	Norma de uso da VPN			
	Código: POL-CRI-010	Subarea: Seguranca	Tempo Execução:	STI Superintendência de Tecnologia da Informação | UFBA
	Estado: APROVADO		Classificação: Reservada	
	Autor: ThiagoLazaroDeSouzaNogueira			
	Revisor: KleberRibeiroMascarenhasSilvaJunior, LuizGonzagaDeAlmeidaNeto, WiltonBritoDeJesus			
	Última atualização: 14 Jun 2022			

1 Apresentação

A VPN da Universidade Federal da Bahia (UFBA) é um serviço de acesso remoto ao ambiente corporativo cibernético da universidade, fornecido, mantido e suportado pela Coordenação de Redes e Infraestrutura (CRI) da Superintendência de Tecnologia da Informação (STI) e ofertado aos seus usuários, de acordo com as diretrizes estabelecidas nesta norma.

A idealização de qualquer serviço do tipo VPN visa oferecer aos seus usuários a praticidade de uso de uma rede corporativa a partir de um acesso à internet, simulando perfeitamente a presença física, com requisitos de segurança que asseguram o ambiente computacional da universidade contra ataques e agentes externos maliciosos.

É imprescindível que todos os usuários do serviço de VPN estejam conscientes dos riscos envolvidos para a instituição em decorrência de mal uso do serviço ou de suas credenciais. Portanto, este documento elencará as responsabilidades dos usuários que forem autorizados à utilização deste serviço.

Dentre os riscos supracitados, podemos exemplificar:

1. Invasão a rede e sistemas: Uma conta qualquer de usuário comprometida pode facilmente dar acesso a um invasor para que o mesmo possa realizar ataques mais agressivos à rede corporativa da UFBA.
2. Integridade de arquivos: Arquivos podem ser modificados de forma indevida com uma conta comprometida, além disso, a conta tendo acesso a sistemas corporativos, esta também poderá efetuar alterações, solicitações e exclusões em nome do proprietário da conta.
3. Golpes a terceiros: Uma conta invadida poderá criar golpes cibernéticos como SPAM, Phishing, dentre outros em nome do proprietário da conta.

O serviço de VPN conta com 3 tipos distintos de acesso, a saber:

a. **Portal de Acesso Remoto** - Acessível a todos os usuários que solicitarem e forem autorizados ao uso da tecnologia, permite acesso ao ambiente interno da UFBA por meio de um portal web disponível em http://acesso.ufba.br:65443. Esta é a opção padrão de acesso à rede corporativa da UFBA.

b. **Túnel de Acesso Remoto (Via cliente VPN)** - O usuário possui permissões semelhantes ao ambiente do Portal de Acesso Remoto, porém é necessária a instalação de um software (cliente) que cria uma interface virtual no computador do usuário, permitindo uso de aplicações do tipo Cliente-Servidor.

Ressalta-se que qualquer usuário com permissão de acesso ao ambiente do Túnel via cliente também poderá fazer uso do Portal de Acesso Remoto.

c. **VPN IPSEC** - Acesso restrito ao corpo técnico de TI para manutenção do ambiente computacional centralizado.

2 Objetivo e Abrangência

A VPN disponibilizada pela STI tem como objetivo fornecer acesso remoto seguro à Rede Corporativa da UFBA a partir de computadores que estejam conectados à internet, fornecendo, assim, uma forma segura para os usuários que tenham a necessidade, exclusivamente relacionada às atividades administrativas e acadêmicas, de acessar recursos disponíveis na rede corporativa.

Por padrão, todos os servidores (docentes e tecnico-administrativos) ativos possuem permissão e concessão de acesso ao serviço de VPN.

Alunos, sejam eles de graduação ou pós graduação, e terceiros (prestadores de serviço) podem fazer uso do serviço, desde que seja encaminhado pedido por solicitante competente para tal e que todas as medidas trazidas nesta norma sejam respeitadas.

3 Conceitos e Definições

Rede Corporativa - Rede interna de uma organização, que em condições padrões de uso não é acessível a partir da internet.

VPN IPSec - Virtual Private Network (Rede Privada Virtual) que utiliza o protocolo IPSec para permitir conexões remotas de usuários às redes corporativas.

