

 DCSI	Norma de Autoridade Técnica NAT 07.08	Exemplar n.º 1
		Pág. 1 de 9
		Versão 01
		05ABR21
Assunto:	POLÍTICAS E PROCEDIMENTOS PARA ACESSO REMOTO À RDE	
Referência (s):	NAT 02.03.03 - Normas técnicas e responsabilidades do utilizador, rev1, de 14JAN14	
NAT Relacionadas		

1. GENERALIDADES

O acesso remoto à Rede de Dados do Exército (RDE) verifica-se nas situações em que os utilizadores, não tendo acesso físico à RDE, usam, em alternativa, uma ligação via internet. Tecnicamente, essa ligação é efetuada recorrendo a uma rede privada virtual, denominada de VPN (*Virtual Private Network*), que deverá ser considerada como parte integrante da RDE e, como tal, deverá cumprir os requisitos de segurança em vigor nesta rede.

2. FINALIDADE

Estabelecer as políticas e procedimentos a adotar pelos diferentes intervenientes na implementação e utilização das ligações VPN do Exército, visando o bom desempenho do serviço e a segurança da informação, nas vertentes da confidencialidade e integridade.

3. ÂMBITO

Pessoal do Exército que utiliza ou venha a utilizar acessos remotos à RDE.

4. EXECUÇÃO

a. Conceito

- (1) O acesso remoto à RDE, quando não corretamente efetuado, acarreta riscos adicionais para a rede, pelo que a instalação de ligações VPN deverá ocorrer apenas em situações em que o utilizador:
 - (a) Está colocado numa U/E/O que não tem acesso à RDE;
 - (b) Necessita, por um período prolongado, de aceder a um serviço da RDE não disponibilizado via internet;
 - (c) Está impossibilitado de se deslocar a uma U/E/O com acesso à RDE.
- (2) Para o efeito e de modo a disponibilizar apenas os acessos estritamente necessários, considera-se necessário definir os perfis de posto de trabalho, atendendo às diferentes tipologias de utilização, nomeadamente como terminal

DCSI	NAT 07.08	Pág. 2 de 9
------	-----------	-------------

remoto permanente ou apenas para aceder ao correio eletrónico e a outros portais *web*.

b. **Responsabilidades**

(1) Comandante/diretor/chefe da U/E/O:

Identifica a necessidade de acesso remoto dos utilizadores da sua U/E/O.

(2) Direção de Comunicações e Sistemas de Informação (DCSI):

(a) Define as políticas e procedimentos de utilização dos acessos remotos.

(b) Através do Centro de Transmissões do Exército (CTE):

1. Recebe os pedidos de atribuição de VPN;

2. Determina a sua exequibilidade;

3. Configura, gere e implementa os requisitos de segurança de todos os acessos remotos à RDE.

c. **Implementação do acesso remoto**

(1) **Modalidade A:** UTILIZANDO UM TERMINAL REMOTO DA RDE

(a) Consiste na configuração de um terminal dedicado para aceder a todos serviços disponibilizados pela RDE.

(b) Implementa a proteção dos dados locais (*Full Disk Encryption*), sendo a autenticação efetuada mediante contas do domínio '[exercito.local](#)', especificamente configuradas no terminal remoto. Da avaliação da ameaça existente no local onde esses terminais irão ser utilizados, poderão ser implementados mecanismos de segurança adicionais, nomeadamente o recurso a um dispositivo adicional com um *token*.

(c) Modalidade que garante maior segurança. Deve ser configurada em computadores portáteis a distribuir a elementos ou forças nacionais destacadas (END/FND) ou a entidades localizadas em U/E/O sem acesso à RDE. Em situações excecionais, devidamente autorizadas, poderá ser distribuída a outros utilizadores individuais.

(d) O principal inconveniente desta modalidade é exigir uma configuração complexa e demorada, bem como necessitar de *hardware* com características técnicas mais exigentes (memória, disco SSD e processador).

(e) Apenas a DCSI (CTE) detém capacidade para fornecer apoio remoto a estes terminais.

