ATO NORMATIVO Nº 02/2024 CGI

Regulamentar as normas de uso da Rede Virtual Privada da Universidade Federal do Sul da Bahia para o uso exclusivo em atividades administrativas e acadêmicas.

O **COMITÊ DE GOVERNANÇA INSTITUCIONAL DA UNIVERSIDADE FEDERAL DO SUL DA BAHIA**, no uso de suas atribuições definidas pela Portaria nº 362/2024,

CONSIDERANDO a Resolução nº 06/2021 - Política de Segurança da Informação da UFSB;

CONSIDERANDO a Resolução nº 24/2021 - Código de Ética Estudantil da UFSB -;

CONSIDERANDO o Decreto Federal nº 1.171/1994 - Código de Ética do Servidor Público;

CONSIDERANDO a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Lei nº 12.965/2014 - Marco Civil da Internet -

CONSIDERANDO o Decreto nº 10.332/2020 - Estratégia de Governo Digital

CONSIDERANDO a Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI);

CONSIDERANDO a Lei nº 13.460/2017 - Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública

CONSIDERANDO a Lei nº 13.709/2018 - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

CONSIDERANDO a Lei nº 13.444/2017 - Dispõe sobre a Identificação Civil Nacional (ICN)

CONSIDERANDO o Decreto nº 8.777/2016 - Institui a Política de Dados Abertos do Poder Executivo Federal

CONSIDERANDO o Decreto nº 7.724/2012 - Regulamenta a Lei nº 12.527/2011, Lei de Acesso à Informação

CONSIDERANDO o Decreto nº 7.845/2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento

CONSIDERANDO a Lei nº 12.737/2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848/1940 Código Penal; e dá outras providências.

RESOLVE:

Art. 1º Aprovar as normas de uso da Rede Virtual Privada da Universidade Federal do Sul da Bahia para o uso exclusivo em atividades administrativas e acadêmicas.

Art. 2º Este Ato entra em vigor na data de sua publicação.

CAPÍTULO I
DO OBJETIVO

Art. 3º Regulamentar o uso da Rede Virtual Privada da Universidade Federal do Sul da Bahia (VPN UFSB), informando suas características e estabelecendo diretrizes para seu uso adequado, a fim de garantir a segurança, privacidade das informações trafegadas, bem como um acesso remoto seguro aos recursos da universidade.

Art.4º O uso da VPN é exclusivo para atividades administrativas e acadêmicas.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 5º Esta Norma se aplica a todos os usuários da comunidade da UFSB que utilizam o serviço VPN.

Art. 6º Servidores (docentes e técnicos-administrativos) da UFSB podem requerer a permissão e concessão de acesso ao serviço da VPN através da abertura de um chamado via Helpdesk (https://helpdesk.ufsb.edu.br/).

Art. 7º Discentes, prestadores de serviço (servidores terceirizados) e pesquisadores externos, podem fazer uso do serviço, desde que seja encaminhado pedido por solicitante competente para tal (docente ou técnico-administrativo da UFSB) através do Helpdesk e que todas as medidas trazidas nesta norma sejam respeitadas.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 8º Para os efeitos do disposto neste Ato, considera-se:

I. **Acesso remoto SSH:** método de acesso remoto seguro a servidores e dispositivos de rede, utilizando o protocolo SSH (Secure Shell) para garantir a criptografia dos dados transmitidos.

II. **Acesso remoto Windows:** método de acesso remoto a computadores que utilizam o sistema operacional Windows, geralmente implementado através do protocolo RDP (Remote Desktop Protocol).

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

IV. **Credenciais de acesso:** informações, como nome de usuário e senha, utilizadas para autenticar um usuário e permitir seu acesso aos recursos da rede.

V. **Criptografia:** técnica de proteção de informações que transforma dados legíveis em formato codificado, acessível apenas a quem possui a chave de decodificação.

VI. **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.

VII. **Permissão:** autorização legal por órgão competente de uso ou acesso de um determinado serviço e/ou sistema.

VIII. **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.

IX. **Rede corporativa:** rede interna de uma organização, que em condições padrões de uso não é acessível a partir da internet.

X. **Rede virtual privada (VPN):** Tecnologia que cria uma conexão segura e criptografada através de uma rede pública, como a internet, simulando a presença física na rede corporativa da universidade.

