# Sistema de Gestão de Segurança da Informação (SGSI)

Este documento visa estabelecer e difundir as Diretrizes da Política de segurança da Informação no âmbito da Jusimed, visando a orientação quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1 Objetivo

Estabelecer as diretrizes de segurança da informação, visando os princípios básicos da Confidencialidade, Integridade, Disponibilidade e Legalidade das informações.

Descrever as regras comportamentais e diretrizes a serem seguidas para prevenir incidentes de segurança da informação e proteção de dados pessoais.

O Manual de Integridade e o Código de Conduta possuem objetivos específicos, mas que reforçam o compromisso da Jusimed com a segurança da informação.

## 2 Escopo

A presente política se aplica a todos os membros da diretoria, colaboradores, estagiários, terceiros, clientes e parceiros comerciais em quaisquer dependências da Jusimed, ou locais onde estes se façam presentes, por meio da utilização, do manuseio ou do processamento eletrônico das informações.

Esta Política estabelece diretrizes para garantir que todos tenham a mesma informação e cumpram as leis de proteção de dados pessoais, visando a segurança da informação.

## 3 Definições

AMEAÇA: causa potencial de um incidente indesejado, que pode resultar em um dano para um sistema ou organização.

ATIVOS DE INFORMAÇÃO: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também as pessoas que a eles têm acesso.

CONFIDENCIALIDADE: Consiste na propriedade da informação que determina que esta não esteja disponível ou não seja exposta a indivíduos, entidades e/ou processos que não tenham sido previamente autorizados pelo proprietário.

CONFORMIDADE: processo que visa verificar o cumprimento das normas estabelecidas.

CONTROLE DE ACESSO: conjuntos de procedimentos com a finalidade de conceder ou bloquear acesso.

CRIPTOGRAFIA: método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.

DISPONIBILIDADE: propriedade da informação que garante que a informação esteja acessível e utilizável, para uso legítimo sempre que requerido.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira mão autorizada ou acidental.

SEGURANÇA DA INFORMAÇÃO: processo de proteção de dados digitais.

VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

# 4 Princípios

Estabelecer o compromisso da Jusimed em resguardar e proteger as informações que estão sob sua guarda dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.

Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da Jusimed no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e ético.

Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

# 5 Diretrizes Gerais

A Jusimed preza pela segurança da informação e as considera com bens importantes. Portanto cabe a cada usuário vinculado à Jusimed zelar e proteger as informações criadas, manuseadas, tramitadas e guardadas no exercício de suas atividades objetivando esclarecer uma comunicação eficiente e esclarecedora com os diversos públicos. A segurança da informação deve fazer parte da rotina diária dos usuários buscando garantir a disponibilidade, confidencialidade e integridade.

Qualquer violação da Política de Segurança da Informação deve ser relatada à gerencia e diretoria para que ações urgentes sejam tomadas na preservação dos aspectos de Segurança da Informação.

Os acessos aos ambientes tecnológicos devem ser realizados através de autenticação (login e senha, digital, etc.) e de acordo com o perfil funcional do colaborador, sendo a autenticação pessoal e intransferível. É de responsabilidade do colaborador qualquer eventual irregularidade encontrada no seu acesso. O gestor da área deve analisar e classificar as informações sob sua competência, conforme grau de importância em relação ao impacto de sua divulgação.

Todos os equipamentos disponibilizados pela Jusimed às respectivas áreas devem ser utilizados no exercício das atividades de trabalho. O uso de redes externas de comunicação (*Internet,* redes privadas, etc.) são controlados através de Servidores de *Firewalls*, Servidores de Acesso à *Internet*, Servidores de *AntiSpam*,

ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, minimizando os riscos para o ambiente operacional.

Como forma de garantir e preservar a segurança da informação, o ambiente tecnológico será auditado periodicamente. A Política de Segurança da Informação deverá ser revisada anualmente, ou em prazo inferior, em função de mudanças legais/regulatórias ou se a Jusimed entender necessário, a fim de incorporar medidas relacionadas a atividades e procedimentos novos ou anteriormente não abordados.

