# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POL.ADM 04 – Rev.02 ABR26



## 01. INTRODUÇÃO

A Política de Segurança da Informação e das Comunicações está baseada nas recomendações do ITIL (sigla para Information Technology Infrastructure Library), reconhecida mundialmente com um código de prática para a gestão, perfazendo um conjunto de boas práticas detalhadas para o gerenciamento de serviços de TI e da segurança da informação, tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento, controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Conselho Regional de Biomedicina -5ª Região.

O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações do Conselho Regional de Biomedicina -5ª Região.

Essa Política aplica-se a todos os membros, colaboradores e terceiros do Conselho Regional de Biomedicina – 5ª Região e demais agentes públicos ou particulares que, oficialmente, executem atividades vinculada à atuação institucional e organizacional do Conselho Regional de Biomedicina – 5ª Região.

## 02. PRINCÍPIOS

São princípios da Política de Segurança da Informação e das Comunicações:

2.1. Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
2.2. Integridade: Propriedade que estabelece que a informação esteja correta,confiável, sem a ocorrência de mudanças não autorizadas;
2.3. Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

## 03. DISPOSIÇÕES GERAIS

A área de Tecnologia da Informação e Administração é a responsável pela organização e salvaguarda

dos dados da organização que inclui Arquivos Físicos, Arquivos Sistêmicos e Banco de Dados, armazenados em equipamentos próprios e também em terceiros contratados para este fim, que compõe o panorama do Conselho Regional de Biomedicina -5ª Região.



O processo de segurança da informação deve envolver todos os colaboradores, independente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio, aplicar segurança a ele e estar em conformidade com regulatóriose a legislação atual.

## 04. O USO DE RECURSOS

O uso e o acesso pelo colaborador à rede corporativa cabeada ou WiFi, computadores, Internet, utilização de e-mail e comunicador corporativo, deverão ser exclusivos para uso profissional, para a execução e desempenho dos objetivos do Conselho Regional de Biomedicina – 5ª Região.

É proibida a saída de qualquer equipamento de propriedade do Conselho Regional de Biomedicina – 5ª Região pelo colaborador, exceto se houver autorização por expresso neste sentido, formalizadapor documento escrito e assinado pelo encarregado responsável.

A entrada e consequente uso de equipamentos de informática pessoais tais como celulares e notebooks, deverá ser comunicada ao Superior Hierárquico do Conselho Regional de Biomedicina -5ª Região, em especial se for utilizada de qualquer forma de suas redes, inclusive Internet. Em hipótese alguma, o Conselho Regional de Biomedicina -5ª Região será responsabilizado por danos no equipamento pessoal do colaborador ou ainda em casos de furto ou roubo.

O uso do e-mail corporativo não garante direito sobre este, pois se constitui de informações pertencentes ao Conselho Regional de Biomedicina -5ª Região.

O Conselho se reserva o direto de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, estejam no disco localda estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na rede local assim como os endereços web visitados e histórico de comunicadores internos, visando assegurar o cumprimento desta política.

Não é permitido o compartilhamento de arquivos estranhos às atividades do Conselho Regional de Biomedicina -5ª Região e não autorizados pelo superior hierárquico, como também a troca de arquivos de foto, vídeo ou música. Não é permitido o acesso a programas de TV na Internet ou qualquer conteúdo sob demanda (streaming), inclusive os jogos da Internet(on-line).

É proibida a transferência (download) de qualquer tipo de programa, arquivos, jogos e similares assim como a tentativa de instalação dos mesmos nas estações de trabalho sem autorização específica do superior hierárquico, exceto os estritamente relacionadosaos serviços inerentes à função do colaborador com vistas às atividades do Conselho Regional de Biomedicina -5ª Região.

Sendo do interesse do Conselho Regional de Biomedicina -5ª Região que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos, observados em todos os casos os termos desta política de uso.
O uso dos aparelhos de telefonia celular corporativo é exclusivamente destinado a contatar partes interessadas na operação e fornecedores, por sua vez, proibida a sua utilização em chamadas particulares.

## 05. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

5.1. A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Organização, com vistas à garantia de integridade,disponibilidade, conformidade e confidencialidade;
5.2. Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);
5.3. Os gerenciamentos dos ativos de informação deverão observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;
5.4. O cumprimento dessa Política, bem como das normas complementares e procedimentos de Segurança da Informação no Conselho Regional de Biomedicina -5ª Região será auditado periodicamente, de acordo com os critérios definidos pela Gerência, vinculado diretamente aos diretores do Conselho Regional de Biomedicina -5ª Região.
As medidas de proteção devem ser planejadas e os gastos na aplicação de controles deve ser compatível com valor do ativo protegido;
5.5. O acesso às informações, sistemas e instalações depende da apresentação de identificador, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;
5.6. A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos devem ser homologados e/ou autorizados pela administração;

5.7. Os requisitos de segurança da informação devem estar explicitamente citados em todos os termos de compromisso celebrados entre a empresa e terceiros;
5.8. Todos os membros, colaboradores e terceiros do Conselho Regional de Biomedicina -5ª Região e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do Conselho e sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do Conselho Regional de Biomedicina -5ª Região.

