



# Política de Segurança da Informação

## Sumário

1.	INTRODUÇÃO .....	3
2.	OBJETIVO .....	3
3.	APLICAÇÃO .....	3
4.	PRINCÍPIO .....	3
5.	INFORMAÇÕES.....	3
6.	PRIVACIDADE DE DADOS PESSOAIS .....	4
7.	SEGURANÇA FÍSICA.....	5
8.	SEGURANÇA LÓGICA .....	5
9.	SENHAS.....	6
10.	ESTAÇÕES DE TRABALHO .....	7
11.	DISPOSITIVOS MÓVEIS E EQUIPAMENTOS PARTICULARES .....	8
12.	E-MAIL CORPORATIVO .....	8
13.	REDE.....	9
14.	MONITORAMENTO .....	10
15.	CONTINUIDADE .....	10
16.	TREINAMENTO E SENSIBILIZAÇÃO .....	11
17.	CONSIDERAÇÕES GERAIS.....	11
18.	REFERÊNCIAS LEGAIS .....	12
19.	SOBRE O DOCUMENTO .....	12
20.	APROVAÇÕES DO DOCUMENTO .....	12
21.	GESTÃO DO DOCUMENTO .....	12

## 1. INTRODUÇÃO

Para nós, Sys Manager Informática LTDA. (“**Sys Manager**”), a informação é um elemento de suma importância e essencial para todos os processos de negócio, sendo assim, um dos ativos mais valiosos. Ciente deste, a informação deve ser protegida e cuidada, utilizando-se de regras, normas, procedimentos e políticas internas, pois, tais informações podem ser alvo de inúmeras ameaças com objetivos de explorar vulnerabilidades e causar prejuízos consideráveis e até mesmo, irreparáveis.

## 2. OBJETIVO

A presente Política de Segurança da Informação (“**Política**”, “**Documento**”, “**POL-003**”) da Sys Manager, tem por finalidade definir diretrizes estratégicas no manuseio, tratamento, controle dos dados, informações classificadas e sensíveis, e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio no âmbito do negócio da Sys Manager, com o propósito de garantir à confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade, de modo a reduzir as chances de perda de dados, fraudes ou invasões.

## 3. APLICAÇÃO

Esta Política abrange a Sys Manager e demais filiais que venham se constituir, aplicando-se, ainda, a todos(as) e quaisquer colaboradores(as) da Sys Manager, incluindo e não limitando-se a estagiários e seus Sócios (“**Colaborador(a)**”, “**Usuário(s)**”), e demais prestadores de serviços que tenham e/ou venham a ter qualquer tipo de acesso aos dados ou informações da Sys Manager, sobre pena de responsabilidade, conforme previsto na legislação brasileira.

Vale informar que a execução do teletrabalho ou home office se dará nos termos e orientações estabelecidos no decreto nº 42.462 de 30 de agosto de 2021.

## 4. PRINCÍPIO

Garantir que este Documentos seja conhecido e compreendida por todos(as), com isso, conscientizando estes sobre os possíveis riscos e responsabilidades, bem como, dar ciência sobre quais medidas devem ser adotadas, caso ocorram possíveis incidentes de segurança da informação, de forma a atingir a melhor proteção à informação.

## 5. INFORMAÇÕES

As informações inicialmente, são classificadas com base na sensibilidade e criticidade, estabelecendo assim, um grau de sigilo adequado para a devida proteção e identificação das mesmas nos seguintes níveis:

NÍVEL	TIPO	DESCRIÇÃO
1	Pública	Pode ser divulgada externamente a qualquer pessoa via site oficial da Sys Manager, campanhas externas e publicações em redes sociais e relacionados
2	Interna	Somente acessada internamente pelo nosso ambiente em nuvem, tais como, políticas, fluxos de processos e procedimentos internos, instrumentos normativos, formulários, e-mails, revisões de acessos e relacionados
3	Confidencial	Somente acessada por um grupo restrito pelo nosso ambiente em nuvem, tais como, contratos, propostas comerciais, dados técnicos de servidores em nuvem, dados pessoais de todos, processos judiciais e relacionados