DCSI	NAT 07.08	Pág. 3 de 9
------	-----------	-------------

(2) **Modalidade B:** UTILIZANDO O TERMINAL DA RDE DO POSTO DE TRABALHO

- (a) Consiste em configurar um computador já em utilização na RDE com uma ligação VPN, sendo este posteriormente deslocado para outro local com acesso à Internet, fora das infraestruturas do Exército.
- (b) O terminal funciona *per si*, tendo ou não a VPN ligada e não utiliza encriptação do disco. Por isso, constitui uma opção menos segura do que a modalidade A.
- (c) Nesta modalidade de acesso remoto, é instalado no computador indicado um cliente VPN com um certificado emitido exclusivamente para um utilizador, sendo este protegido por uma *password* que é previamente enviada para o utilizador.
- (d) É uma opção de recurso, devendo ser de carácter temporal limitado.
- (e) Tem como vantagem a rapidez da instalação e de não necessitar de equipamento adicional e específico, pois as estações de trabalho das U/E/O já estão configuradas com as políticas da RDE.
- (f) O administrador de rede local da respetiva U/E/O tem capacidade de dar apoio remoto através da consola de administração do *System Center Configuration Manager* (SCCM) e mantém a responsabilidade pela monitorização dos terminais configurados com esta modalidade, devendo, designadamente, cumprir o preconizado no manual de procedimentos do administrador local.

(3) **Modalidade C:** UTILIZANDO UM TERMINAL COM ACESSO À INTERNET ATRAVÉS DO PORTAL VPN

- (a) Esta modalidade permite o acesso a alguns recursos da RDE, nomeadamente ao portal pessoal, à gestão documental, entre outros, através de uma VPN acedida via portal web no seguinte endereço: <https://rd.exercito.pt>.
- (b) Poderá ser utilizado qualquer terminal para acesso a este Portal VPN, sem a necessidade de qualquer configuração adicional.
- (c) Como requisito prévio, os utilizadores deverão efetuar o registo individual, configurando a autenticação multifator através da página principal da Intranet do Exército (icon “Multifator”, na área SERVIÇOS).
- (d) O acesso ao portal é feito com as credenciais da RDE, nomeadamente NIM e password, acrescido de um segundo fator de autenticação, código enviado para um endereço de correio eletrónico alternativo ou via SMS, ou utilizando outro esquema de dupla autenticação como o *Microsoft Authenticator*.
- (e) Modalidade preferencial para aceder remotamente à RDE, a menos que as necessidades operacionais justifiquem a adoção de outra modalidade.

DCSI	NAT 07.08	Pág. 4 de 9
------	-----------	-------------

- (f) Acesso aos recursos do portal VPN através de grupos de utilizadores sistematizados em função da tipologia e da necessidade de aceder a serviços/informação da, nomeadamente:

1. GRUPO ACESSO

- Acessibilidade ao *Portal pessoal*, ao *Webmail* e ao *Portal da intranet*;
- Utilizadores sem necessidades suplementares de acesso aos sistemas de informação;
- Pessoal colocado fora da estrutura do Exército.

2. GRUPO UTILIZADOR

- Acessibilidade do Grupo ACESSO, à Gestão Documental, aos portais colaborativos da sua U/E/O e ao SIGOp;
- Utilizadores com necessidades de acesso aos sistemas de informação.

3. GRUPO TÉCNICO

- Acessibilidade do Grupo UTILIZADORES, a ferramentas de gestão e controlo de serviços de rede e ao *ServiceDesk*;
- Administradores de rede local e administradores de domínio.

4. GRUPO ADHOC

- A definir em função de necessidades específicas.

d. **Dados de autenticação e encriptação**

- (1) Os elementos de autenticação e encriptação devem ser convenientemente protegidos, devendo, em caso de suspeita de comprometimento, ser imediatamente alterados.
- (2) O certificado digital, com *password*, atribuído a um utilizador, permite a encriptação do tráfego entre o terminal do utilizador e o servidor de VPN na RDE, sendo essencial a proteção desse certificado. O titular do certificado é responsável por todas as ações realizadas através desse acesso VPN.
- (3) Por razões de segurança, os certificados devem ser renovados a cada dois anos. Para o efeito o utilizador é alertado automaticamente da data em que o certificado expira, devendo, caso continue a necessitar da ligação VPN, solicitar a respetiva renovação junto do administrador de rede local que encaminhará o pedido para a DCSI (CTE), via *ServiceDesk*.
- (4) No caso dos terminais remotos (modalidade A), configurados com contas de função distribuídos a END/FND, o certificado deverá ser alterado sempre que o militar é

DCSI	NAT 07.08	Pág. 5 de 9
------	-----------	-------------

substituído. Deverá ser elaborado um certificado de transferência, conforme Anexo B, e enviada uma cópia assinada à DCSI (CTE).

