POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

MONTVERUM ASSET MANAGEMENT LTDA.

maio/2026

MONTVERUM
ASSET

SUMÁRIO

APRESENTAÇÃO **3**
OBJETIVOS **3**
ABRANGÊNCIA **3**
PROGRAMA DE SEGURANÇA DA MONTVERUM **4**
DESLIGAMENTO DE COLABORADORES **11**
MONITORAMENTO E TESTES PERIÓDICOS **11**
PROTEÇÃO DE DADOS PESSOAIS **11**
VIGÊNCIA E ATUALIZAÇÃO **14**
ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA **15**

APRESENTAÇÃO

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética ("Política") da **MONTVERUM ASSET MANAGEMENT LTDA.** ("**MONTVERUM**"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da **MONTVERUM**, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da **MONTVERUM**.

OBJETIVOS

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da **MONTVERUM**, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

A **MONTVERUM** buscou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da **MONTVERUM**, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

ABRANGÊNCIA

Este procedimento se aplica a **MONTVERUM**, em atendimento aos requisitos do sistema de gestão de Compliance.

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos Ativos disponibilizados pela **MONTVERUM** ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela **MONTVERUM**, sendo de responsabilidade individual e coletiva o seu cumprimento.

Qualquer informação sobre a **MONTVERUM**, ou de qualquer natureza relativa as atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que é de extremo valor para a **MONTVERUM**, dado o princípio fundamental de confiança que a instituição trabalha para manter junto aos seus clientes,

a **MONTVERUM** utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA (4ª Edição).

O referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a **MONTVERUM** abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de *Compliance* da **MONTVERUM**, sob a direção do Diretor de Risco e *Compliance* da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a **MONTVERUM** conta com o suporte e assessoria da empresa terceirizada de TI.

PROGRAMA DE SEGURANÇA DA MONTVERUM

i **Identificação de Riscos**:

Como se sabe, as ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

a) Malware (e.g. *ransomware, vírus, worms, trojans, spyware, adware, rootkits, screenlogger, bots*) – softwares desenvolvidos para corromper computadores e redes;

b) Engenharia social (e.g. *clickjacking; phishing, quishing, smishing, vishing, deepfake*) – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;

c) Ataques de DoS (Negação de Serviços), DDoS (Negação de ServiçoDistribuída) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da organização, no caso das *botnets*, o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços;

d) Intrusões (e.g. ataque de força bruta e MitM – *Man in the Middle*, em que um invasor se insere entre duas partes que estão se comunicando, interceptando e, potencialmente, modificando a comunicação sem que nenhuma das partes saiba) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a **MONTVERUM** pode estar sujeita a má funcionalidade dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

Para a identificação e avaliação de riscos, são realizadas as seguintes ações:

a) Identificação dos ativos relevantes da **MONTVERUM** (sejam equipamentos, sistemas processos ou dados) usados para seu correto funcionamento;
b) Avaliação das vulnerabilidades dos ativos, identificando-se possíveis ameaças e graus de exposição;

c) Mensuração de impactos, considerando aspectos financeiros, operacionais e reputacionais, bem como da probabilidade dos riscos identificados se materializarem.

ii **<u>Ações de Prevenção e Proteção</u>**

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para **MONTVERUM**, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para **MONTVERUM**, em caso de incidente de segurança.

Deste modo, a **MONTVERUM** preza pela segregação das informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) níveis diferentes, quais sejam:

a) **Nível 1**:

- Quaisquer informações e/ou dados que a **MONTVERUM** teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) **Nível 2**:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) Nível 3:

Todas as Informações Confidenciais, a saber:

- know-*how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela **MONTVERUM**;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela **MONTVERUM**; e

- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da **MONTVERUM** e/ou de seus sócios e clientes.

A partir da definição acima, a **MONTVERUM** se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na ordem de relevância dos níveis, do maior para o menor, indicados acima.

Estrutura de TI

I Propriedade dos Recursos de TI:

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da **MONTVERUM**. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da **MONTVERUM**, salvo expressa permissão do Diretor de Risco e *Compliance*.

II Disponibilização e uso:

Todos os computadores disponibilizados para os Colaboradores da **MONTVERUM** têm por objetivo o desempenho das atividades profissionais na **MONTVERUM**, não devendo ser utilizado para quaisquer outros fins.