**Visto isso, seguem algumas considerações:**

- Quanto ao envio de informações confidenciais, quer seja por e-mail ou outras mídias, é necessário ter certeza que o destinatário pode ter acesso às Informações;
- Os usuários de notebooks, por força da necessidade de negócio, devem evitar o armazenamento de informações confidenciais em seus discos locais e sim, estas informações devem ser armazenadas na nuvem de dados da Sys Manager, ou seja, Microsoft Sharepoint Online ou OneDrive;
- Todo e qualquer arquivo, independente da extensão, que precisar ser enviado internamente e/ou externamente, via e-mail, somente podem ser enviados através de links de compartilhamento gerados pelo Microsoft SharePoint Online ou OneDrive. Vale destacar que, para envios externos, os links deverão ter validade de visualização de 3(três) dias corridos; e
- É terminantemente proibido fazer, divulgar ou compartilhar informações, comentários, mensagens ou discussões sobre a Sys Manager e seus clientes, bem como, informações referentes a qualquer estratégia, através de redes sociais, salas de bate-papo, wikis, mundos virtuais e blogs (Mídias Sociais), a menos que expressamente autorizado pela Diretoria da Sys Manager.

## 6. PRIVACIDADE DE DADOS PESSOAIS

Possui ligação direta com a informação e classificação das mesmas, com isso, a privacidade e proteção dos dados pessoais devem ser asseguradas conforme requerido em legislação e regulamentação vigente (Lei nº 13.709, de 14.08.2018- Lei Geral de Proteção de Dados – LGPD), quando aplicável.

Visto isso, qualquer informação pessoal, mensagem eletrônica ou arquivo, só poderá ser acessada com a permissão do remetente, destinatário ou dono da mensagem ou arquivo, salvo por ordem judicial, bem como, qualquer divulgação de dados de colaboradores é determinadamente proibida, salvo em casos em que a identificação do indivíduo seja excluída.

A privacidade e proteção dos seguintes grupos de dados pessoais deve ser seguida e respeitada a todo tempo:

- CPFs;
- Histórico médico;
- Origem étnico-racial;
- Crenças religiosas ou filosóficas;
- Opiniões políticas;
- Associação a sindicatos;
- Dados biométricos usados para identificar um indivíduo;
- Dados genéricos;
- Dados de saúde; e
- Dados relacionados a preferências sexuais, vida sexual e/ou orientação sexual.

É de suma importância que até mesmo os dados pessoais básicos, devem ser protegidos e tratados com a devida atenção, sejam eles: nomes completos, endereços, datas de nascimentos, bem como dados de currículos, certificados, fotos, registros de emprego e até informações de mídias sociais.

## 7. SEGURANÇA FÍSICA

A segurança física é baseada no acesso das pessoas aos nossos ambientes que possuam equipamentos de tecnologia da informação, para assim garantir a devida proteção destes, de acessos não autorizados, limitando a circulação apenas para pessoas treinadas, capacitadas e/ou autorizadas, com o principal objetivo de mitigar e prevenir possíveis danos e interferências aos equipamentos de tecnologia da informação. Sendo assim, estes ambientes devem ser protegidos de forma a evitar acesso não autorizado.