XI. **Segurança da informação:** conjunto de práticas e medidas para proteger informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados.

XII. **Unidade gestora do serviço:** representada pela Superintendência de Tecnologia da Informação (STI) e pelos Setores de Operações Locais de TIC dos campi Jorge Amado (CJA), Sosígenes Costa (CSC) e Paulo Freire (CPF) da UFSB.

XIII. **Usuário:** discentes, Docentes, Técnicos-Administrativos, Prestadores de serviço (servidores terceirizados) que utilizam os recursos da rede da universidade.

XIV. **VPN IPSec:** IPSec (Internet Protocol Security) é um protocolo de segurança utilizado em VPNs que oferece criptografia e autenticação para proteger os dados transmitidos

através de redes públicas. Com software cliente dedicado, o VPN IPSec estabelece túneis de rede seguros entre duas redes, ideal para conexões de site-a-site.

XV. **VPN SSL:** é um protocolo de segurança que permite a criação de conexões VPN seguras através de navegadores web, utilizando criptografia SSL (Security Sockets Layer).

CAPÍTULO IV
DAS DIRETRIZES

Art. 9º Para concessão de credencial de acesso à VPN, o requisitante, obrigatoriamente, deve solicitar no sistema de chamados da UFSB, o Helpdesk.

Art. 10º A ativação da VPN será realizada após a assinatura do Termo de Responsabilidade (Anexo I) via SIPAC (Sistema de Patrimônio, Administração e Contratos).

Art. 11º A instalação e configuração dos aplicativos necessários ao estabelecimento da conexão VPN ficarão a cargo do próprio usuário, apoiado pelo Manual de Uso da VPN (Disponível em: https://manuais.ufsb.edu.br/books/conectar-vpn-ufsb) e Unidade Gestora do Serviço, quando necessário.

Art. 12º As credenciais de acesso serão as mesmas usadas na autenticação dos serviços da UFSB.

Art. 13 º O usuário da VPN é o único responsável pela salvaguarda das informações necessárias ao acesso à Rede Corporativa (nome de usuário, senha, endereço do *gateway* remoto e demais informações de acesso remoto).

Art. 14º O acesso à Rede Corporativa por meio da VPN deverá ser exclusivamente para usos relacionados às atividades administrativas e acadêmicas, sendo terminantemente vedada a utilização do serviço para demais fins.

Art. 15º O compartilhamento das credenciais de acesso à VPN é terminantemente proibido, podendo caracterizar crime de Violação de Sigilo Funcional, tipificado na Lei nº 12.737/2012. É importante salientar que todo acesso é registrado e auditado, em conformidade com a LGPD e a Política de Segurança da Informação da UFSB.

Art. 16º Não é recomendado o uso da VPN em redes WiFi públicas, abertas (sem criptografia) ou compartilhadas por terceiros.

Art. 17º Para acesso à Rede Corporativa da UFSB através da VPN, o computador/servidor do usuário deve:

I. Possuir mecanismo de controle de acesso, que utilize no mínimo usuário e senha;
II. Aplicativo antivírus atualizado;
III. Sistema operacional com licença válida, se Windows;
IV. *Patches* de segurança atualizados e instalados;
V. Configurar o *firewall* de maneira que as regras sejam as mais restritivas possíveis, para maximizar a segurança.

Art. 18º Os equipamentos pessoais para acesso à VPN passam a ser uma extensão da Rede Corporativa da UFSB e como tal, estão sujeitas às mesmas regras, políticas e regulamentações que se aplicam aos equipamentos de propriedade da UFSB, ou seja, as máquinas dos usuários com acesso a VPN devem ser configuradas para atender às normas da instituição.

Art. 19º Preferencialmente o computador do usuário da VPN da UFSB deve ser restrito ao usuário detentor da credencial de acesso. Havendo necessidade do compartilhamento do computador, as informações, definidas no aplicativo de acesso à VPN, deverão ser excluídas.

Art. 20º É de responsabilidade do solicitante informar à Unidade Gestora do Serviço o desligamento ou inatividade de qualquer integrante possuidor de credenciais de acesso à VPN, colaborando assim com a segurança da Rede Corporativa da UFSB.