O não cumprimento do estabelecido na Política de Segurança da Informação da Jusimed poderá acarretar sanções administrativas disciplinares e/ou contratuais.

O cumprimento da Política de Segurança da Informação deverá ser prioridade constante de todos os colaboradores, de modo a reduzir os riscos de falhas, danos e prejuízos que possam comprometer a imagem e as atividades da Jusimed, bem como os interesses e a segurança de seus clientes.

Ficam estabelecidas as seguintes diretrizes gerais:

Tratamento das informações

a) Os ativos de informação da instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.

Tratamento de incidentes de redes

a) Os incidentes de segurança da informação devem ser registrados e gerenciados.

b) Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pela Jusimed, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais na empresa.

Gestão de risco

a) Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pela Jusimed, para a identificação e implementação das medidas de proteção necessárias para a mitigação ou eliminação dos riscos.

Gestão de continuidade

a) Deve ser adotada a gestão de continuidade de negócios em segurança da informação, segundo critérios a serem definidos pela Jusimed, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, através de ações de prevenção, resposta e recuperação dos ativos que sustentam os processos críticos da Instituição.

Auditoria e Conformidade

a) Deve-se manter a conformidade com as legislações vigentes.

Controles de acesso

a) Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso.

b) Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação. Segurança de recursos humanos

c) Todo colaborador deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades.

Segurança física e do ambiente

a) Todo ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade. Gerenciamento de operações e comunicações

b) Deve-se garantir a operação segura e correta dos recursos de processamento da informação. Aquisição, desenvolvimento e manutenção de sistemas

c) Todos os sistemas de informação adquiridos ou desenvolvidos para uso da Jusimed devem ter sua continuidade garantida, independentemente de eventuais mudanças na relação Jusimed – fornecedor.

# 6 Referências Legais e Normativas

Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos

ABNT NBR ISO/IEC 27005:2019 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação



# 7 Gestão de Segurança da Informação

Todos os Colaboradores deverão:

a) Cumprir fielmente a Política de Segurança da Informação;

b) Buscar orientação do comitê de *Compliance* em caso de dúvidas relacionadas à segurança da informação;

c) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

d) Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades condizentes com a atividade desenvolvida pela Jusimed;

e) Cumprir as leis e normas sobre propriedade intelectual no que se refere às informações de propriedade ou controladas pela Jusimed;

f) Comunicar imediatamente ao comitê de *Compliance* qualquer descumprimento ou violação da Política de Segurança da Informação.

Ademais, os colaboradores deverão adotar a todo tempo comportamento seguro e consistente com o objetivo de proteção das informações da Jusimed, com destaque para as seguintes práticas a serem adotadas:

a) Os colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das informações;

b) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);

c) A senha do colaborador é pessoal e intransferível, não podendo ser compartilhada, divulgada a outros Colaboradores ou a terceiros, anotada em papel ou em sistema visível ou de acesso não protegido;

d) Somente softwares permitidos pela Jusimed podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática contratada pela Jusimed;

e) Arquivos eletrônicos de origem desconhecida não devem ser abertos ou executados nas estações de trabalho;

f) Mensagens eletrônicas e seus anexos que contenham Informações confidenciais não poderão ser parcial ou totalmente reproduzidos sem o consentimento do autor, sendo vedada qualquer divulgação ou uso não autorizado de mensagens eletrônicas ou de seus anexos;

g) Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.

# 8 Diretrizes

## 8.1 Utilização da Informação

A Jusimed monitora as informações corporativas, podendo estender ao recebimento, envio e armazenamento, utilização e manuseio, sem prévia notificação às áreas ou aos colaboradores, visando garantir e proteger o sigilo e a segurança das mesmas.