### Visto isso, seguem algumas considerações:

- As chaves referentes, devem estar localizadas em local sem acesso público;
- Toda e qualquer pessoa que necessitar comparecer fisicamente em algum de nossos escritórios, deverá ser devidamente identificada nas áreas de recepção, incluindo e não limitando-se a recepção do predial onde nosso escritório está instalado, ou seja, qualquer pessoa não autorizada, terá sua entrada vetada, concluindo assim, que o uso de qualquer forma visível de identificação por estas pessoas, é obrigatório.
- A proteção contra ameaças externas e/ou do meio-ambiente, desde as dependências do prédio onde a Sys Manager está instalada, até a porta do escritório da mesma, bem como o monitoramento e controle do acesso físico, é de responsabilidade da administração do prédio onde a Sys Manager está instalada.
- Caso o profissional esteja no escritório da Sys Manager, no final do expediente, o último colaborador terá a responsabilidade de desligar as luzes, ar-condicionado e outros aparelhos que estiverem ligados. E o mesmo deverá se certificar que as portas estarão trancadas;
- Somente colaboradores do Departamento de T.I ou pessoas autorizadas pelo mesmo podem ter acesso ao CPD da Sys Manager;
- É dever de todos os colaboradores preservarem os bens que compõe o escritório da Sys Manager, tais como, micro-ondas, cafeteira, mesas, cadeiras etc.; e
- O escritório da Sys Manager é monitorado por câmeras de vídeo e áudio 24(vinte e quatro) horas, para assim, garantir a correta segurança dos nossos colaboradores, visitante e demais prestadores de serviços.

## 8. SEGURANÇA LÓGICA

A segurança lógica é baseada em um conjunto de recursos executados para proteger sistemas, dados, programas e ambientes tecnológicos nos geral, contra tentativas de acessos de pessoas e/ou programas desconhecidos/indevidos, permitindo assim, que o acesso virtual a estes, seja baseado nas necessidades de cada usuários, ou seja, as necessidades de permissões e/ou solicitações de acesso aos recursos de T.I da Sys Manager devem ser baseadas nas necessidades de negócio, considerando-se o perfil funcional dos usuário e somente serão consideradas as solicitações formais, abertas via [Service Desk](#).

### Visto isso, seguem algumas considerações:

- Toda e qualquer ação de criação, alteração e exclusão relacionada a qualquer usuário, somente será realizada/atendida após abertura de chamado formal, via [Service Desk](#) pelo Departamento Pessoal.

- A fim de haver um controle quanto aos privilégios de acesso dos usuários, qualquer afastamento, seja temporário ou permanente, incluindo a mudança de departamento de atuação, deverá ser informado formalmente via [Service Desk](#), pelo Departamento Pessoal, para que sejam tomadas as medidas cabíveis quanto a suspensão provisória e permissão do acesso; e
- Toda e qualquer nova aquisição relacionada a T.I, sejam elas equipamentos, serviços e/ou softwares, devem ser homologadas pelo Departamento de T.I antes de qualquer fechamento de negócio, bem como, participar, quando cabível, de reuniões e/ou tratativas relacionadas a T.I para com a aquisição desejada.
- Todas as contas de usuários e senhas, estão armazenadas em nosso Active Directory, alocado em nuvem da Microsoft Azure, bem como, todo o gerenciamento das referidas contas;
- Todo e qualquer SSD e/ou HD dos notebooks disponibilizados pela Sys Manager é protegido com criptografia, ou seja, caso o mesmo seja indevidamente removido, não é possível ter acesso aos dados do mesmo; e
- Todos e quaisquer notebooks disponibilizados pela Sys Manager possuem antivírus instalado, bloqueando acessos a sites indevidos e possíveis ameaças, sendo assim, nenhum usuário tem permissão para desativar o mesmo, pois está bloqueado por senha.

## 9. SENHAS

Em complemento da segurança lógica, a forma mais convencional de conclusão da identificação de acesso dos usuários é a senha, a mesma é uma informação pessoal e intransferível, que protege a identidade dos usuários, evitando que outras pessoas se passem por estes usuários. Ciente deste, vale destacar que, o uso de dispositivos e/ou senhas de identificação de outrem, constitui em crime, vide Código Penal Brasileiro (art. 307).