Art. 21º A validade do acesso ao serviço da VPN será de:

I. prestadores de serviço (servidores terceirizados) e pesquisadores externos: o acesso será válido por 6 (seis) meses;

II. discentes: o acesso será válido por 1 (um) ano.

§1º Após o término da validade do acesso, os pesquisadores externos terão um prazo adicional de 2 (dois) meses para solicitar a renovação. Caso a renovação não seja solicitada dentro deste período, o acesso será excluído.

§2º A inatividade do acesso por 6 (seis) meses resultará na suspensão do serviço para qualquer usuário.

§3º Havendo necessidade de renovação, a solicitação de revalidação do acesso VPN deve ser realizada pelo solicitante competente via Helpdesk.

§4º O acesso ao serviço da VPN poderá ser revogado a qualquer momento, em caso de incidente ou uso indevido do serviço.

Art. 22º Fica restrito apenas uma única conexão VPN, por usuário, com a Rede Corporativa da UFSB.

Art. 23º A cada usuário será provido o acesso à Rede Corporativa da UFSB por meio da VPN de apenas 1 (um) equipamento devidamente registrado no cadastro de usuários da Unidade Gestora do Serviço.

Art. 24º Não será permitido utilizar programas "*peer-to-peer*" (Torrent, eMule, Napster, Bitcoin, entre outros) sobre a VPN.

Art. 25º Não será permitido utilizar o acesso a VPN para transferência de grandes volumes de dados.

Art. 26º A Unidade Gestora do Serviço não se responsabiliza pelo que é feito, pelo usuário, ao utilizar o serviço VPN.

Art. 27º Contas de setores não são elegíveis para fazerem uso do acesso à VPN.

CAPÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES DA UNIDADE GESTORA DO SERVIÇO

Art. 28º Orientar quanto aos procedimentos de instalação e configuração das VPNs disponíveis no ambiente da UFSB, bem como realizar o credenciamento e descredenciamento de usuários, mediante pedido do solicitante ou de acordo com a validade do acesso.

Art. 29º Orientar o usuário nas dificuldades relacionadas aos softwares integrantes do serviço VPN, mediante solicitação do usuário via Helpdesk.

§1º Não cabe a Unidade Gestora do Serviço realizar suporte técnico aos softwares instalados nos servidores de projetos de terceiros, sendo este de única e exclusiva responsabilidade do pesquisador.

Art. 30º Descredenciar o usuário após a sua desvinculação da UFSB ou após findar-se o prazo de validade do acesso, obedecendo às regras, normas e diretrizes vigentes.

Art. 31º Monitorar o volume de dados das conexões VPN e desconectar qualquer sessão onde se verifique taxas divergentes da média normal das outras sessões que comprometam o bom desempenho da Rede Corporativa da UFSB.

Art. 32º Auditar, quando necessário e com autorização do usuário, os sistemas utilizados e a comunicação de dados para acesso, por meio de VPN à Rede Corporativa da UFSB, a fim de verificar a aderência aos requerimentos de segurança aqui mencionados.

Art. 33º A Unidade Gestora do Serviço poderá por motivos de segurança e/ou outros, suspender o serviço de VPN, sem aviso prévio.

Art. 34º Avaliar requisições dos usuários e demais questões técnicas relacionadas ao serviço VPN, sempre com a finalidade de prezar pela segurança da informação da instituição.

Art. 35º Apoiar o Comitê de Segurança da Informação da UFSB no julgamento de penalidades aos usuários que infringirem as diretrizes desta norma.

Art. 36º A Unidade Gestora do Serviço não poderá ser responsabilizada por:

a) Equipamento infectado ou invadido por atacantes
b) Equipamento avariado no momento do consumo de serviços
c) Proteção de computador não pertencente à UFSB
d) Proteção das informações nos computadores dos usuários
e) Monitoração clandestina do computador dos usuários
f) Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários

Art. 37º Em hipótese alguma a Unidade Gestora do Serviço será responsável pela instalação no equipamento do usuário ou de terceiros, de códigos maliciosos em decorrência da navegação na internet pelo usuário.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO (COSIC)

Art. 38º Deliberar sobre penalidades impostas aos descumprimentos desta norma.

