

	Instrução de Trabalho - IT	Coordenação 	Execução 
---	-------------------------------------	--	---

Processo Solicitar acesso remoto no ambiente corporativo			
Versão 01/2026	Data de Emissão 11/02/2026	Macroprocesso (Governo de SC) Infraestrutura e Urbanismo	Macroprocesso (SIE) Gestão de Tecnologia da Informação

1. INFORMAÇÕES DO PROCESSO

1.1 Objetivo do Processo

Permitir o acesso à ferramenta Tactical RMM que é uma ferramenta destinada exclusivamente ao suporte técnico e gerenciamento remoto de estações de trabalho pela equipe de Infraestrutura. Dessa forma, a equipe de TI poderá realizar o suporte, gestão técnica e controle da máquina à distância.

1.2 Informações Complementares

O uso do AnyDesk, TeamViewer e outras ferramentas de acesso remoto foram bloqueadas em dezembro de 2025.

1.3 Características do Processo

1.3.1 Tipo de Processo:

☐ Processo Gerencial
 ☐ Processo Finalístico
 ☒ Processo Suporte

1.3.2 Tipo de Tramitação:

☐ Setorial
 ☒ Intersectorial
 ☐ Intragovernamental
 ☐ Interinstitucional

1.4 Responsável

<i>Cargo</i>	<i>Setor</i>	<i>Telefone</i>	<i>E-mail</i>
Gerente	GEINO - Gerência de Inovação	(48) 366-49304	geino@sie.sc.gov.br

1.5 Interessados (Destinatário - Cliente)

- SIE - Secretaria de Estado da Infraestrutura e Mobilidade;

1.6 Atores Envolvidos

- Gestor do usuário solicitante;
- Usuário/solicitante;
- GEINO - Gerência de Inovação / Setor de Infraestrutura.

1.7 Recursos tecnológicos (sistemas e integrações)

1. SGPE - Sistema de Gestão de Processos Eletrônicos;
2. E-mail institucional;
3. VPN - Virtual Private Network;
4. Tactical RMM - Remote Monitoring and Management.

1.8 Parâmetros SGPe

<i>Assunto</i>		<i>Classe</i>		<i>Controle de acesso (sigilo)</i>

1.9 Legislação, normativas e outras referências

- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018;
- Políticas de Segurança da Informação;
- Normas internas de acesso remoto.

1.10 Indicadores de performance

Indicador	Métrica	Periodicidade de Análise

1.11 Definições

- GEINO - Gerência de Inovação;
- GLPI - Sistema para Abertura de Chamados;
- Tactical RMM - ferramenta gratuita, de código aberto e auto-hospedada (self-hosted) para Monitoramento e Gerenciamento Remoto (RMM) de máquinas Windows, focada em Provedores de Serviços Gerenciados (MSPs) e administradores de TI, oferecendo acesso remoto, automação de tarefas (scripts, patches), inventário de hardware/software e alertas em uma única plataforma web.
- VPN - Virtual Private Network: permite que o servidor trabalhe como se estivesse fisicamente dentro da rede do órgão, acessando: sistemas internos, pastas de rede, intranet, sistemas corporativos restritos.

2. DIAGRAMA DO PROCESSO

O Diagrama do processo pode ser visualizado no link: [clique aqui](#)

3. RELAÇÃO DAS ATIVIDADES

Necessidade de acesso remoto no ambiente corporativo da SIE

SIE/Usuário

1. Abrir chamado (GLPI)

Solicitar o seu acesso remoto à ferramenta Tactical RMM, via chamado no GLPI, informando nome completo do usuário, setor/gerência de atuação, justificativa do acesso, patrimônio e período de acesso.

*O processo avança para a **atividade 3 - Receber chamado (GLPI)***

Necessidade de acesso remoto no ambiente corporativo da SIE

SIE/Gestor do usuário solicitante

2. Abrir chamado (GLPI)

Solicitar acesso remoto à ferramenta Tactical RMM, via chamado no GLPI, informando nome completo do usuário, setor/gerência que o usuário atua, justificativa do acesso remoto, patrimônio e período de acesso.

SIE/GEINO/Setor de Infraestrutura

3. Receber chamado (GLPI)

O responsável pela liberação do acesso remoto receberá o chamado, com a solicitação.

4. Analisar solicitação (GLPI)

A solicitação recebida, via chamado no GLPI, será analisada a fim de verificar se foi o próprio usuário que solicitou o acesso ou se foi realizada pelo gestor.