A utilização para outros fins e/ou divulgação de assuntos relacionados especialmente, mas não se limitando, a aspectos operacionais, comerciais, sobre pacientes, sobre colaboradores, jurídicos, financeiros, contábeis, tecnológicos ou qualquer outro que se relacione às atividades da empresa obriga o colaborador a obter a autorização formal da Jusimed. O conteúdo dos prontuários do paciente é amparado pelo sigilo profissional, conforme destacado na Constituição Federal e nos Conselhos de Classe dos profissionais da Saúde. O acesso às informações de pacientes é restrito aos profissionais envolvidos diretamente no atendimento ao cliente, não devendo ser compartilhadas com terceiros por nenhum meio. O sigilo das informações é responsabilidade de todos os colaboradores da Jusimed. É proibida a utilização não autorizada de informações da Jusimed, de

pacientes ou comentários pessoais que afetem a imagem da instituição em mecanismos de comunicação instantânea, bem como em e-mails, redes sociais ou quaisquer outros meios.

Todos os colaboradores que tenham acesso a informações da Jusimed ou sob a guarda da Jusimed – privilegiadas, pessoais ou sensíveis ou não – não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas. As restrições incluem a utilização de dados em palestras, apresentações, treinamentos ou qualquer ato de divulgação para o público externo sem aprovação prévia da liderança responsável.

As informações devem ser classificadas como públicas, restritas ou confidenciais, seguindo os critérios estabelecidos, a ausência de classificação formal ocasiona a classificação automática de “Restrita”, devendo ser manuseadas e protegidas com cuidado compatível com sua classificação, não sendo deixadas expostas ou desprotegidas. O armazenamento das informações é realizado por tempo determinado pela Jusimed e/ou legislação vigente.

## 8.2 Gestão de Senhas

A senha certifica que o usuário é quem diz ser e que tem o direito de acesso ao recurso disponibilizado. O uso de senha forte minimiza os riscos e inibe uma ação mal-intencionada; uma senha fraca, por sua vez, pode comprometer todo o ambiente tecnológico.

Para garantirmos que as senhas de acesso sejam fortes a Jusimed recomenda o tamanho mínimo 8 caracteres;

I. Conter pelo menos uma letra maiúscula
II. Conter pelo menos uma letra minúscula;
III. Conter números (0 a 9);
IV. Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ;

A senha deverá ser alterada a cada 90 dias. Um lembrete será enviado 5 dias antes.

A senha deve ser individual, intransferível e mantida em segredo, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso.

Em caso de desligamento do colaborador, o TI deverá ser comunicado para que a conta seja inativada de forma imediata.

## 8.3 Controle de Acesso

Os colaboradores da Jusimed possuem um login único e intransferível e recebem liberações e acessos a rede e ao sistema de acordo com seus cargos e funções.

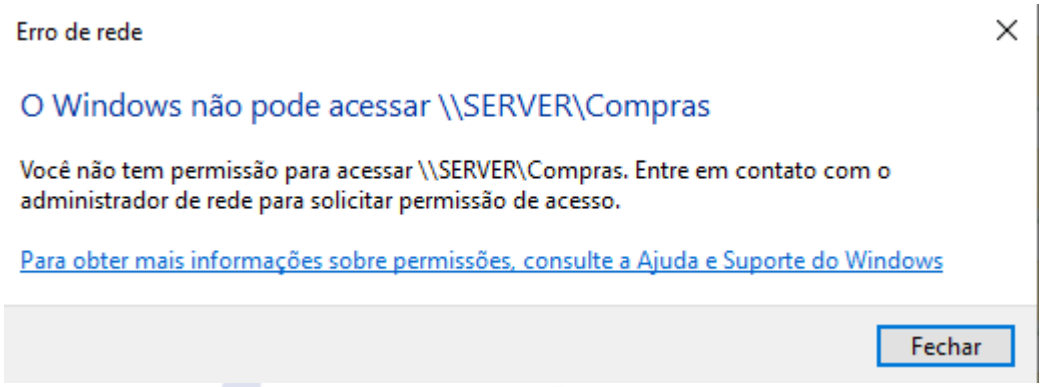
Caso haja a necessidade de alteração de acesso, o colaborador deverá enviar um e-mail para o gestor. Este analisará a necessidade e em caso afirmativo, o administrador fará a alteração do acesso do colaborador.

