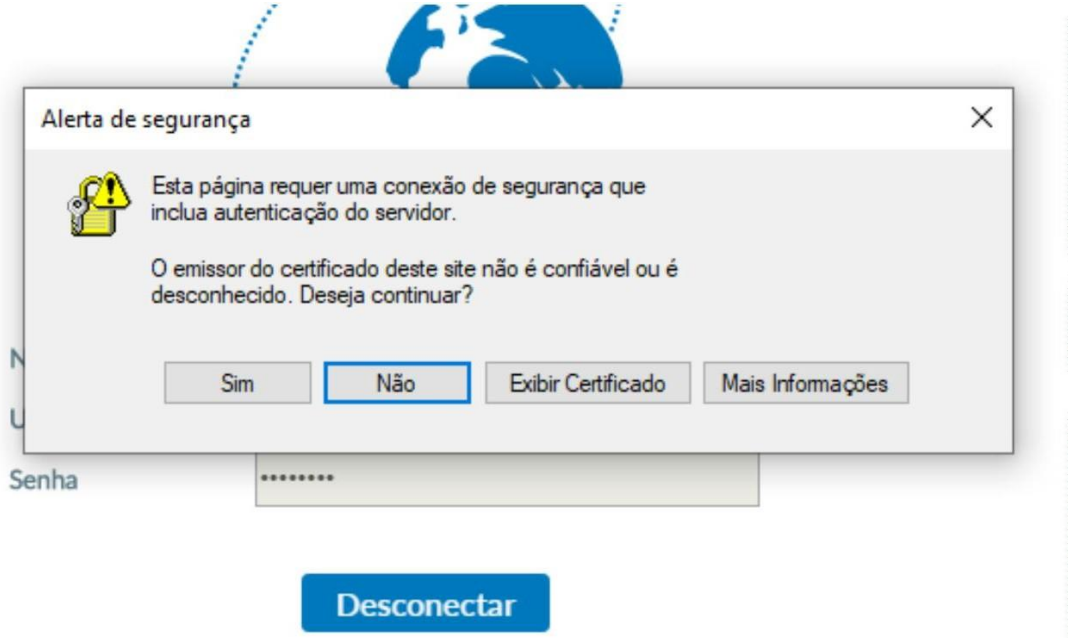
Insira as informações para configuração da VPN **"Nome da Conexão: VPN_PRODERJ"**, **"Gateway Remoto: vpn.rj.gov.br"**, **"Usuário: seu_usuário_de_VPN"**, em seguida clique em **"Salvar".**



Clicar duas vezes no ícone do FortiClient VPN para abrir

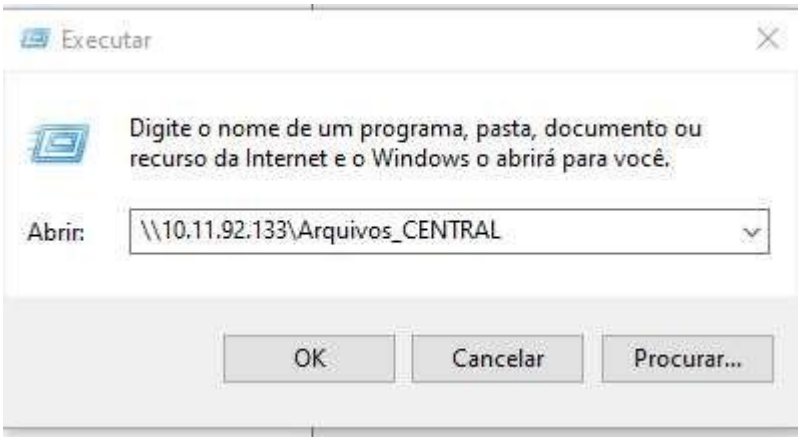
Usuário devera inserir seu usuário e senha de acesso VPN que foi disponibilizado via e-mail pelo PRODERJ depois de ter preencher o formulário para criação de acesso a VPN.