*O processo pode seguir um dos dois caminhos: **atividade 6 - Verificar acesso à VPN do usuário (GLPI)** ou para a **atividade 5 - Solicitar autorização do gestor (GLPI)***

Se, solicitação do colaborador/usuário solicitante

5. Solicitar autorização do gestor (GLPI)

Nos casos em que o chamado foi aberto pelo usuário/colaborador, deve ser solicitada a autorização do seu gestor para o acesso remoto do usuário. Desta forma, o gestor será adicionado ao chamado no GLPI.

*O processo avança para a **atividade 16 - Receber solicitação de autorização (GLPI)***

Se, solicitação do gestor

6. Verificar acesso à VPN do usuário (GLPI)

O setor de infraestrutura irá verificar se o usuário possui acesso à VPN para poder prosseguir com os cadastros na ferramenta Tactical RMM. Por meio da VPN o usuário poderá acessar à rede interna do órgão, ou seja, os sistemas internos, as pastas de rede e a intranet.

*O processo pode seguir para a **atividade 8 - Realizar análise técnica** ou para a **atividade 7 - Informar solicitante sobre necessidade de acesso à VPN (GLPI)***

Se, usuário sem acesso à VPN

7. Informar solicitante sobre necessidade de acesso à VPN (GLPI)

Ao ser constatado que o usuário não tem acesso à VPN, a equipe de TI deve informar ao solicitante a necessidade de providenciar o acesso. Portanto, deve ser informado ao usuário que ele deverá abrir novo chamado para solicitar o acesso à VPN.

*O processo pode seguir para a **atividade 13 - Abrir novo chamado (GLPI)***

Se, usuário com acesso à VPN

8. Realizar análise técnica

Será realizada a verificação sobre os próximos passos que serão realizados para liberar o acesso à ferramenta Tactical RMM.

O processo pode seguir um dos dois caminhos: **atividade 9 - Realizar novos cadastros (Tactical RMM)** ou para a **atividade 12 - Atualizar informações (Tactical RMM)**

Se, sem cadastro no Tactical RMM

9. Realizar novos cadastros (Tactical RMM)

Para liberar o acesso à ferramenta será necessário realizar cadastros na Tactical RMM:

- Máquina;
- Usuário;
- Vincular o Grupo de acesso.

Além disso, são definidos o nível de permissão e a validade de acesso.



Cadastro concluído.

10. Confirmar liberação de acesso (GLPI)

Após o cadastramento do usuário na ferramenta, o usuário deve ser informado por meio do chamado aberto no GLPI. Desta forma, devem ser informados os dados de acesso remoto do usuário na ferramenta padrão Tactical RMM.

A ferramenta adotada pela SIE é um dispositivo de acesso remoto e gerenciamento de máquinas.



Acesso liberado.

11. Encerrar chamado(s) (GLPI)

Após realizar todas as etapas da liberação do acesso remoto ao usuário, o chamado poderá ser encerrado, concluindo o atendimento.

Por meio da ferramenta, a equipe de TI poderá: acessar remotamente o computador do usuário, realizar o suporte técnico, instalar programas, corrigir problemas e monitorar equipamentos.



Resultado do processo: Acesso concedido e chamado encerrado.

Se, com cadastro no Tactical RMM

12. Atualizar informações (Tactical RMM)

Caso o usuário já tenha realizado acesso remoto anteriormente por meio da ferramenta Tactical RMM, o responsável pela liberação do novo acesso ao usuário poderá realizar a atualização do cadastro para a obtenção de um novo usuário.

*O processo segue para a **atividade 10 - Confirmar liberação de acesso (GLPI)***

SIE/Usuário

13. Abrir novo chamado (GLPI)

Para ser realizada a liberação do uso da ferramenta Tactical, é necessário que o computador do usuário tenha acesso à VPN.

SIE/GEINO/Setor de Infraestrutura

14. Receber novo chamado (GLPI)

A equipe da Infraestrutura deve receber o chamado da solicitação de acesso a VPN a fim de providenciar o acesso do computador à rede interna do órgão.

15. Criar usuário (VPN)

O usuário será cadastrado na VPN a fim de liberar o acesso à rede interna da instituição.

*O processo segue para a **atividade 9 - Realizar novos cadastros (Tactical RMM)***

SIE/Gestor do usuário solicitante

16. Receber solicitação de autorização (GLPI)

O gestor receberá a solicitação para autorizar o acesso remoto do usuário, via chamado no GLPI.

*O processo pode seguir um dos dois caminhos **atividade 18 - Autorizar acesso remoto (GLPI)** ou a **atividade 17 - Negar autorização da solicitação (GLPI)***

Se, solicitação não autorizada

17. Negar autorização da solicitação (GLPI)

No caso do gestor não autorizar o acesso remoto solicitado pelo usuário, o chamado deverá ser encerrado.