A revisão dos acessos ao sistema será feita anualmente pelo gestor. O sistema permite gerar um relatório dos programas que o usuário tem acesso, bem como se vem sendo acessado, permitindo avaliar a necessidade de manter os programas liberados.

O acesso de usuários desligados da Jusimed deve ser revogado imediatamente no momento da comunicação do desligamento realizado pelo departamento de RH.

Em caso de troca de função, o gestor deverá informar ao responsável do TI para informar os acessos que o colaborador poderá utilizar.

Ex:




## 8.4 Acesso Externo

O acesso externo será liberado somente em caso de urgência.

O colaborador deverá enviar um e-mail para a alta direção solicitando o notebook da Jusimed justificando a necessidade e o período que ficará de posse do mesmo.

O colaborador poderá acessar o sistema e a rede de acordo com as liberações do seu login.

A fim de minimizarmos os riscos associados a perda de confidencialidade e integridade das informações, não serão permitidos copiar, extrair ou inserir arquivos através de dispositivos móveis. Para isso, os acessos às “portas” serão bloqueados para atender as exigências do SGSI.

Não serão permitidos a instalação de software e/ou aplicativos e acesos a sites.

O notebook possui proteção antivírus/ antimalware e o firewall permitirá apenas que usuários e aplicações autorizadas possam se comunicar entre si.

Após a utilização, o suporte de TI fará uma inspeção na máquina para garantir que esteja seguro para uma próxima utilização.

## 8.5 Uso da Internet

Todos os equipamentos da Jusimed são controlados através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, minimizando os riscos para o ambiente operacional.

A Jusimed mantém regras de utilização e bloqueio de acesso a determinados sites, aplicativos, conteúdos que não sejam relacionados ao desenvolvimento de suas atividades, processos, pesquisas e competências. A empresa reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. E os ajustes em relação às liberações de acesso serão permitidas desde que justificáveis.

Não é autorizado a divulgação de mensagens de conteúdo ilegal, com qualquer sentido discriminatório, ideológico ou em desacordo com os princípios éticos e morais da Jusimed.

Não é permitido o acesso a programas na Internet ou qualquer conteúdo sob demanda (streaming). É proibido o uso de jogos, inclusive os da Internet (on-line). É proibido downloads de arquivos que não estejam relacionados ao trabalho.

O uso do e-mail corporativo não garante direito sobre este, pois se constitui de informações pertencentes à empresa.

O colaborador que divulgar informações confidenciais da empresa, poderá sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade criminal ou civil.

A entrada e consequente uso de equipamentos de informática pessoais tais como tablets e notebooks, deverá ser comunicada ao gestor imediato, em especial se for de qualquer forma utilizada qualquer de suas redes, inclusive Internet. Em hipótese alguma a Jusimed será responsabilizada por danos no equipamento pessoal do colaborador ou ainda em casos de furto ou roubo.



## 8.6 Segurança da informação

Os colaboradores têm o dever de assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos não sejam deixados desprotegidos em locais de trabalho pessoais ou públicos quando não estão em uso, mesmo que seja por um curto período de tempo ou ao final do dia.

Além da proteção contra acesso não autorizado, as informações devem ser protegidas contra desastres tais como incêndios, terremotos, inundações ou explosões.

No acesso à informação, somente devem ser usados recursos tecnológicos devidamente homologados e autorizados.

As informações com classificação “Restrita” ou “Confidencial” deverão ser descartadas utilizando métodos que impeçam a reconstrução, tal como a utilização de fragmentadoras.

Os colaboradores devem zelar pela guarda e integridade das informações nos ambientes onde atuam, protegendo os locais onde existem armazenamento de informações, sejam físicos ou eletrônicos, por meio da guarda ou proteção por senha, além da racionalização de recursos que realizam cópia de documentos.

A informação exposta de forma inadequada ou sem o zelo requerido pode ser o suficiente para pessoas mal-intencionadas descobrirem aspectos corporativos ou pessoais, fazendo uso indevido de tais informações.

