FAQ - PGD – CGTI/DAF

Versão 4

21.05.2021 – Atualizada pela Coordenação-Geral de Tecnologia da Informação – CGTI/DAF

Regras Gerais

1. Quem é responsável por implantar e manter o sistema informatizado do programa de gestão?

A Coordenação de Sistemas – COSIS/CGTI/DAF é responsável por implantar e manter o sistema selecionado pela DIREX para disponibilização aos usuários. Atualmente a manutenção do sistema resta prejudicada, visto que não há equipe disponível para a devida atividade.

No que tange a sustentação da Infraestrutura do ambiente disponível, a Coordenação de Infraestrutura de Tecnologia da Informação e Comunicações – COINF/CGTI/DAF é responsável por executar essas ações.

2. Como se dará o acesso remoto a um recurso disponível apenas na rede interna, caso seja necessário?

O acesso remoto, Virtual Private Network – VPN, será concedido conforme solicitação do usuário e aprovação da chefia imediata, estritamente ao sistema/recurso necessário a execução de suas funções, mediante justificativa fundamentada.

A concessão do acesso VPN ao recuso solicitado depende de análise da viabilidade técnica e legal, considerando inclusive o licenciamento contratado para o respectivo recurso almejado.

Nem todos os servidores que aderirem ao PGD irão necessitar de acesso às ferramentas restritas à rede interna do DNIT.

3. Quais sistemas já estão disponíveis para acesso e publicado na INTERNET (WEB)?

Os principais softwares/sistemas que estão publicados na internet:

- SIAET - Sistema Informatizado de Autorização Especial de Trânsito;
- SGO - Sistema de Gerenciamento de Obras de Arte especiais;
- SIPROD - Sistema de Projetos e Obras Delegadas;
- NPO - Sistema Nova Programação Orçamentária;
- SUPRA - Sistema Supervisão Rodoviária Avançada;
- SIOR – Sistema Integrado de Operações;
- SISDNIT - Sistema Integrado de Informações;
- SIAC - Sistema de Acompanhamento Físico e Financeiro de Contratos e Medições.
- SGF- Sistema de Gestão Financeira;
- SEI- Sistema Eletrônico de Informações;
- E-mail - Correio Eletrônico;

- Qualitor - Sistema de Atendimento de Chamados;
- Dnit Cloud - Sistema de Armazenamento e Compartilhamento em nuvem;
- 90COMPOR - Orçamento e Planejamento de Obras (*ComporWeb*);
- TEAMS – Microsoft *Teams* e demais sistemas integrados (office365 online);

Para obter informações quanto a disponibilidade de acesso via internet em outros sistemas, favor entrar em contato com a CGTI por meio do e-mail cgti@dnit.gov.br.

4. Qual a Ferramenta oficial e essencial para o teletrabalho?

O TEAMS é a ferramenta utilizada para uso corporativo e apoio colaborativo do modelo de trabalho Home Office, garantindo que a produtividade dos seus servidores e colaboradores e os resultados da Autarquia não sejam prejudicados e realizados de forma segura por meio de reuniões, ligações, chats, envio de arquivos e armazenamento em nuvem (OneDrive).

Vale ressaltar que a plataforma TEAMS do DNIT somente é disponibilizada para os usuários que possuam e-mail com domínio @dnit.gov.br.

A forma de participação em reunião por videoconferência para outros usuários, inclusive externos será mediante CONVITE,

5.Como faço para solicitar a VPN?

Para concessão de acesso VPN, o usuário deverá gerar um processo SEI, Tipo "Gestão da Informação: Credenciamento de Segurança", com a especificação: "Solicitação de Acesso Via VPN", a nível restrito (Hipótese Legal: Controle Interno (Art. 26, §3º, Lei 10.180/2001), e:

a) Inserir e preencher, no processo, o formulário de "Solicitação de Acesso VPN"; e

b) Inserir e preencher, no processo, o Termo Confidencialidade e Segurança da Informação.

Obs.: Recomenda-se a leitura de todos as disposições dos citados documentos até o final, para ciência, atentando-se a todos os campos a serem marcados ("Estou ciente", "Declaro que").

c) Após devidamente preenchidos, com todos os sistemas e/ou diretórios e/ou bases a serem acessados, contendo justificativas sólidas e detalhadas quanto à necessidade do acesso, os documentos devem ser assinados pelo solicitante e seu chefe imediato.

d) Após isso, o solicitante deve encaminhar o processo à Divisão de Segurança da Informação - DSINF/CGTI/DAF.

6. Os servidores atuando em programa de gestão (PGD) poderão valer-se do serviço de suporte ao usuário?

Não será provido nenhum tipo de suporte técnico na máquina pessoal do usuário, ainda que de forma remota. Também não haverá atendimento de suporte técnico na residência do usuário, mesmo dentro do horário de expediente. Portanto, a manutenção do computador de trabalho pessoal é de responsabilidade do usuário, conforme Art. 23 da Instrução Normativa Nº 65, de 30 de julho de 2020.