Usuário comunicado.



Resultado do processo: Acesso remoto concedido e chamado encerrado.

Se, solicitação autorizada

18. Autorizar acesso remoto (GLPI)

O acesso remoto do subordinado será liberado após solicitação formal via chamado e validação da chefia imediata.

*O processo retorna para a **atividade 6 - Verificar acesso à VPN do usuário (GLPI)***

4. PRIVACIDADE DE DADOS

4.1 Existem Dados Pessoais no Processo?

☒ Sim ☐ Não

4.2 Existem exceções de aplicação da LGPD para o processo?

Processo relacionado com:	Seleção
a) Segurança Pública	☐
b) Defesa Nacional	☐
c) Segurança do Estado	☐
d) Atividades de Investigação e Repressão de Infrações Penais	☐

Fonte: LGPD

4.3 Dados Pessoais são sensíveis?

☐ Sim ☒ Não

4.4 Os dados Sensíveis estão relacionados:

Tipo de Relação	Seleção
Origem racial ou étnica.	☐
Convicção religiosa.	☐
Opinião política.	☐
Filiação a sindicato ou a organização de caráter religioso.	☐
Filosófico ou político	☐
Saúde ou à vida sexual	☐
Genéticos ou biométricos	☐

Fonte: LGPD

4.5 Qual base legal está relacionada com a utilização dos dados?

Base Legal LGPD	Seleção
Consentimento	☐
Cumprimento de obrigação legal ou regulatória	☐
Execução de políticas públicas	☐
Realização de estudos por órgão de pesquisa	☐
Execução ou criação de contrato	☐
Exercício regular de direitos	☐
Proteção da vida	☐
Tutela da saúde	☐
Legítimo interesse	☐
Proteção do crédito	☐

Fonte: LGPD

4.6 Quais são os Dados Pessoais:

Dados Pessoais	Dados Sensíveis
Nome completo	

Fonte: Elaborado pelo Especialista.

4.7 Dados são anonimizados no processo?

☐ Sim ☒ Não

5. RELAÇÃO DE DOCUMENTOS

5.1 Os documentos do processo são produzidos no Setor ou recebidos/custodiados no setor?

☐ Produzido no Setor ☐ Existe documento enviado (fonte externa)

5.2 Relação dos documentos produzidos (anexados) para processo:

Tipo documental no SGPe	Código Plano de Classificação	Nome do Documento	Descrição do Documento

Fonte: Elaborado pelo Especialista.

5.3 Os documentos são inseridos em ordem no processo (seguindo padronização)?

☐ Sim ☐ Não

6. ANÁLISE DA CLASSIFICAÇÃO E DA TEMPORALIDADE DOS DOCUMENTOS

6.1 Existe plano de classificação e tabela de temporalidade para os documentos no órgão?

☐ Sim ☐ Não

6.2 Todos os documentos no processo estão no plano de classificação e na tabela de temporalidade?

☐ Sim ☐ Não

6.3 Relação de documento e a temporalidade corrente, intermediário, destinação:

Tipo documental no SGPe	Código Plano de Classificação	Nome do Documento	Temporalidade		
			Corrente	Intermediário	Destinação (eliminação ou guarda permanente)

Fonte: Elaborado pelo Especialista.

7. HISTÓRICO DE REVISÕES

Versão nº	Responsável pela elaboração da IT	Data	Síntese da Revisão
01/2026	Analista de processo: Thaís Castilho de Andrade Revisão: Alex do N. P. da Silva e Cleto Moisés Cardoso	11/02/2026	Mapeamento do processo Solicitar acesso remoto no ambiente corporativo V01



Assinaturas do documento



Código para verificação: **F6H22S5N**

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:



CARLA SILVANIRA BOHN (CPF: 892.XXX.709-XX) em 12/02/2026 às 09:42:10

Emitido por: "SGP-e", emitido em 27/02/2019 - 14:13:23 e válido até 27/02/2119 - 14:13:23.

(Assinatura do sistema)

Para verificar a autenticidade desta cópia, acesse o link <https://portal.sgpe.sea.sc.gov.br/portal-externo/conferencia-documento/U0IFXzY5NjVfMDAwMDU5NTFfNTk1MV8yMDI2X0Y2SDIyUzVO> ou o site

<https://portal.sgpe.sea.sc.gov.br/portal-externo> e informe o processo **SIE 00005951/2026** e o código **F6H22S5N** ou aponte a câmera para o QR Code presente nesta página para realizar a conferência.