## 06. ACESSOS, LOGINS E SENHAS

Todos os computadores possuem senha de acesso individual, cumprindo os requisitos de segurança e sistema operacional atualizado periodicamente.
Todos em sistema de grupo de trabalho, com compartilhamento de impressoras.



- Os acessos externos podem ser realizados somente via VPN (OPENVPN);
- Acessos de diretórios limitados por permissões destinadas ao usuário.

## 07. BACK-UP E PLANO DE CONTINGÊNCIA

**Estratégia Geral Backup:**

O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore (Restaurar os dados, recuperar os dados salvos em backup).

1. Cabem aos administradores prever a realização de testes periódicos de restauração,no intuito de averiguar os processos de backup e estabelecer melhorias.
2. A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.
3. As Mídias (ou dispositivos de armazenamento) deverão ser armazenados em locais seguros, de difícil acesso, ou em localidade diversa da origem dos dados (backup off- site).
4. As solicitações de restauração de arquivos deverão ser abertas formalmente atravésde e-mail ou ferramenta de atendimento help-desk, que deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

**Estratégia:**
Rotinas de Backup CRBM

| SOLUÇÃO | MODO DE OPERAÇÃO | ROTINAS |
|---|---|---|
| COBIAN BACKUP | INTERNO | DIARIAMENTE/ FULL |
| AMAZON AWS | EXTERNO CLOUD | DIARIAMENTE/ FULL |

## 08. ATIVOS ORGANIZACIONAIS E DIAGRAMA DE REDE

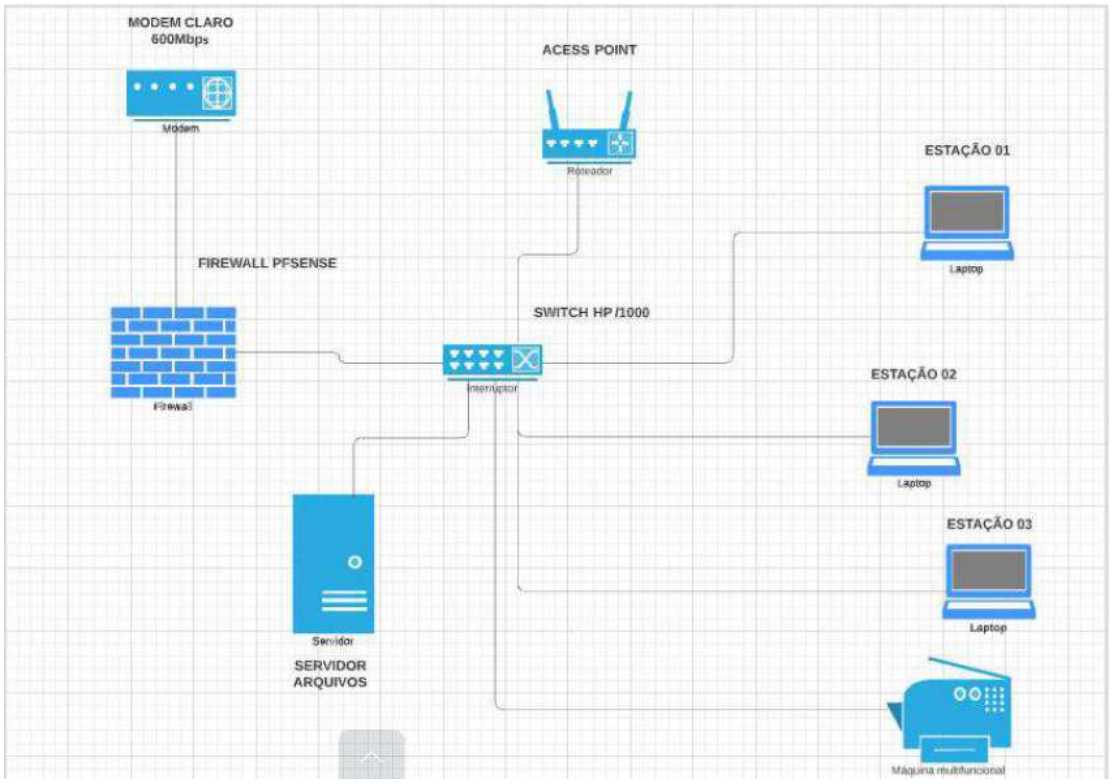



Imagem 01 - Ilustrativa

## 09. MANTEUTENÇÃO DAS INSTALAÇÕES FÍSICAS

A manutenção de equipamentos computadorizados, wi-fi – access point, rede cabeada e servidor ficam sob encargo do parceiro externo de TI - Vanti Tecnologia. Para a manutenção das impressoras, contrata-se empresas especializadas dependendo do modelo de cada impressora