A disponibilização e uso dos computadores da **MONTVERUM** respeitam as seguintes regras:

a. A cada novo Colaborador, o Diretor de Risco e *Compliance* autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;

b. Todos os equipamentos, *software*s e permissões acessos devem ser testados, homologados e autorizados pela área responsável;

c. O Diretor de Risco e *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;

d. Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável;

e. A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela **MONTVERUM** é sua assinatura eletrônica no servidor da **MONTVERUM**;

f. É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Diretor de Risco e *Compliance*.

g. Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Risco e *Compliance* à área responsável.

III **Softwares:**

A implantação e configuração de *softwar*es da **MONTVERUM** respeitam as seguintes regras:

- Todos os *softwar*es, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável*;*
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área responsável;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- A utilização de equipamentos pessoais por terceiros nas instalações da **MONTVERUM** e a conexão destes na rede interna à Internet requer autorização prévia da área responsável. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

IV **Responsabilidades do usuário**:

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela **MONTVERUM**.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da **MONTVERUM** em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela **MONTVERUM**.

V **Outras Proteções aos Computadores**

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);

- "Log-*off*" automático por inatividade durante o período de 24 horas;
- Bloqueio de sistemas de gerenciamento de computador à distância.

VI Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da **MONTVERUM**, este deve sempre resguardar a imagem da **MONTVERUM**, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Contenham informações que não colaborem para o alcance dos objetivos da **MONTVERUM**;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

É proibido o uso de serviços de mensagem instantânea (WhatsApp, *Skype*, etc), através dos computadores da **MONTVERUM**, exceto em eventuais situações de uso profissional.

Também se faz expressamente proibido o uso de serviços de rádio, streaming, download de vídeos, filmes e músicas, através dos computadores da **MONTVERUM**.

VII Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da **MONTVERUM**.

VIII Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

A **MONTVERUM** disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@montverum.com.br)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à **MONTVERUM**.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a **MONTVERUM**.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável.

IX Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela **MONTVERUM** mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da **MONTVERUM**.

X Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na **MONTVERUM**.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a **MONTVERUM**, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da **MONTVERUM**; e
- Sejam incoerentes com o Código de Ética Corporativa da **MONTVERUM**.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da **MONTVERUM** é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da **MONTVERUM**.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado. O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem;
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

XI Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Risco e *Compliance*.

XII Armazenamento em Nuvem (Cloud)

A **MONTVERUM** poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud*).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

DESLIGAMENTO DE COLABORADORES

No caso desligamento de Colaboradores, será realizado o imediato desligamento de todos os acessos deste Colaborador, dentre os quais acesso ao banco de dados e ao e-mail corporativo.

Da mesma maneira, caso o Colaborador seja transferido de área, este deverá ter seus acessos adequados à sua nova função, de forma a não dispor de acesso às informações incompatíveis com as atividades executadas.

MONITORAMENTO E TESTES PERIÓDICOS

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área responsável. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a **MONTVERUM** esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais.

Ademais, serão realizados Testes Periódicos de Segurança a **MONTVERUM**, sempre objetivando a preservação dos dados mantidos pela **MONTVERUM**, em especial os confidenciais.

PROTEÇÃO DE DADOS PESSOAIS

Princípios Norteadores:

A **MONTVERUM** compromete-se a observar os princípios elencados no art. 6º da LGPD:

a) - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

g) - segurança: utilização de medidas 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 difusão;

h) - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

j) – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais tem direito de solicitar à **MONTVERUM**, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) confirmação de existência de tratamento;
b) acesso aos dados;
c) correção de dados incompletos, inexatos ou desatualizado;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;
e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;
g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) revogação do consentimento, nos termos da Lei.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela **MONTVERUM** durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a **MONTVERUM** estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à **MONTVERUM**, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a **MONTVERUM** cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da **MONTVERUM** para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da LGPD.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada sempre que necessário, e sua alteração acontecerá a qualquer momento, caso seja averiguada a necessidade de atualização do seu conteúdo.

HISTÓRICO DAS ATUALIZAÇÕES DESTA POLÍTICA

Histórico das atualizações			
Data	**Versão**	**RESPONSÁVEL**	**DESCRIÇÃO DA MODIFICAÇÃO**
26/05/2026	1ª	**João Carlos Nogueira Neto** Diretor de Compliance	Versão Inicial

JOAO CARLOS NOGUEIRA NETO:26937217846

Assinado de forma digital por JOAO CARLOS NOGUEIRA NETO:26937217846
Dados: 2026.05.27 12:07:57 -03'00'

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, [NOME DO COLABORADOR], inscrito no CPF/MF sob o nº [NÚMERO DE INSCRIÇÃO], declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informações e Segurança Cibernética da **MONTVERUM**. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

São Paulo, [Data]

_____

Colaborador