**Com o objetivo de auxiliar na criação e gestão de senhas, as regras abaixo devem ser consideradas:**

- O usuário é responsável por zelar pela confidencialidade e sigilo de suas senhas e logins, sendo assim, responsabilizados pelas operações realizadas com a utilização de suas credenciais;
- É proibida a divulgação e/ou empréstimo de qualquer senha;
- Em caso de uso indevido de qualquer senha, a mesma deve ser trocada imediatamente;
- A senha inicial/temporária é fornecida pelo Departamento de T.I via e-mail, após a criação da conta do usuário em nosso Microsoft Azure AD (Active Directory);
- É proibido o compartilhamento de toda e qualquer senha de administrador;
- Senha de comum utilização de um departamento, como por exemplo, senha para abertura ou edição de documentos específicos, deve ser criada pelo gestor do departamento, armazenada em software interno de gerenciamento e segurança de senhas e disponibilizada ao Gerente de Tecnologia da Informação;
- Nenhuma senha, em hipótese alguma, deve ser anotada e/ou deixada próximo a mesas, notebooks, computadores, teclado, monitor e demais formas relacionadas; e

- As senhas devem ser criadas possuindo, no mínimo, 8 (oito) caracteres e ao menos 1 (um) caractere de cada um dos seguintes grupos: letras maiúsculas e minúscula, números e caracteres especiais.

## 10. ESTAÇÕES DE TRABALHO

Todos os notebooks registrados como patrimônio da Sys Manager, constituem-se em estações de trabalho, desde que sejam utilizados por nossos colaboradores para o desempenho de suas atividades e somente para fins profissionais.

**Visto isso, seguem algumas considerações que devem ser adotadas quanto ao uso destas estações de trabalho:**

- É proibido modificar, instalar e/ou remover softwares e/ou hardwares sem autorização do Departamento de T.I da Sys Manager, pois, tal atitude, pode acarretar problemas de segurança, comprometendo assim, o desempenho das estações de trabalho;
- Somente devem ser utilizados softwares devidamente licenciados, com isso, vale informar que, o uso de software não licenciado e/u considerado “pirata”, constitui infração, vide Lei (nº 9.609/1998);
- Independentemente do local, ao se ausentar da estação de trabalho, efetue o bloqueio pelo seu teclado (*WinKey* + L) ou “logoff” da mesma, evitando assim, acessos indevidos através de suas credenciais;
- Os notebooks somente serão liberados após assinatura completa do formulário (FORM-003 Termo de Responsabilidade de Equipamentos);
- No momento em que o colaborador devolver o notebook para a Sys Manager, o mesmo, deverá assinar obrigatoriamente o formulário (FORM-004 Termo de Devolução de Equipamentos), e após este, todo e qualquer dado e/ou documento pessoal que possa existir no mesmo, será excluído imediatamente, ou seja, proibido salvar e/ou manter arquivos pessoais em notebooks disponibilizados pela Sys Manager.
- É aconselhável que, para evitar o acesso indevido de outras pessoas as informações de navegação, pesquisas e demais ações realizadas nas estações de trabalho, em hipótese alguma deve-se deixar salvo o login e senha nos mesmos;
- Em casos de furto/roubo/perda dos notebooks, deve-se comunicar imediatamente as autoridades policiais, registrando assim, um B.O (Boletim de Ocorrência) e após, deve ser comunicado formalmente e imediatamente ao gestor imediato, ao gestor do Departamento de T.I e ao Departamento Administrativo para avaliação da situação e adoção das medidas necessárias;
- O Usuário é responsável pela conservação, integridade, utilização e informações constantes na estação de trabalho que utiliza. Cuidados como desligar o notebook, inclusive o monitor, ao final do dia e não manter líquidos próximo aos equipamentos são fundamentais para garantir que a vida útil dos mesmos não seja reduzida;
- Não é permitido conectar qualquer tipo de Pen Drive, CD, HD, SSD e/ou SD desconhecido ou suspeito em qualquer equipamento da Sys Manager, sendo assim, ao encontrar algum dispositivo relacionado, entre em contato imediatamente com o Departamento de T.I;

- Para evitar perda de acessos em portais de fornecedores ou demais portais externos utilizados no dia a dia de trabalho, é proibido o cadastro nestes com o e-mail pessoal e/ou pessoal corporativo, ou seja, deve-se sempre, cadastrar o e-mail do departamento responsável pelo acesso direto ao portal.