Observar na barra de tarefas do Windows que vai aparecer outra janela aguardando usuário clicar em SIM

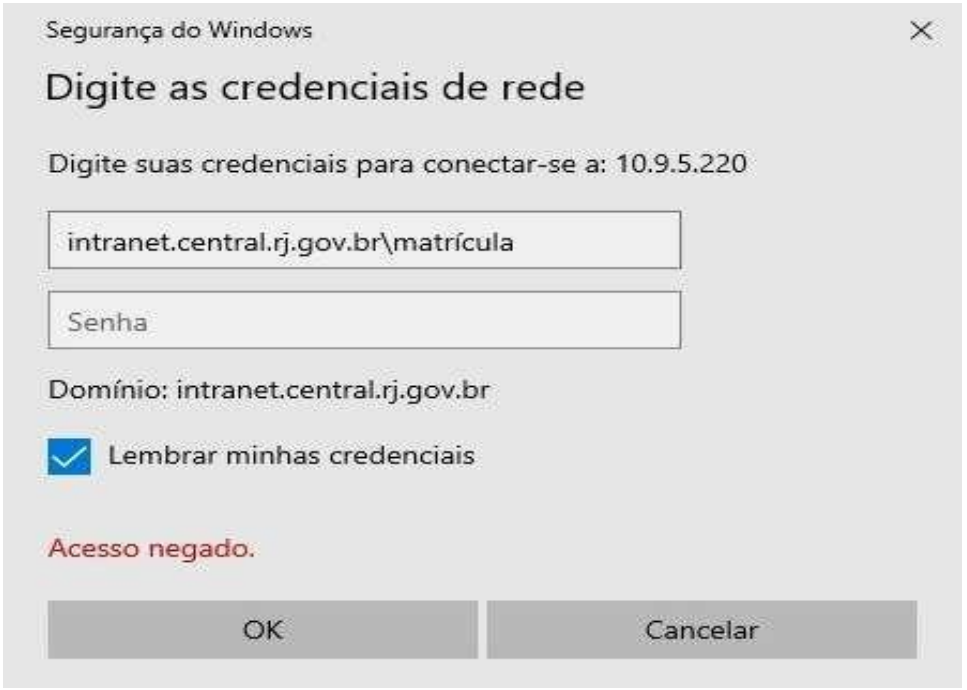


Quando aparecer essa tela CONECTADA é só clicar em minimizar.

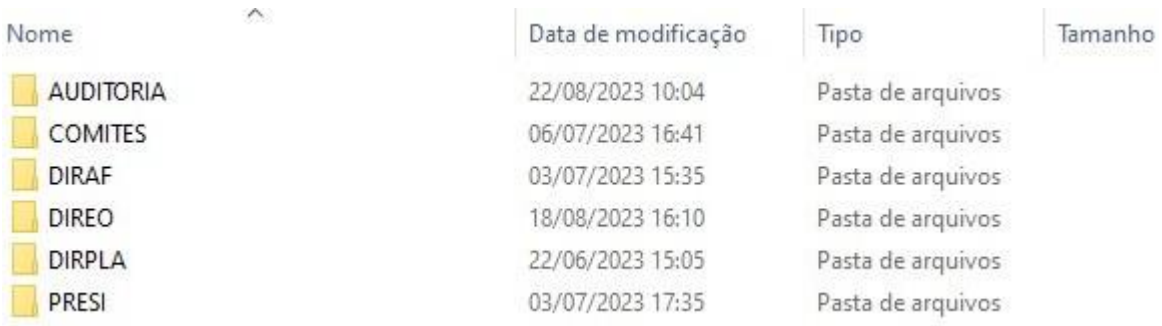
Clicar nas teclas:  **ou vá no menu executar, e digite o seguinte caminho:**



Obs: Quando aparecer a janela solicitando suas credenciais (usuário e senha), não esquecer de digitar na frente do seu usuário **intranet.central.rj.gov.br** como na tela seguinte. Não esquecer também de marcar a opção LEMBRAR MINHAS CREDENCIAIS



Agora basta localizar sua pasta, seguindo a hierarquia conforme organograma da CENTRAL.



Acesso à rede pela VPN concluído com sucesso.