Ainda assim, o usuário pode se valer dos atendimentos relacionados a disponibilidade de sistemas, acesso e perfil de acesso aos sistemas, todos disponíveis através do Portal de Atendimento (Qualitor).

7. Como se dará o acesso aos sistemas que necessitam de configurações especiais na máquina (SIAFI/HOD, certificado digital, etc.), posto que não haverá suporte em máquina pessoal?

A COINF/DSINF/CGTI/DAF disponibilizará manuais de procedimentos com as configurações necessárias para os navegadores (versão, habilitação ou não de java, etc.), de forma que o usuário garanta a compatibilidade técnica necessária de sua máquina. É de inteira responsabilidade do usuário a execução dos procedimentos no seu computador pessoal.

8. O acesso ao Sistema Eletrônico de Controle de Frequência - SISCOF será liberado pela CGTI, ao servidor que aderir ao PGD?

Até o momento a Coordenação-Geral de Gestão de Pessoas, que é a área responsável pelo sistema em questão não autorizou o acesso ao SISCOF por VPN.

9. Quais são os recursos mínimos necessários para a máquina do usuário aderente ao PGD, a fim de garantir a sua acessibilidade e a segurança da informação?

a) Sistema de Antivírus devidamente atualizado, de preferência aqueles reconhecidamente seguros pelo mercado. Segue link de forma exemplificativa, não taxativa: https://www.antivirusguide.com/best-antivirus/?lp=default&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=6478205166&utm_content=99672426616&utm_term=anti%20virus&cid=508925511803&pl=&feeditemid=&targetid=kwd-10697621&mt=b&network=g&device=c&adpos=&p1=&p2=&geoid=1001541&gclid=Cj0KCQjw7pKFBhDUARIsAFUoMDbrhorcZccVY9Kccydhv9gW2h5dUir9rHYYX5Rpyrsvmq8pUIUpJjwaAhdCEALw_wcB

b) Sistema operacional devidamente atualizado, licenciado e configurado. Importante o servidor se atentar se as ferramentas inerentes ao trabalho realizado no DNIT são compatíveis com o Sistema Operacional utilizado. Importante atentar-se também se o SO utilizado ainda recebe suporte da fabricante (atualizações de segurança). No caso do Microsoft Windows, por exemplo, o Windows 7 não deve ser utilizado, posto que não recebe mais suporte pela fabricante.

c) Ferramentas de escritório (editores de texto, de planilhas, etc.) devidamente atualizado e licenciado. Cabe salientar que o TEAMS dispõe de OFFICE365 integrado para uso online, não sendo previsto a instalação na máquina pessoal do usuário.

d) Conexão de internet compatível e viável ao uso das ferramentas relacionadas às respectivas atividades do servidor;

e) Estação de trabalho (Desktop ou Notebook) com configuração e recurso compatíveis ao uso das ferramentas relacionadas às respectivas atividades. Recomenda-se que a estação de

trabalho utilizada no teletrabalho não seja compartilhada com outras pessoas, bem como não seja empregada em uso recreativo (jogos, etc.).

10. O usuário poderá acessar a intranet fora do DNIT?

Caso necessário, o acesso à intranet, se efetivará via Virtual Private Network – VPN, e será concedido conforme solicitação do usuário, estritamente ao sistema/recurso necessário a execução de suas funções, mediante justificativa fundamentada.

11. Quais outros procedimentos e práticas que o servidor em PGD pode seguir para ajudar a garantir a Segurança da Informação no DNIT, mesmo trabalhando remotamente?

Ter ciência da Política de Segurança da Informação e demais instruções normativas relacionadas à Segurança da Informação e a proteção dos dados sensíveis (LGPD). Atentar-se as dicas e cartilhas de segurança publicadas por meio da Coordenação-Geral de Comunicação - CGCOM/DG.

Além disso, é dever do participante manter a infraestrutura necessária para o exercício de suas atribuições, inclusive aquelas relacionadas à segurança da informação, enquanto estiver exercendo suas atribuições dentro do programa de gestão.

O servidor pode cooperar (não obrigação) em caso de incidentes de segurança críticos, entregando o computador para perícia à ETIR - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

O Servidor que identificar possíveis incidentes de segurança da informação, deve relatar o evento encaminhado e-mail para etir@dnit.gov.br

ERISNEI GALDINO DA SILVA MEDEIROS

Assinado digitalmente por ERISNEI GALDINO DA SILVA MEDEIROS
DN: C=BR, O=ICP-Brasil, OU=33683111000107, OU=Pessoa Física A3, OU=ARSERPRO, OU=Autoridade Certificadora SERPRORFC, CN=ERISNEI GALDINO DA SILVA MEDEIROS
Razão: Eu sou o autor deste documento
Localização: sua localização de assinatura aqui
Data: 2021-05-28 16:36:42
Foxit Reader Versão: 10.0.0