## 11. DISPOSITIVOS MÓVEIS E EQUIPAMENTOS PARTICULARES

Nossos colaboradores, visitante e demais prestadores de serviços poderão utilizar dispositivos móveis e equipamentos particulares no escritório da Sys Manager, desde que tenham ciência das seguintes regras e considerações:

- Todo acesso a nossa rede interna de internet poderá ser monitorado para maior segurança de nosso ambiente;
- Temos uma rede específica para visitantes e uma para dispositivos móveis;
- Se necessário acesso a rede de internet, solicite o mesmo ao Time de Suporte presente no local, mediante a verificação de proteção apropriada para uso autorizado e seguro;
- Após acesso concedido acesso em nossa rede de internet, em hipótese alguma, podem ser executados nestes dispositivos móveis e equipamentos particulares, softwares de características maliciosas, que possam comprometer o funcionamento de nossa rede;
- É de total propriedade do proprietário, utilizar somente softwares legalizados; e
- É proibido o armazenamento de toda e qualquer informação e documentação de propriedade da Sys Manager e de seus clientes nestes dispositivos móveis e equipamentos particulares, incluindo e não limitando-se a Pen Drive, armazenamento em nuvem pessoal e semelhantes.

## 12. E-MAIL CORPORATIVO

O e-mail corporativo é restrito apenas para atividades profissionais de seus usuários, com isso, é necessária a ciência das seguintes regras e considerações:

- É proibido enviar e/ou arquivar mensagens que não estejam relacionadas a tais atividades e/ou que contenham assuntos que provoquem assédio, perturbação e/ou correlatos, bem como, temas difamatórios, discriminatórios, caluniosos, degradantes, ofensivos, violentos, ameaçadores, obscenos, pornográficos, ilegais e antiéticos, ou seja, que não tenham relação com as atividades profissionais do colaborador, por meio de arquivos, textos, fotos, imagens, sons e/ou vídeos;
- A qualquer momento que julgar necessário, o Departamento de T.I pode utilizar mecanismos para bloqueio, na entrada ou saída de mensagens, por tamanho, por anexos e download de arquivos que não sejam condizentes com as atividades da Sys Manager;
- Utilizamos mecanismos de prevenção contra perda de dados, chamado DLP (*Data Loss Prevention*), para garantir que toda e qualquer informação confidencial permaneçam com a segurança devida, mitigando assim a possível perda dos mesmos; e
- É proibida a alteração de assinatura de e-mail corporativo, somente poderá ser alterada, após aprovação do gestor imediato e mediante solicitação via sistema de chamados, pelo [Service Desk](#).

## 13. REDE

Todos e quaisquer colaboradores da Sys Manager estão autorizados e/ou poderão fazer uso dos recursos da rede corporativa da mesma, desde que estejam utilizando o domínio sysmanager.com.br, tais como:

- E-mail corporativo;
- Internet;
- Compartilhamento e armazenamento de arquivos (Microsoft Sharepoint Online);
- Estações de Trabalho;
- Softwares e sistemas da informação; e
- Serviços de impressão.