As informações visuais em ambientes de reuniões requerem o mesmo grau de segurança, sigilo e zelo para não visualização por pessoas não autorizadas. O colaborador deve descartar apropriadamente tais informações, de acordo com a sensibilidade da informação. A falta de cuidado com uma área de trabalho pode levar ao comprometimento de informações pessoais e organizacionais.

## 8.7 Gestão de Ativos

Os ativos de informação considerados são: as informações, os equipamentos (hardwares) e sistemas (softwares) e os usuários que fazem o uso desse conjunto.

a) Informação: A informação pode ser armazenada em meio eletrônico ou meio físico como: documentos, relatórios, arquivos de configuração e planilhas de funcionários; Exemplo: Dados sigilosos de clientes.

b) Hardware: Envolve toda infraestrutura tecnológica de uma organização, oferecendo todo o suporte em armazenamento, processamento, nas transações e uso das informações. Como exemplo: Os computadores portáteis, os servidores e as mídias de armazenamento;

c) Software: São programas de computadores que utilizados executam armazenamento, processamento, acesso e leitura. Exemplo: sistemas operacionais e aplicativos;

d) Usuários: São todos aqueles funcionários, técnicos, operadores, administradores ou da alta direção que estão inseridos nos processos da organização.

Todos os equipamentos são controlados através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, minimizando os riscos para o ambiente operacional.

Os ativos de informação deverão ser inventariados e protegidos anualmente ou sempre que se fizer necessário, sendo de responsabilidade do técnico de TI. Neste contexto serão mapeadas as suas ameaças e vulnerabilidades.

Cada ativo de informação possui um responsável (custodiante) e um proprietário. O proprietário do ativo de informação deve criar e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Serão passiveis de monitoramento e auditorias e terão seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos.

Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

O uso dos ativos para fins pessoais é permitido desde que não prejudique os interesses da Jusimed e não atrapalhe a rotina de trabalho.

A classificação da informação deve orientar os usuários quanto ao tratamento da informação durante seu ciclo de vida, independentemente da forma de armazenamento, principalmente quanto ao uso de controles como criptografia ou descarte seguro de mídias.

## 8.8 Dispositivos Móveis e Mídias de Armazenamento

Os dispositivos móveis fornecidos pela Jusimed possuem antivírus instalados e o colaborador não tem permissão para instalar aplicativos ou alterar configurações de segurança. Sempre que possível, deve-se evitar o uso de redes públicas. Recomenda-se manter as conexões de comunicação, como bluetooth e infravermelho desabilitadas e somente habilitar quando for necessário.

O dispositivo móvel particular não tem permissão para acessar a rede.

Visitantes que necessitarem conectar seus dispositivos móveis à internet, usarão a rede “VISITANTES”.

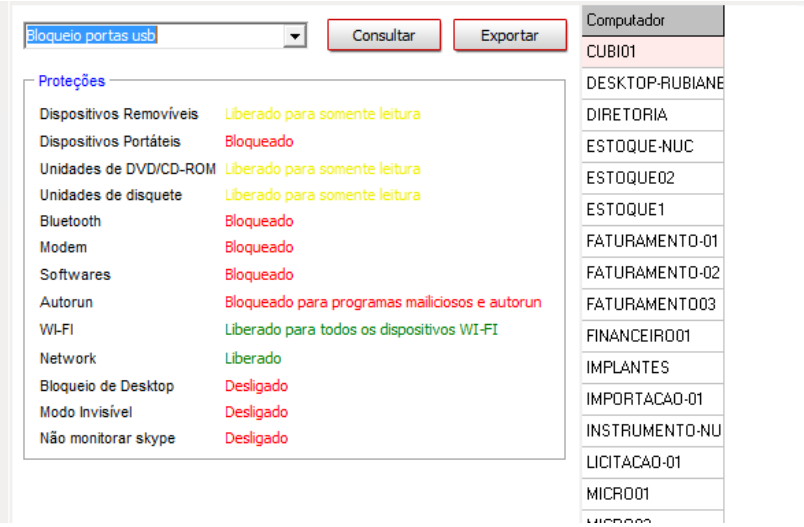
É proibida a utilização de dispositivos móveis removíveis, como pen drive e HD Externo, para armazenar ou copiar qualquer tipo de informação que possa gerar perda de confidencialidade e integridade.

