| | Norma de Acesso Remoto | | |
|---|---|---|---|
| | Código: POL-CRI-012 | Subarea: Seguranca | Tempo Execução: |
| | Estado: AGUARDANDO REVISAO | | Classificação: Publica |
| | Autor: ThiagoLazaroDeSouzaNogueira | | |
| | Revisor: EdmilsonNascimento1, SergioDaSilvaCarlos | | |
| | Última atualização: 30 Aug 2021 | | |

# 1 Campo de Aplicação

Esta norma se aplica a todo o ambiente cibernético da Universidade Federal da Bahia (UFBA).

# 2 Objetivo e Abrangência

Normatizar o acesso remoto dos usuários aos meios de Tecnologia da Informação e Comunicações (TIC) da Universidade Federal da Bahia.

# 3 Conceitos e Definições

3.1 **Acesso Remoto** - Qualquer acesso realizado oriundo da Internet para os serviços computacionais da UFBA, inclusive os disponibilizados de forma aberta para a Rede Mundial de Computadores.

3.2 **VPN** - Virtual Private Network ou Rede Virtual Privada. Tecnologia que permite acesso remoto seguro à rede corporativa por meio de uma credencial de acesso.

3.3 **Incidente de segurança** - é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações (POSIC).

# 4 Diretrizes

4.1 É imprescindível que todos os usuários de serviços com acesso remoto estejam conscientes dos riscos envolvidos para a instituição em decorrência de mal uso do serviço ou de suas credenciais.

4.2 Devem ser adotados controles que restrinjam o acesso de usuários não autorizados aos serviços remotos hospedados no ambiente computacional da UFBA.

4.3 O acesso remoto à Rede Corporativa deve ser exclusivamente relacionado 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.

4.4 O serviço oficial de VPN fornecido pela Superintendência de Tecnologia da Informação (STI) é o único meio autorizado e homologado para realização de acesso remoto ao ambiente de TIC da UFBA.

4.5 O uso do serviço de VPN para acesso remoto aos serviços computacionais da UFBA deve obedecer aos ditames de norma específica, sendo obrigação de todos os usuários o conhecimento desta.

4.6 Qualquer acesso remoto realizado deve ser registrado em log interno e passível de auditoria pela STI ou órgão competente, obedecendo aos limites estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e Política de Segurança da Informação e Comunicações (POSIC) desta Universidade.

4.7 Baseados em aspectos legais e técnicos, os controles adotados para proteção dos dados e serviços podem restringir acessos que possam comprometer o ambiente computacional e tragam riscos de cibersegurança para a Universidade.

4.8 É responsabilidade do usuário zelar pelas credenciais de acesso ao ambiente remoto, sendo proibido o compartilhamento dessas credenciais, sob pena de incorrer em crime de violação de sigilo funcional, tipificado no Decreto-Lei nº 2.848/40 (Código Penal).

4.9 O usuário deve utilizar e construir suas senhas conforme boas práticas determinadas na Norma de Senhas da Universidade.

4.10 É recomendável o uso de software antimalware e firewall pessoal nos dispositivos utilizados para acesso remoto, de forma a minimizar os riscos relacionados à segurança das informações.

4.11 Não é recomendado o acesso remoto ao ambiente computacional da UFBA utilizando redes wifi públicas, abertas (sem criptografia) ou compartilhadas por terceiros.

4.12 O acesso remoto a servidores Windows deve ser realizado utilizando o protocolo RDP, com controle de acesso por meio de usuário e senha. Para servidores Linux deve ser sempre utilizado protocolo SSH, com controle de acesso por meio de usuário e senha e/ou certificado digital.

4.13 O acesso remoto a ativos de rede deve ser utilizado prioritariamente o protocolo SSH. Nos casos onde não for possível o uso do protocolo SSH, pode ser utilizado, **excepcionalmente**, o protocolo Telnet para acesso remoto a esses dispositivos.

4.14 Não é permitido uso de softwares de colaboração remota em servidores da rede UFBA, como TeamViewer, AnyDesk ou qualquer outro software não homologado pela STI.

4.15 A qualidade de conexão da internet do usuário pode influenciar diretamente na qualidade dos serviços acessados remotamente, assim sendo, é responsabilidade do usuário checar com seu provedor de acesso eventuais problemas técnicos percebidos.

4.16 Qualquer incidente de segurança envolvendo o ambiente de acesso remoto deve ser remetido à Central de Serviços da STI, através dos meios oficiais de comunicação, disponíveis em https://sti.ufba.br .

# 5 Violação a esta Norma de uso e sanções

O descumprimento de diretrizes mencionadas nessa norma pode acarretar em sansões administrativas, civis e penais, cumulativas ou não, sem prejuízo das demais previsões normativas relacionadas.

# 6 Disposições Finais

N/A

# 7 Referências

Lei nº 8.112/90 - Dispõe sobre o regime jurídico dos servidores públicos civis da União;

Lei nº 13.709/18 - 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;

# 8 Controle de versão

| Rev | Data | Descrição | Itens revisados | Revisado por |
|---|---|---|---|---|
| 00 | 26/08/2021 | Criacao do Documento | -- | nogueira.thiago |
| **Rev** | **Data** | **Descrição** | **Itens revisados** | **Revisado por** |
| 01 | 30/08/2021 | Alteração do Documento | -- | nogueira.thiago |