### Visto isso, seguem algumas considerações:

- Os recursos serão liberados para os colaboradores, sempre que um novo colaborador for efetivamente contratado, levando em consideração àqueles recursos que são indispensáveis para realização das atividades dos mesmos, sendo necessário login e senha para efetivação dos devidos acessos;
- Cada departamento da Sys Manager possui seu respectivo acesso restrito ao recurso de compartilhamento e armazenamento de arquivos (Microsoft Sharepoint Online), com permissões de leitura, gravação e exclusão. Ciente deste, é de total responsabilidade do gestor do departamento, os dados e informações críticas referentes ao respectivo departamento, bem como, pela correta definição atribuição de permissões neste recurso;
- Em hipótese alguma, os colaboradores poderão utilizar dos recursos supracitados para fazer download e/ou distribuição de softwares pirateados, ação que constitui em crime, vide Código Penal Brasileiro (art. 184);
- A instalação de softwares e/ou sistemas nas estações de trabalho, pelo usuário, é proibida. Este somente pode ser realizado pelo Departamento de T.I, via sistema de chamados, pelo [Service Desk](#);
- É proibido utilizar os recursos supracitados para deliberadamente propagar qualquer tipo de vírus, *worms*, spam ou programas de controle de outros computadores.
- É disponibilizado, de forma controlada, acesso a rede sem fio (Wi-fi) para todos os colaboradores e visitantes, de forma segregada para cada um destes, garantindo assim, o isolamento de ambas as redes;
- Visando a proteção das informações da Sys Manager de ataques maliciosos, o Departamento de T.I mantém ativas ferramentas de controle de tráfego da internet, filtragem de e-mails e de isolamento/restrição de acesso à suas redes internas; e
- É proibido acessar, as seguintes categorias de sites: apostas, propaganda, adultos, com material obsceno/ofensivo, atividades criminais/ilícitas, armas, violência, expressões de ódio, encontros, chat, hacking e jogos.

## 14. MONITORAMENTO

Todo o ambiente Sys Manager tem seu uso monitorado e passível de auditoria para fins de gestão de colaboradores e mitigação de falhas e riscos empresariais, incluindo e não limitando-se a todo acesso e uso das informações, notebooks, demais recursos de T.I e seus ambientes físicos e lógicos. Possibilitando assim a rápida identificação de eventos ou alertas de incidentes referentes a Segurança da Informação, validando com isso, a eficácia dos controles internos implantados

Com isso, toda sua atividade poderá ser monitorada com a finalidade de garantir que toda e qualquer disposição dissertada neste documento esteja sendo seguida de forma adequada, este monitoramento considera toda a rede corporativa da Sys Manager, incluindo e não limitando-se ao e-mail corporativo, estações de trabalho disponibilizadas pela Sys Manager, sites e etc..

Neste, vale ressaltar que, todo notebook recebido tem seu uso monitorado para fins de gestão de colaboradores, mitigação de falhas e riscos empresariais. Este monitoramento é realizado por um Software instalado no equipamento, chamado fSense, cujo os objetivos são de coletar e identificar gaps no dia-a-dia das equipes, facilitar o entendimento da gestão na qual poderá ajudar o profissional em ações corretivas para atingir as metas estabelecidas, possibilitar ter visões dos padrões de comportamento relacionados ao monitoramento de atividades relacionadas à Segurança da Informação e uso correto do ambiente computacional e com isso, complementar e aumentar a produtividade das equipes prevendo falhas antes que elas aconteçam.

Bem como, para garantir a segurança dos nossos colaboradores, visitantes e das informações confidenciais, todo o escritório da Sys Manager é monitorado por câmeras de vídeo e áudio. Tal faz-se necessário apenas para fins legítimos, incluindo prevenção de roubo, investigação de incidentes de segurança, proteção de informações confidenciais e garantia de que as políticas internas da Sys Manager estão sendo seguidas.

O uso das câmeras de vídeo e áudio é restrito apenas para pessoas autorizadas, treinadas e com permissão para acesso restrito a este tipo de informação. Em complemento, as informações coletadas por tais câmeras, são protegidas de acordo com as leis aplicáveis e relacionadas a proteção de dados, não sendo compartilhadas com terceiros sem autorização prévia.

**Obs.:** Para preservar a intimidade de nossos colaboradores, os banheiros não possuem monitoramento.

## 15. CONTINUIDADE

Toda e qualquer ação que for contra este documento, incluindo e não limitando-se a todos e quaisquer eventos sob suspeitas e/ou confirmados, que possam comprometer a integridade, confidencialidade e disponibilidade de ativos e/ou serviços de informação, são considerados incidentes de Segurança da Informação. Dentre estes, podemos citar:

- Mau funcionamento (sistemas e/ou serviços);
- Ataques (engenharia social e/ou negação de serviço);
- Acessos não autorizado;
- Envio e/ou recebimento (códigos maliciosos);
- Alterações em sistemas causando perdas (sem aprovação devida); e
- Extravio e/ou roubos (dados e/ou equipamentos com informações críticas).

