MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE

DELIBERAÇÃO CGSIC/IFS Nº 15, DE 05 DE JULHO DE 2024

Aprova a Política de uso da VPN do Instituto Federal de Sergipe.

A PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, faz saber que, no uso das atribuições legais que lhe confere a Lei nº 11.892 de 29 de dezembro de 2008, em conformidade com as Portarias IFS nº 1.039 de 28/04/2014, 1.339 de 05/06/2014 e 3.795 DE 06/12/2019, e considerando a Instrução Normativa GSI nº 1 de 2/05/2020 e a 1ª Reunião Extraordinária do Comitê Gestor de Segurança da Informação em 2024, ocorrida em 04 de julho de 2024,

Resolve:

Art. 1º Aprovar a Política de Uso da VPN do Instituto Federal de Educação, Ciência e Tecnologia de Sergipe – IFS, na forma do anexo, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a elaboração de uma Política de Uso da VPN visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação listada no quadro de referência legal e de boas práticas.

Art. 2º Esta Deliberação entra em vigor no dia 1º de agosto de 2024.

Aracaju, 05 de julho de 2024.

Ruth Sales Gama de Andrade
Presidente do CGSIC/IFS

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Secção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Política de Segurança da Informação e Comunicações do IFS - POSIC	Em sua íntegra
Decreto-Lei 2.848/40 - Código Penal	Em sua íntegra
Lei nº 12.737, de 30 de novembro de 2012: Dispõe sobre a tipificação criminal de delitos informáticos	Em sua íntegra
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Em sua íntegra
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	Em sua íntegra
Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014	Em sua íntegra
Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação – Regula o acesso a informações previsto na Constituição Federal.	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013	Em sua íntegra
ABNT NBR ISO/IEC 27002:2013	Em sua íntegra
Lei nº 13.460, de 26 de junho de 2017 - Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública	Em sua íntegra

POLÍTICA DE USO DA VPN

CAPÍTULO I

DOS PRINCÍPIOS GERAIS E DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Uso da VPN está alinhada com a Política de Segurança da Informação do IFS.

Art. 2º O objetivo desta política é prover as diretrizes gerais para o uso apropriado de conexões VPN (Virtual Private Network), para acesso à rede computacional do IFS, visando o bom desempenho do serviço e a segurança da informação no que tange aos aspectos de confidencialidade e integridade.

Art. 3º Esta política se aplica a todos os servidores, terceirizados, bolsistas e alunos, na utilização da VPN e que estejam devidamente autorizados e cadastrados na base de contas de usuários no domínio do IFS.

Art. 4º A VPN (Virtual Private Network) é uma rede privada virtual que permite ao usuário, de forma segura utilizando encriptação de dados, receber um número IP da rede do IFS em seu equipamento remoto. Dessa forma, mesmo não estando nas dependências do IFS, será possível acessar os servidores e sistemas hospedados com permissão de acesso apenas local (intranet).

Art. 5º A conexão via VPN ao ambiente computacional instalado no IFS é provido pela DTI/COSEG, por meio de uma conta de usuário, com vínculo institucional atualizado.

Seção I

Das definições

Art. 6 º Para os efeitos desta política considera-se:

I. Segurança da Informação - proteção da informação de vários tipos de ameaças, visando garantir a continuidade do negócio, minimizar os riscos que possam comprometê-lo e maximizar o retorno sobre os investimentos e as oportunidades de negócio. É obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais, funções de hardware e software. Além disso, ela pode ser realizada com a implementação de controles que deverão ser monitorados, analisados e continuamente melhorados, com o intuito de atender aos objetivos do negócio, mitigando os riscos e garantindo os preceitos de segurança da organização: confidencialidade, integridade, disponibilidade e autenticidade.

II. Ameaça - todo e qualquer evento que possa explorar vulnerabilidades, geralmente é um fator externo à organização, podendo ser também a causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas, pessoas ou a própria organização. Classificam-se em:

intencionais, ação da natureza, e não intencionais. São exemplos de ameaças: erros humanos, falhas de hardware, falhas de software, ações da natureza, terrorismo, vandalismo, entre outras.

III. Vulnerabilidade - qualquer fraqueza que possa ser explorada para comprometer a segurança de sistemas ou informações, além disso, pode ser uma fragilidade de um ativo ou grupo de ativos que venha a ser explorada por uma ou mais ameaças. Comparando-as, a ameaça é o evento ou incidente, enquanto a vulnerabilidade é a fragilidade que será explorada para que a ameaça se concretize. São exemplos de vulnerabilidades: falta de treinamento de funcionários, sistema aceitar qualquer valor nos seus campos, desatualização dos servidores de banco de dados, entre outras.

IV. Riscos de segurança da informação - possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, assim prejudicando a organização.