## 10. FIREWALL

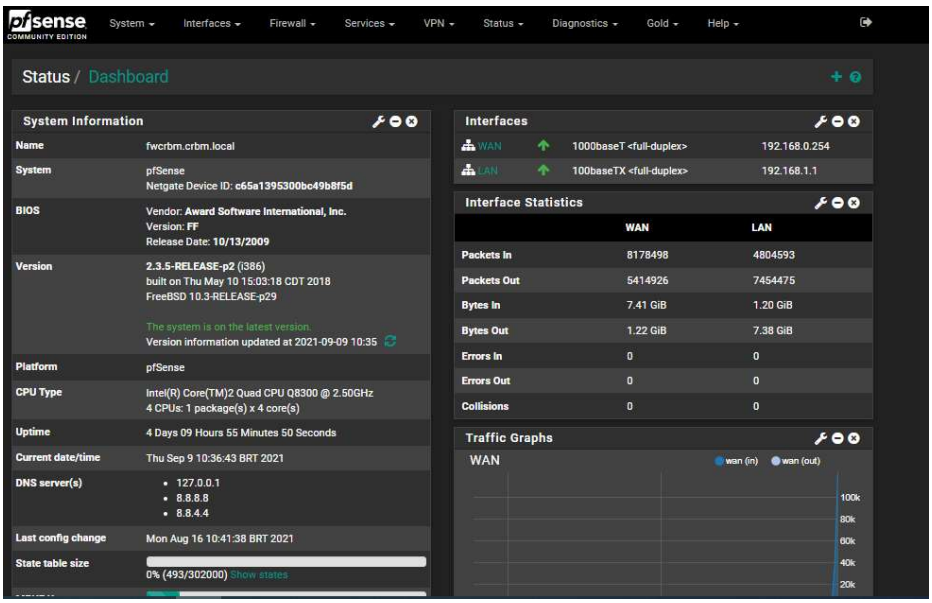
A proteção feita por meio da firewall da rede LAN e WAN, que confere maior controle dos dados e

são gerenciados pelo sistema PfSense (Imagem ilustrativa abaixo e arquivos em ANEXO).

Este servidor é responsável por garantir a segurança e o roteamento dos pacotes da rede do CRBM-5, segue abaixo outros itens gerenciados pelo PfSense:

Firewall; Servidor (internet, DHCP, NTP, Proxy…); Antivírus; Antispyware; Antispam; Filtragem de conteúdo; Detecção de intrusão, entre outros; VPN (Muito utilizado no formato home office).






## 11. ANTIVIRUS

Todos os equipamentos possuem antivírus Bitdefender internet Security, devidamente instalados e monitorados periodicamente.

## 12. CONEXÃO VPN CRBM-5 SC

A Estrutura do CRBM-5 localizada em Santa Catarina está atualmente conectada à nossa rede principal por meio de uma conexão segura OpenVPN, com o firewall Pfsense servindo como o ponto de controle e segurança. Essa configuração garante uma comunicação confiável e protegida entre as duas localidades, permitindo uma troca eficiente de dados e informações.

## 13. ASSEGURAR DISPONIBILIDADE

Contamos com um link de internet da Claro Net de 600MB como principal e a empresa BLUE3 com um IP fixo de 150 MB de backup ou redundância e não possui controles de acessos e sujeitos a regras de navegação ou bloqueio de navegação.



## 14. PROCESSO DE ATENDIMENTOS DE T.I

Este procedimento tem como objetivo registrar a abertura de chamados para suporte de Informática, de forma manual, com rastreabilidade eletrônica e utilização de uma plataforma de help-desk.

Os chamados podem ser registrados através do whatsup que suporta o grupo de funcionários do Conselho **51 98610-0800** ou pelo e-mail **https://chamados.vanti.inf.br**

## 15. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança da informação deve ser entendida como parte fundamental da cultura do crbm-5. Incidente de segurança da informação podem ser subentendidos como desídia quando não observados, indo de encontro aos valores estabelecidos pelo CRBM-5.

## 15. CONTROLE DE VERSÕES DESTE DOCUMENTO

| Revisão | Data | Itens Alterados | Elaboradores | Aprovadores |
|---|---|---|---|---|
| 00 | 26/08/2021 | Rev. 00 | Dany Silva |  |
| 01 | 12/06/2024 | Rev. 01 | Inácio Borges |  |
| 02 | 01/04/2026 | Rev.02 | Inácio Borges |  |

| Nome: | Data: | Assinatura: |
|---|---|---|