Comportamentos anômalos de sistemas e/ou mau funcionamento, podem ser indicadores de um ataque de segurança e/ou violação referente a segurança atual, com isso, sempre deve-se reportar situações relacionadas imediatamente como um evento de incidente da informação, via [Service Desk](#), enviando prints, mensagens de tela e demais descrições necessárias. Visto isso, não é indicado que o colaborador tome ações sozinho, sim, que o mesmo notifique ao ponto de contato devido, tomando assim, somente ações coordenadas.

## 16. TREINAMENTO E SENSIBILIZAÇÃO

Todo e qualquer colaborador da Sys Manager deverá receber treinamento e conscientização apropriados, incluindo e não limitando-se as atualizações periódicas das políticas, normas, processos e procedimentos internos, relacionados a Segurança da Informação.

- Visto isso, é recomendado que, o treinamento e sensibilização quanto a Segurança da Informação seja realizado contemplando os seguintes aspectos:
- Comprometimento da alta gestão;
- Torna conhecida toda e qualquer informação relacionada;
- Tornar transparente a responsabilidade pessoal por seus próprios atos e omissões, incluindo e não limitando-se ao compromisso em proteger toda e qualquer informação que pertença a Sys Manager e/ou Terceiros;
- Treinamentos e sensibilização devem ser periódicos;
- Procedimentos básicos de segurança da informação (como notificar incidentes) e controles individuais básicos (segurança de senhas, controles contra códigos maliciosos, mesa limpa e tela limpa); e
- Devem ser sustentados por um programa de treinamento, educação e sensibilização de segurança da informação. Estando alinhado com as políticas, normas e procedimentos relevantes à segurança da informação da Sys Manager, sempre levando em consideração, as informações da mesma a serem protegidas e controles que devem ser implementados para proteger a informação.

## 17. CONSIDERAÇÕES GERAIS

- Esta política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto;
- Esta política é revisada com periodicidade anual ou conforme o entendimento da Alta Gestão da Sys Manager;
- O objetivo é garantir aos integrantes da Sys Manager, bem como sua administração e recursos e dados armazenados no servidor de maneira segura. Para tal, medidas adequadas deverão ser tomadas respeitando os princípios de confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos; e
- Todas as pessoas que estiverem autorizadas a utilizar informações e sistema Sys Manager fora de suas dependências físicas, deverão obedecer às mesmas diretrizes estabelecidas para os equipamentos instalados internamente.

## 18. REFERÊNCIAS LEGAIS

Lei nº 13.709, de 14.08.2018- Lei Geral de Proteção de Dados – LGPD;  
 Lei Federal nº 12.965, de 23.04.2014 - Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;  
 ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Sistema de Gestão de Segurança da Informação (SGSI);  
 ABNT NBR ISO/IEC 27002:2013 - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

## 19. SOBRE O DOCUMENTO

Código	Descrição	Versão	Emissão	Classificação
POL-003	Política de Segurança da Informação	1-2023	08/03/2023	Uso Interno

<b>Criador por:</b>	Departamento de Governança de T.I
---------------------	-----------------------------------

## 20. APROVAÇÕES DO DOCUMENTO

	Nome	Cargo/Departamento
<b>Emissor (es)</b>	Wellysson Macena	Governança de T.I
<b>Revisor (es)</b>	Leonardo Maximiano	Gerente de T.I
<b>Aprovador (es)</b>	Marcos Andersen	CTO
	Germano Fortuna	CEO

## 21. GESTÃO DO DOCUMENTO

Revisão	Data	Descrição	Por
vs1	08/03/2023	Criação	Departamento de Governança de T.I
vs1	05/04/2023	Entrada em Vigor	Departamento de Governança de T.I