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

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

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

VIII. 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.

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

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

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

CAPÍTULO II

DA POLÍTICA DE USO

Seção I

Das competências

Art. 7º Compete aos usuários com privilégios de acesso à rede local do IFS via VPN:

I. Garantir a veracidade e exatidão dos dados pessoais fornecidos para o cadastro.

II. Ser responsável pelo seu acesso à Internet, por qualquer instalação de software necessário ou por qualquer valor associado a isto.

III. Assegurar que somente pessoas autorizadas tenham acesso permitido às redes internas do IFS através de sua conta para utilização da VPN.

IV. 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, 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.

V. 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).

VI. 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 do IFS (POSIC).

VII. Não utilizar a VPN em redes WiFi públicas, abertas (sem criptografia) ou compartilhadas por terceiros.

VIII. Todos os computadores conectados às redes internas do IFS via VPN devem estar com as versões mais atualizadas de softwares antivírus, e com os últimos “patches” de segurança instalados.

VIII. Estabelecer somente uma única conexão VPN com a rede do IFS.

IX. 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.

X. Utilizar equipamentos com sistemas operacionais compatíveis com a infraestrutura de computação do IFS conforme Art. 6º da Instrução Normativa nº 04/2016/DTI, que dispõe sobre a Política do Catálogo Padrão de Softwares no âmbito Administrativo e Acadêmico no IFS.

XI. Aceitar que os equipamentos pessoais para acesso à VPN passem a ser uma extensão da rede do IFS e como tal, estão sujeitas às mesmas regras, políticas e regulamentações que se aplicam aos equipamentos de propriedade do IFS, ou seja, suas máquinas devem ser configuradas para atender às normas da instituição.

XII. Aceitar que o software de VPN possa fazer auditorias em suas máquinas e caso ela não esteja configurada conforme as normas da instituição o cliente de VPN não permitirá a conexão até a máquina ser devidamente retratada.

XIII. Não alterar, sem prévio consentimento, a configuração default da VPN fornecida pela COSEG.

XIV. Não utilizar programas “peer-to-peer” sobre VPN.

XV. Não utilizar o acesso VPN para transferência de grandes volumes de dados que não seja com intuito institucional.

XVI. Não utilizar quaisquer outras soluções de acesso remoto diferente da adotada oficialmente pela COSEG, tais como TeamViewer, AnyDesk, Chrome Remote Desktop e similares sem que haja a autorização expressa da área de Segurança da Informação (COSEG).

XVII. Zelar pelo fiel cumprimento desta norma, bem como dos princípios de segurança da informação;

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

XIX. Notificar a ETIR/COSEG sobre qualquer incidente envolvendo sua conta de acesso ou serviços informatizados do IFS durante o uso do serviço de VPN.

Art. 8º Compete a DTI/COSEG:

I. Liberar todo o tráfego de dados entre a estação de trabalho do usuário e a rede local do IFS numa única conexão (túnel VPN). Qualquer outro tráfego fora da VPN será descartado.

II. 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 ao bom desempenho da rede local do IFS.

III. Auditar, quando necessário e com autorização do usuário, os sistemas utilizados e a comunicação de dados para acesso, por meio de VPN a rede do IFS, a fim de verificar a aderência aos requerimentos de segurança aqui mencionados;

IV. A Coordenadoria de Segurança da Informação do IFS - COSEG poderá por motivos de segurança e/ou outros, suspender o serviço de VPN, sem aviso prévio.

V. Orientar quanto aos procedimentos de instalação e configuração das VPNs disponíveis no ambiente IFS, bem como realizar o credenciamento e descredenciamento de usuários obedecendo às regras, normas e diretrizes presentes na Política de controle de acesso do IFS;

VI. 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;

VII. Sugerir melhorias técnicas e processuais, no que se refere ao serviço de VPN, adotando, neste caso, uma postura proativa;

VIII. Não permitir dispositivos sem antivírus instalado a atualizado; e

IX. Não permitir que sistemas operacionais que não estavam homologados pelo catálogo de serviço acesse a VPN.

CAPÍTULO III

DAS CONSIDERAÇÕES FINAIS

Art. 9ª Esta política poderá ser desdobrada em outros documentos normativos específicos, que deverão preservar coerência e alinhamento com os elementos norteadores nesta estabelecidos.

Art. 10. A política será revisada anualmente, ou ainda quando uma nova tecnologia surgir, ou instruções normativas existentes sofrerem alterações ou conforme necessidade do CGSIC.

Art. 11. Os casos omissos e as situações imprevistas serão encaminhados à avaliação e decisão da autoridade máxima do IFS.

Art. 12. O não cumprimento das normas definidas nesta norma poderá acarretar sanções administrativas, civis e penais, cumulativas ou não, a depender do incidente ocasionado ou postura adotada pelo usuário, assegurado aos envolvidos o contraditório e a ampla defesa.