É proibido fotografar, trafegar e difundir informações provenientes da Jusimed.

As senhas serão alteradas a cada três meses.

Periodicamente será realizada uma auditoria para a verificação do tipo de tráfego realizado nos dispositivos móveis corporativos.

Caso o colaborador tente fazer uso das mídias de armazenamento nas portas USB receberá a mensagem de bloqueio ou dispositivo utilizado somente para leitura.



## 8.9 Backup

A importância dos backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de backup, e por isso o armazenamento nesses locais é de total responsabilidade do usuário.

O backup dos servidores de aplicações e bancos de dados ocorre diariamente por volta das 6h da manhã (horário de Brasília, GMT-3) e são retidos durante 7 (sete) dias.

Todos os e-mails, anexos e arquivos armazenados no diretório possuem um serviço de backup a parte. O serviço monitora o volume de alterações nestes documentos e cria versões automaticamente, podendo gerar até 6 (seis) backups por dia. Todas as versões geradas permanecem armazenadas enquanto o serviço estiver contratado, por prazo indefinido.

## 8.10 Descarte de Mídia

O descarte de mídia não é descarte de informação, pois esta é objeto de legislação especifica. Informação somente pode ser descartada depois de devido processo e autorização. Mídias somente podem ser descartadas se a informação armazenada puder ser descartada ou tiver sido preservada em outro meio.

Em mídias magnéticas ainda em funcionamento, deve ser usado um software especifico (formatação não é suficiente!) para apagar fisicamente todo o conteúdo do disco rígido, antes da eliminação. No caso do equipamento não estar funcional, a unidade deve ser retirada para ser limpa em outro equipamento compatível com uso de software especifico. Se a unidade não estiver funcional ela deve ser destruída mecanicamente.

Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte e/ou remanejamento/ reutilização interna, para assegurar que todos os dados sigilosos e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem ser descartados através da destruição física ou sobrescritos de forma segura

Documentos impressos que contenham informações pessoais, financeiras ou outros dados importantes para a empresa serão picotados.

## 8.11 Criptografia

São utilizados controles criptográficos para proteger as informações da Jusimed. Somente algoritmos de criptografia aprovados pela área de TI podem ser utilizados.

O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave. As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização. Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada. Mecanismos de autenticação são estabelecidos para garantir a segurança do acesso às chaves.

## 8.12 Controle do Ambiente Físico

A Jusimed utiliza o controle físico e controles lógicos.

O controle físico é a implementação de medidas de segurança em uma estrutura definida usada para deter ou evitar acesso não autorizado a material delicado. A empresa conta com câmeras de vigilância e portas trancadas com senhas para abertura.

Os controles lógicos usam software e dados para monitorar e controlar o acesso a informações e sistemas de computação. Na Jusimed são utilizados os controles de acesso (senha) e criptografia (mecanismo para tornar alguma informação ilegível a outra pessoa ou outro sistema).

Para um controle eficiente a Jusimed faz o controle lógico com físico, através dos backups periódicos.

## 8.13 Auditoria e Conformidade

O cumprimento desta política de segurança deverá ser avaliado periodicamente por meio de verificações de conformidade, que inclusive poderão ser feitas com o apoio de entidades externas e independentes. Devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades, de forma a obter o absoluto cumprimento destes instrumentos legais e normativos. O processo de auditoria deve identificar todos os controles que governam o sistema de informação e avalia sua efetividade. Para cumprir este objetivo o processo de auditoria deve compreender por completo as operações, instalações físicas, telecomunicações, sistemas de controle, objetivos de segurança de dados, estrutura organizacional, pessoal, procedimentos e manuais da organização. As auditorias devem rever tecnologias, procedimentos, documentos, treinamento e recursos humanos.