Art. 39º Auxiliar na melhoria contínua da segurança do serviço, de ofício ou a pedido da Unidade Gestora do Serviço.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES DO USUÁRIO DO SERVIÇO

Art. 40º Informar os dados para cadastro do acesso a VPN com precisão e veracidade, reconhecendo que a inconsistência destes poderá implicar a impossibilidade de utilizar o serviço VPN.

Art. 41º Manter o sigilo da senha de acesso que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

Art. 42º Atualizar as informações pessoais, quando necessário, sendo responsável pela omissão ou erros nas informações pessoais cadastradas.

Art. 43º Reparar quaisquer danos diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer outro usuário, ou, ainda a qualquer terceiro, inclusive em virtude do descumprimento do disposto nesta norma ou de qualquer ato praticado a partir de seu acesso ao serviço VPN.

Art. 44º Não alterar, sem prévio consentimento da Unidade Gestora do Serviço, a configuração *default* da VPN fornecida.

Art. 45º Zelar pelo fiel cumprimento desta norma, bem como dos princípios de segurança da informação.

Art. 46º Zelar pela sua credencial de acesso, utilizando as boas práticas para o uso e construção da senha.

Art. 47º Notificar a Unidade Gestora do Serviço sobre qualquer incidente envolvendo sua conta de acesso ou serviços informatizados da UFSB durante o uso do serviço da VPN.

CAPÍTULO VII
DA VIOLAÇÃO A ESTA NORMA DE USO E SANÇÕES

Art. 48º O não cumprimento das normas definidas neste documento poderá acarretar sanções administrativas aplicáveis no âmbito da UFSB, sem prejuízo de eventuais responsabilidades civis e penais, que poderão ser apuradas pelos órgãos competentes, conforme legislação vigente.

Art. 49º A depender da gravidade e das consequências do descumprimento das normas supramencionadas, poderão ser aplicadas as seguintes sanções administrativas, sem prejuízo de outras medidas previstas na legislação aplicável:

I. **Advertência**: O usuário será formalmente notificado por e-mail institucional ou telefone cadastrado, sendo alertado sobre a infração cometida e as possíveis consequências em caso de reincidência.

II. **Suspensão temporária do serviço**: O acesso ao serviço VPN poderá ser suspenso por um período de **7 a 30 dias corridos**, conforme a gravidade da infração, com notificação formal ao usuário.

III. **Suspensão por tempo indeterminado:** O acesso ao serviço VPN poderá ser suspenso por prazo indefinido, a depender da gravidade da infração, sendo garantida a possibilidade de revisão da penalidade mediante solicitação fundamentada ou avaliação administrativa. O usuário será formalmente notificado sobre a penalidade aplicada.

   a. **Encaminhamento à CPAC:** Quando a conduta do usuário configurar possível infração disciplinar, nos termos das normas institucionais, a ocorrência poderá ser analisada pela STI, unidade responsável pela gestão da VPN, que decidirá pelo encaminhamento à Comissão Permanente de Atividades Correcionais (CPAC) para apuração e eventuais providências em âmbito correcional.

Art. 50º Sempre que uma sanção administrativa for aplicada, o superior imediato do usuário será notificado formalmente sobre o ocorrido.

Art. 51º Cabe ao Comitê de Segurança da Informação da UFSB avaliar a gravidade das infrações e recomendar a aplicação das penalidades acima descritas, zelando pelo cumprimento justo e proporcional das sanções.

Art. 52º Cabe à Superintendência de Tecnologia da Informação da UFSB aplicar as penalidades definidas neste documento, conforme a recomendação do Comitê de Segurança da Informação.

Art. 53º Em casos excepcionais que demandem medidas adicionais, o Comitê de Segurança da Informação da UFSB poderá avaliar e recomendar sanções complementares, em consonância com a legislação vigente e demais normativas institucionais.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 54º 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.

Art. 55º Os serviços de VPN não elencados nesta norma serão descontinuados quando a presente norma entrar em vigor.

Itabuna, 06 de fevereiro de 2025

JOANA ANGELICA GUIMARAES DA LUZ:57521239091
Assinado de forma digital por JOANA ANGELICA GUIMARAES DA LUZ:57521239091
Dados: 2025.02.06 15:22:48 -03'00'

JOANA ANGÉLICA GUIMARÃES DA LUZ
PRESIDENTE DO COMITÊ DE GOVERNANÇA INSTITUCIONAL