- (5) Sempre que a utilização da VPN deixe de ser necessária, a DCSI (CTE) deve ser imediatamente informada, via *ServiceDesk*, de modo a proceder à revogação do respetivo certificado, impedindo assim eventuais acessos não autorizados.

e. **Autorização formal**

- (1) A atribuição da VPN será realizada após preenchimento de formulário, conforme anexo A, sendo este verificado pelo administrador de rede local da U/E/O e autorizado pelo respetivo cmdt/dir/ch.
- (2) O formulário deverá ser preenchido preferencialmente em formato digital e utilizando a assinatura digital. Na impossibilidade, e após assinatura manual, deverá ser digitalizado.
- (3) No formulário, deve constar a identificação do utilizador, posto, NIM, nome e contacto telefónico, a identificação do terminal a configurar (nome no domínio '[exercito.local](#)' e endereço MAC), bem como a especificação de quais os serviços que justificam a necessidade de acesso remoto. Após preenchimento deverá ser enviado para a DCSI (CTE) via *ServiceDesk*.
- (4) Após autorizada a configuração do terminal para acesso remoto, a auditoria prévia e configuração do terminal, com a instalação do respetivo certificado, é efetuada pela DCSI (CTE), em coordenação com o administrador de rede local da U/E/O.
- (5) No caso da modalidade A, após a receção do pedido de configuração do terminal remoto (formulário do anexo A) a DCSI (CTE) confirma os requisitos de hardware e informa a U/E/O da viabilidade do pedido. Após autorização, a U/E/O entrega na DCSI (CTE) o respetivo computador. Após a configuração este equipamento é devolvido ao utilizador mediante a assinatura do documento onde constam os termos de utilização do terminal, conforme Anexo B.

f. **Responsabilidades do utilizador da VPN**

- (1) O utilizador de um terminal com ligação VPN à RDE deve cumprir com todas as normas em vigor na RDE.
- (2) O utilizador é responsável pela boa utilização e salvaguarda física do terminal, assegurando que apenas pessoal devidamente autorizado tenham acesso ao mesmo.

DCSI	NAT 07.08	Pág. 6 de 9
------	-----------	-------------

- (3) O utilizador não deve permitir que o certificado seja exportado para uso nouro equipamento que não aquele para o qual foi emitido. No caso de suspeita de má utilização ou de usurpação do certificado, o acesso ser-lhe-á bloqueado e iniciada a competente investigação de segurança.
- (4) Excetuando quando previamente autorizados pela DCSI (CTE), é vedada ao utilizador e ao administrador de rede local quaisquer alterações à configuração original da VPN instalada.
- (5) Quando estabelecida a VPN o terminal encontra-se logicamente ligado à RDE. Assim, por motivos de segurança, a VPN deverá ser desligada sempre que o acesso à RDE não estiver a ser necessário.
- (6) Em caso de extravio ou suspeitas de acesso indevido, deve ser contactado imediatamente o CTE/DCSI.
- (7) Relativamente à utilização do portal VPN, o utilizador deve zelar pela segurança do dispositivo que utiliza para aceder ao portal, tendo sempre presente que a informação descarregada deverá ser eliminada logo que não seja necessária, especialmente se for considerada sensível.

g. **Utilização da VPN para teletrabalho ou serviço em prontidão no domicílio**

- (1) Em contexto de teletrabalho ou serviço em prontidão no domicílio, a exposição ao risco aumenta. Eventuais situações de comprometimento destes terminais poderão concorrer para o comprometimento da RDE.
- (2) Qualquer uma das modalidades de VPN pode ser utilizada para a execução de teletrabalho em ambiente não controlado, desde que se disponha de um acesso à Internet.
- (3) Para se deslocalizar um terminal da sua estação de trabalho para outro local, o administrador de rede local da U/E/O tem de ter conhecimento, deverá existir a autorização explícita do cmdt/dir/ch da U/E/O e parecer favorável do CTE/DCSI, conforme Anexo A.

h. **Monitorização dos acessos remotos**

- (1) A DCSI (CTE) monitoriza todos os acessos remotos à RDE, identificando possíveis ameaças que possam colocar em risco a informação residente ou a própria rede.
- (1) Caso sejam detetadas situações anómalas na utilização das VPN, o utilizador deverá ser imediatamente contactado, no sentido de se esclarecer a situação, mitigar riscos e eliminar eventuais ameaças.

DCSI	NAT 07.08	Pág. 7 de 9
------	-----------	-------------

- (2) Para eventuais situações que não sejam imediatamente resolvidas e constituam uma ameaça grave à RDE, a DCSI (CTE) deve desativar o acesso do terminal à RDE via VPN e instaurar a competente investigação de segurança.