## 8.14 Respostas a Incidentes de Segurança

A área de Segurança da Informação, representado pelo responsável da TI, em conjunto com a área de *Compliance*, são responsáveis por manter procedimentos para os processos de Gerenciamento de Incidente e de Resposta a Incidente de Segurança.

Os gestores devem assegurar que todos os sistemas de informação que armazenam informações custodiadas (confidenciais) pela Jusimed usam trilhas de auditoria para registrar e reportar:

- Todas as tentativas de violação da segurança do sistema.
- Todos os eventos significativos relacionados à administração do sistema bem como a segurança das transações e informações custodiadas (confidenciais) pela Jusimed.
- O nível de detalhe das trilhas de auditoria deve ser compatível com o nível de risco do processo associado.

Os incidentes relacionados a riscos à segurança poderão ser denunciados através do *Compliance* (pelo formulário de contato no site da empresa), de forma confidencial ou informando nome e e-mail. Todos os incidentes relatados terão sua causa investigada.

O responsável pela TI deverá relatar qualquer violação às disposições estabelecidas na presente Política.
As violações devidamente apuradas, poderão implicar:

- Na aplicação das sanções previstas na legislação trabalhista;
- Na aplicação das sanções previstas na LGPD;
- Na aplicação das sanções previstas em contrato aos prestadores de serviço;
- Na aplicação dos procedimentos legais cabíveis.

O setor de Compliance junto com o setor de TI devem avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis. Deverão comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares, através de formulário próprio constante do site da Autoridade Nacional de Proteção de Dados e deverão elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas.

O prazo máximo para a comunicação é de 48 horas contados da ciência do incidente (mesmo que ainda não esteja confirmado).

Os gestores devem assegurar que as trilhas de auditoria sejam revisadas periodicamente de forma compatível com o nível de risco do processo associado. O processo de revisão deve ser segregado para assegurar que os revisores não revisem sua própria atividade.

Qualquer atividade suspeita deve ser imediatamente verificada e tomadas as ações corretivas necessárias.

O responsável pela TI deverá relatar qualquer violação às disposições estabelecidas na presente Política.

As violações devidamente apuradas, poderão implicar:

- Na aplicação das sanções previstas na legislação trabalhista;
- Na aplicação das sanções previstas na LGPD;
- Na aplicação das sanções previstas em contrato aos prestadores de serviço e estagiários;
- Na aplicação dos procedimentos legais cabíveis.

### 8.15 Treinamento e Conscientização de Segurança da Informação

Cada gestor deve garantir que todos da Jusimed e os fornecedores, ao iniciar a relação com a Jusimed ou quando tiverem alteração significativa na responsabilidade do trabalho, recebam treinamento sobre aspectos de segurança da informação relacionados a sua função. Os gestores devem assegurar que todos os colaboradores da Jusimed e de fornecedores recebam anualmente material de conscientização aprovado pela Jusimed.

## 9 Considerações Finais

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar o setor de *Compliance*. O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável. Este documento é de uso interno, porém, em alguns casos pode ser disponibilizado a terceiro mediante prévio consentimento do setor de *Compliance*, sendo certo que o respectivo envio deve ser realizado exclusivamente em meio físico ou em formato “pdf”, (documento protegido), contendo as diretrizes de confidencialidade.

# ANEXO 1

# TERMO DE CIÊNCIA E RESPONSABILIDADE

Pelo presente instrumento, eu _____, inscrito no C.P.F. sob o n.º_____, e funcionário (a)/ prestador de serviços da empresa Jusimed Importação e Comércio de Produtos Médicos Ltda, declaro ter ciência da Política de Segurança da Informação da Jusimed, bem como suas normas complementares, comprometendo-me a cumprir o disposto no citado.

Assumo a responsabilidade por: I) tratar o(s) ativo(s) de informação como patrimônio da Jusimed; II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da empresa.

Nestes termos,

Curitiba, ____/ _____/ _____

_____
Assinatura e setor

_____
Assinatura e Nome da autoridade responsável pela autorização do acesso