VPN SSL - Virtual Private Network (Rede Privada Virtual) que utiliza o protocolo SSL/TLS para permitir conexões remotas de usuários às redes corporativas.

Portal de Acesso Remoto - Portal WEB sobre o protocolo SSL/TLS que faz a interface entre o usuário e a rede corporativa utilizando os conceitos da VPN SSL acima.

Forticlient - Aplicação cliente que é instalada no computador do usuário para possibilitar conexões VPN (IPSec e SSL) diretas, sem necessidade de acesso ao Portal de Acesso Remoto.

Permissão - **Autorização legal** por profissional competente de uso ou acesso de um determinado serviço e/ou sistema.

Concessão - **Autorização técnica** de uso de um determinado serviço e/ou sistema, desde que o usuário possua permissão para tal.

LGPD - Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018.

Solicitante - Dirigente de unidade administrativa/acadêmica, chefe, coordenador de programa de pós-graduação ou de grupo de pesquisa e demais dirigentes legalmente constituídos.

Usuário - Pessoa que usa o serviço de VPN, a partir de uma conta válida na rede UFBA.

4 Diretrizes

a. A instalação e configuração dos aplicativos necessários ao estabelecimento da conexão VPN ficarão a cargo do próprio usuário, apoiado pela Central de Serviços da STI, caso deseje.

b. O acesso à Rede Corporativa por meio da VPN deverá ser exclusivamente para usos relacionados às atividades administrativas e acadêmicas, sendo proibida a sua utilização para outra finalidade que não o

desempenho das atividades relacionadas à sua função nesta Instituição.

c. O possuidor das credenciais de acesso à VPN é o único responsável pela salvaguarda das informações necessárias ao acesso à Rede Corporativa (senha, nome de usuário, endereço do *gateway* remoto e demais informações de acesso remoto).

d. O compartilhamento das credenciais de acesso à VPN é terminantemente proibido, podendo caracterizar crime de Violação de Sigilo Funcional, tipificado no Decreto Lei nº 2.848/40 (Código Penal). Ressalta-se que todo acesso é registrado e auditado, em conformidade com a LGPD e Política de Segurança da Informação e Comunicações da UFBA (PoSIC).

e. Não é recomendado o uso da VPN em redes WiFi públicas, abertas (sem criptografia) ou compartilhadas por terceiros.

f. Os computadores que possuírem aplicativos configurados com as informações de acesso à Rede Corporativa por meio da VPN deverão possuir mecanismo de controle de acesso que utilize, no mínimo, usuário e senha, e aplicativo antivírus atualizado, devendo o uso desses ser restrito ao usuário detentor da credencial de acesso. Havendo a necessidade do compartilhamento do computador, as informações, definidas no aplicativo de acesso à VPN, deverão ser excluídas.

g. Para a concessão de credencial de acesso à VPN o Solicitante do Setor, obrigatoriamente, necessita solicitar via Central de Serviços.

h. A responsabilidade de informar à STI o desligamento ou inatividade de qualquer integrante possuidor de credenciais de acesso à VPN é do Solicitante, colaborando assim com a segurança da Rede Corporativa da UFBA.

i. O acesso ao serviço de VPN a usuários não-servidores (alunos e terceiros) terá **validade de um ano**. Havendo necessidade de renovação deste prazo, a solicitação de revalidação do acesso VPN deve ser realizada pelo Solicitante legal, dentro dos prazos de validade para cada conta.

j. Contas institucionais não são elegíveis para fazerem uso do acesso à VPN.

5 Competência e Responsabilidades

Cabe à STI

- Orientar quanto aos procedimentos de instalação e configuração das VPNs disponíveis no ambiente UFBA, bem como realizar o credenciamento e descredenciamento de usuários, mediante pedido do Solicitante;
- Orientar o usuário nas dificuldades técnicas apresentadas relacionadas aos sistemas operacionais e softwares integrantes do serviço de VPN, mediante solicitação do usuário à Central de Serviços;
- Descredenciar o usuário após sua desvinculação da UFBA, obedecendo as regras, normas e diretrizes vigentes;
- Avaliar a solução, requisições de usuários e demais questões técnicas relacionadas ao serviço de VPN, sempre com a finalidade de prezar pela segurança da informação da instituição;
- Sugerir melhorias técnicas e processuais, no que tange ao serviço de VPN, adotando, neste caso, uma postura proativa; e
- Apoiar o Comitê de Segurança da Informação e Comunicações no julgamento de penalidades aos usuários que infrigirem as diretrizes desta norma.

Cabe ao Comitê de Segurança da Informação e Comunicações – CSIC:

- Deliberar sobre penalidades impostas aos descumprimentos desta norma; e
- Auxiliar na melhoria contínua da segurança do serviço, de ofício ou a pedido da STI.

Cabe ao Usuário do Serviço:

- Zelar pelo fiel cumprimento desta norma, bem como dos princípios de segurança da informação;
- Zelar pela sua credencial de acesso, utilizando as boas práticas para o uso e construção da senha; e
- Notificar a STI sobre qualquer incidente envolvendo sua conta de acesso ou serviços informatizados da UFBA durante o uso do serviço de VPN;

6 Violação a esta Norma de Uso e Sanções

a. O não cumprimento das normas definidas nesta norma poderá acarretar em sanções administrativas, civis e penais, cumulativas ou não, a depender do incidente ocasionado ou postura adotada pelo usuário.

b. A depender das consequências resultantes do descumprimento das normas supramencionadas, caberão as seguintes sanções administrativas, sem prejuízo das demais provisões normativas legais:

1. **Advertência** - alerta ao usuário através de seu e-mail ou telefone pessoal;
2. **Suspensão temporária do serviço** - usuário perderá o acesso ao serviço VPN por um período que pode variar de 7 a 30 dias corridos, a depender da gravidade do fato, sendo enviado ao solicitante uma notificação do ocorrido;
3. **Suspensão permanente do serviço** - usuário perderá acesso ao serviço VPN por tempo indeterminado, sendo enviado ao solicitante uma notificação do ocorrido;

c. Havendo aplicação de quaisquer das sanções administrativas supracitadas o superior imediato responsável pelo usuário será notificado do fato ocorrido.

d. Cabe ao **Comitê de Segurança da Informação e Comunicações – CSIC** a avaliação das penalidades acima descritas, zelando pelo justo cumprimento.

e. Cabe à **Superintendência de Tecnologia da Informação - STI** aplicar as penalidades definidas acima.

f. Demais sanções deverão ser direcionadas para o **CSIC** para avaliação e providências cabíveis, concomitantemente às sanções administrativas supracitadas.

7 Disposições Finais

Sempre que houver mudança de tecnologia ou arquitetura do serviço de VPN, por necessidade da instituição, esta norma deverá ser revisada e adequada para a realidade a que se dispõe.

Os serviços de VPN não elencados nesta norma serão descontinuados quando a presente norma entrar em vigor.

Esta norma entra em vigor a partir de 15 de junho de 2022, data em que foi publicada a referida Portaria.

8 Referências

- Lei nº 8.112/90 - Dispõe sobre o regime jurídico dos servidores públicos civis da União;
- Lei nº 13.708/18 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Decreto-Lei 2.848/40 - Código Penal; e

- Política de Segurança da Informação e Comunicações da UFBA - POSIC;

9 Controle de versão

Rev	Data	Descrição	Itens revisados	Revisado por
00	11/02/2021	Criação do Documento	--	nogueira.thiago
01	03/03/2021	Atualização do Documento	--	cristinofilho
02	22/06/2021	Atualização do Documento pós revisão da Coordenação	--	nogueira.thiago
03	03/08/2021	Atualização do Documento pós 2ª revisão da Coordenação	--	nogueira.thiago
04	19/08/2021	Atualização do Documento pós 3ª revisão da Coordenação	--	nogueira.thiago
05	27/08/2021	Atualização do Documento pós revisão da Superintendência	--	nogueira.thiago
06	27/09/2021	Atualização do Documento pós revisão da Superintendência	--	nogueira.thiago
07	25/04/2022	Alteração do termo 'Portal SSL' para 'Portal de Acesso Remoto', conforme definido em reunião com coordenação	--	nogueira.thiago