5. INSTRUÇÕES DE COORDENAÇÃO

- a. A disponibilização de um terminal de acesso remoto à RDE determina que o utilizador tenha o prévio conhecimento da presente NAT e da NAT 02.03.03.
- b. Os contactos com a DCSI (CTE) devem ser efetuados preferencialmente via *ServiceDesk*, através do e-mail cte.apoio@exercito.pt, telefone 421060 / 218117053.
- c. Para situações urgentes contactar o graduado de serviço à Sala de Situação da DCSI, telefone 421111 / 913283671.

6. ENTRADA EM VIGOR

Esta NAT entra em vigor na data da sua publicação, devendo ser revista sempre que se considere necessário.

O Vice-Chefe do Estado-Maior do Exército

**Rui Davide Guerra Pereira
Tenente-General**

AUTENTICAÇÃO


O Diretor de Comunicações e Sistemas de Informação

**Luis Filipe Camelo Duarte Santos
Brigadeiro-General**


Anexos:

- A - FORMULÁRIO DE PEDIDO DE CONFIGURAÇÃO DE ACESSO REMOTO À RDE
- B - TERMOS DE UTILIZAÇÃO DO TERMINAL REMOTO

Distribuição: Conforme lista BRAVO da NAT 00.01 da DCSI

 DCSI	NAT 07.08 ANEXO A	Exemplar n.º 1
		Pág. 8 de 9
		Versão 01
		05ABR21
Assunto:	Formulário de pedido de configuração de acesso remoto à RDE	

PEDIDO DE CONFIGURAÇÃO DE ACESSO REMOTO À RDE (NAT 07.08 da DCSI) [depois de preenchido enviar para cte.apoio@exercito.pt]	
IDENTIFICAÇÃO DA U/E/O	
IDENTIFICAÇÃO DO REQUERENTE (utilizador do terminal)	Posto: NIM: Nome:
	Contacto telef:
	Tenho conhecimento das NAT 07.08 e NAT 02.03.03 da DCSI.
	Data: Assinatura:
MOTIVO DO PEDIDO (justificar a necessidade do acesso remoto e quais os serviços necessários aceder)	
TERMINAL A CONFIGURAR (a preencher pelo administrador de rede local)	MARCA/MODELO:
	NOME DE DOMÍNIO:
	MAC ADDRESS:
	MAC ADDRESS (PLACA WIFI):
	Modalidade de acesso remoto: A <input type="checkbox"/> B <input type="checkbox"/> Data: Assinatura:
AUTORIZAÇÃO	O CMDT/DIR/CHEFE Autorizo o pedido, Data: Assinatura:
CONFIGURAÇÃO (CTE/DCSI)	Configurado por:
	Obs:
	Data: Assinatura:

 DCSI	NAT 07.08 ANEXO B	Exemplar n.º 1
		Pág. 9 de 9
		Versão 01
		05ABR21
Assunto:	Termos de utilização do terminal remoto	

ATRIBUIÇÃO DE ACESSO REMOTO À RDE (NAT 07.08 da DCSI)	
<p align="center"><u>Termo de Responsabilidade</u></p> <p>O terminal abaixo indicado está configurado para permitir aceder à Rede de Dados do Exército (RDE) através da Internet, por meio de uma ligação encriptada segura, denominada por VPN (<i>Virtual Private Network</i>), mediante utilização de um Certificado instalado e autorizado para determinados utilizadores. A utilização deste terminal é regulada pela NAT 07.08 da DCSI.</p> <p>A segurança física do terminal deve ser salvaguardada pelo utilizador.</p> <p>Em caso de extravio ou suspeitas de acesso indevido, deve ser contactado imediatamente o Centro de Transmissões do Exército/DCSI através dos seguintes contactos:</p> <ul style="list-style-type: none"> • <u>ServiceDesk</u>: 421060 / 218117053 cte.apoio@exercito.pt • Graduado de serviço à sala de situação da DCSI: 421111 / 913283671 	
UTILIZADORES AUTORIZADOS (exemplo: 'afg.ts')	
DADOS DO MATERIAL (indicar quantidade, designação e número de série)	
<p>Ao assinar este termo de responsabilidade declaro que:</p> <ul style="list-style-type: none"> • Tenho conhecimento das NAT 07.08 e NAT 02.03.03 da DCSI; • Tomei conhecimento que o equipamento fornecido permite aceder à RDE, devendo cumprir as normas em vigor para essa rede; • Recebi o material acima descrito mediante as condições especificadas. 	
IDENTIFICAÇÃO DO UTILIZADOR	Posto: NIM: Nome:
	Contato telefónico:
	Data:
	Assinatura: