



# **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

## **REVISÃO 02**



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 2 de 21
Título: Política de Segurança da Informação	

## SUMÁRIO

1.	Contextualização.....	3
2.	Objetivo .....	3
3.	Áreas de relacionamento (destinatários).....	3
4.	Documentos de referência.....	3
5.	Autoridade e responsabilidades .....	4
6.	Princípios de segurança da informação.....	4
7.	Política de segurança da informação.....	5
8.	Obrigações gerais.....	6
9.	Propriedade intelectual .....	8
10.	Política de uso .....	8
11.	Dados dos colaboradores. Aparelhos dos colaboradores. ....	8
12.	Programas ilegais .....	9
13.	Permissões e senhas .....	10
14.	Estações de computador de trabalho dos colaboradores.....	10
15.	Monitoramento de e-mails.....	10
16.	Compartilhamento de dados .....	11
17.	Mesa e tela limpa .....	11
18.	Acesso à internet.....	12
19.	Comportamento corporativo em mídias e redes sociais .....	13
20.	Backup, segurança e confiabilidade.....	14
21.	Admissão, afastamento e demissão de colaborador .....	15
22.	Promoção e transferência de colaborador .....	16
23.	Penalidades .....	16
24.	Informação e comunicação.....	16
25.	Termo e definições .....	17
26.	A empresa e a política de segurança.....	18
27.	Situações não contempladas .....	18
28.	Vigência.....	19
29.	Histórico de revisão.....	19
30.	Aprovação e classificação da informação.....	19



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 3 de 21
Título: Política de Segurança da Informação	

## 1. CONTEXTUALIZAÇÃO

A DMS LOGISTICS é uma empresa provedora dos mais modernos processos no segmento de logística global, possibilitados pelo aperfeiçoamento contínuo de seus serviços tecnológicos junto às filiais e parceiros distribuídos pelos cinco continentes do mundo.

A política de segurança da informação visa a redução desse risco, protegendo a DMS LOGISTICS das ameaças e vulnerabilidades, e do impacto aos seus ativos, que podem comprometer a confidencialidade, integridade e disponibilidade da informação.

## 2. OBJETIVO

A DMS LOGISTICS tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação e promover a melhoria contínua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com os ambientes web e clouds. Assim, assegurar a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos interesses da DMS LOGISTICS e de suas partes interessadas.

A critério único da DMS LOGISTICS, esta política de segurança da informação e cibernética poderá ser avaliada e revista regularmente ou no caso de ocorrência de circunstâncias e eventos que justifiquem ou requeiram essa avaliação e revisão, de forma a garantir sua permanente atualização, adequação, efetividade e proteção dos ativos da DMS LOGISTICS.

## 3. ÁREAS DE RELACIONAMENTO (DESTINATÁRIOS)

A Política de segurança da informação, na DMS LOGISTICS, aplica-se a todos os todos os sócios, administradores, diretores, gerentes, prepostos, empregados, prestadores de serviços e demais terceiros usuários autorizados pela DMS LOGISTICS, que venham a ter acesso e utilizar, a qualquer título e natureza, no exercício de suas atividades, dados, informações, recursos, ferramentas, sistemas, aplicações ou serviços de propriedade ou controle da DMS LOGISTICS, incluindo trabalhos executados externamente que utilizem o ambiente de processamento da Organização, ou acesso a informações pertencentes à DMS LOGISTICS.

A divulgação da política às partes interessadas da DMS LOGISTICS é feita através do site da DMS, treinamentos de integração, reciclagens e e-mails ao menos uma vez ao ano.

Esta política é aplicável ainda aos Colaboradores em trabalho remoto, incluindo, em teletrabalho e home office. A DMS LOGISTICS poderá estabelecer, a seu critério único, políticas, processos e diretrizes de segurança de informação específicas para estes casos.

## 4. DOCUMENTOS DE REFERÊNCIA

- Lei nº 9.279/1996 - Regula direitos e obrigações relativos à propriedade industrial
- Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)
- Lei 13.853/2019 - Modifica a Lei Geral de Proteção de Dados Pessoais, publicada em 2018

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 4 de 21
Título: Política de Segurança da Informação	

- NBR ISO/IEC 27001:2013 – Segurança da Informação
- NBR ISO 9001:2015 – Gestão de Qualidade

## 5. AUTORIDADE E RESPONSABILIDADES

- Diretores: É competência dos Diretores da DMS analisar, revisar e aprovar esta Política sempre que se fizer necessário. Esta Política entra em vigor na data de sua aprovação pela Diretoria e revoga quaisquer documentos em contrário.
- Gestor de TI e infraestrutura: Cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada regularmente de forma a garantir que quaisquer alterações no direcionamento da DMS LOGISTICS sejam incorporadas a mesma e esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.
- Gestores: É de responsabilidade do Gestor de cada área estabelecer critérios relativos ao nível de confidencialidade das informações (relatórios e/ou mídias) geradas por sua área. As informações devem ser classificadas como: Pública, Interna, Confidencial ou Restrita.
- Colaboradores: Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar Gestor de TI e Infraestrutura para consulta sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização.

A seu critério único, os Diretores da DMS LOGISTICS poderão implementar comitê destinado à avaliação, revisão, implementação e fiscalização desta Política e dos seus termos e condições.

Em caso de dúvida ou questão relativamente ao disposto nesta política, o Colaborador deverá entrar em contato com o Gestor de TI e Infraestrutura pelos seguintes meios: [\_\_]

A DMS LOGISTICS promoverá, desenvolverá, atualizará e implementará, de forma regular e contínua, as demais políticas, processos e práticas necessárias para viabilizar e consumir esta política de segurança de informação e cibernética, incluindo, mas não se limitando: (i) política de continuidade de negócio, destinada a garantir as atividades de negócio críticas e essenciais da DMS LOGISTICS; (ii) política de gestão e recuperação de desastres; (iii) política de avaliação de risco de fornecedores; (iv) e demais políticas correlatas que se façam necessárias ou convenientes, a critério da DMS LOGISTICS.

## 6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- Confidencialidade: Garantir de que a informação somente estará acessível para pessoas autorizadas;
- Integridade: Assegurar de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
- Disponibilidade: Assegurar de que a informação estará disponível sempre que for necessário.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 5 de 21
Título: Política de Segurança da Informação	

- Conformidade: Garantir o cumprimento dos requisitos, podendo ser obrigações legais e/ou contratuais com as partes interessadas e com aspectos legais e regulatórios.
- Capacitação: Incentivar à realização de treinamentos e capacitação na área de segurança da informação.

## 7. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A DMS LOGISTIC tem como política oferecer aos nossos clientes soluções logísticas de alta performance com base na criatividade e na otimização constante das operações, do sistema de gestão da qualidade, segurança da informação e segurança, promovendo a melhoria contínua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com os ambientes web e cloud. Assim, assegurar a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos interesses da DMS LOGISTICS e de suas partes interessadas.

A DMS LOGISTICS se compromete a:

1. Prestar serviços de agenciamento de cargas aéreas e marítimas de importação e exportação.
2. Salvar seus ativos de informação para reduzir a vulnerabilidade e incidentes.
3. Assegurar a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos interesses da DMS LOGISTICS e de suas partes interessadas.
4. Avaliar os riscos dos negócios com objetivo de assegurar a satisfação do cliente, requisitos de aplicáveis e viabilidade financeira;
5. Alinhar a gestão da segurança da informação aos nossos negócios.
6. Realizar o tratamento da informação em todo seu ciclo de vida de modo ético e responsável.
7. Garantir a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo de vida: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.
8. Identificar, analisar, avaliar e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares.
9. Adotar mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens, e roubo e ataques, em todo o ciclo de vida das informações.
10. Monitorar de forma contínua os ativos de informação e utilizamos processos, controles e tecnologias de prevenção e resposta a ataques.
11. Disseminar a cultura de segurança da informação por meio de programa permanente de sensibilização, conscientização e capacitação.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 6 de 21
Título: Política de Segurança da Informação	

12. Preservar os requisitos de segurança da informação na contratação de serviços ou de pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários.
13. Conceder a colaboradores e a terceiros somente o acesso às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal.
14. Identificar, por meio do controle de acesso, cada usuário individualmente e nos casos devidamente comprovados de tratamento indevido da informação corporativa o responsabilizamos, juntamente com o administrador que lhe concedeu o acesso.
15. Analisar as ocorrências de tratamento indevido de informações corporativas sob os aspectos legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades.
16. Satisfazer plenamente as necessidades dos nossos clientes e aumentar constantemente a sua satisfação, razão pela qual atribuímos grande importância à promoção da consciência da qualidade entre os nossos colaboradores.
17. Investir em treinamento e capacitação do nosso maior capital, os nossos colaboradores para que todos estejam integrados ao sistema de gestão de qualidade e segurança da informação.
18. Trabalhar na melhoria contínua dos processos e sistemas de Qualidade e segurança da informação.
19. Garantir uma equipe dedicada e qualificada com orientação empreendedora e inovadora. Os executivos orientam pelo exemplo e criam o ambiente interno para atingir as metas de qualidade.
20. Assegurar que as relações com nossos fornecedores são de benefício mútuo. Para isso, é indispensável uma comunicação transparente, um acordo sobre objetivos comuns em relação aos requisitos do cliente e a cooperação na melhoria dos processos conjuntos.
21. Promover as atividades e os recursos associados para atingir os resultados em todo o sistema e em todos os níveis da hierarquia.

A contratação, manutenção e implementação de sistemas, aplicativos, programas e demais recursos e ferramentas de informação da DMS LOGISTICS deverão levar sempre em conta os riscos de segurança existentes e as respectivas medidas, controles e mecanismos de mitigação. A DMS LOGISTICS executará avaliações regulares e contínuas, incluindo por meio de terceiros, sobre as medidas, controles e mecanismos de segurança de seus sistemas, aplicativos, programas e demais recursos e ferramentas de informação, incluindo, análises de impacto de risco.

## **8. OBRIGAÇÕES GERAIS**

Todos os Colaboradores da DMS LOGISTICS devem considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a DMS LOGISTICS e deve sempre ser tratada profissionalmente.



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 7 de 21
Título: Política de Segurança da Informação	

Os Colaboradores devem observar e cumprir, a todo o tempo, o disposto nesta política de segurança e cibernética, sob pena das sanções e medidas legais e contratuais aplicáveis. A DMS LOGISTICS monitora e fiscaliza, por conta própria ou mediante o uso de terceiros, o cumprimento e conformidade dos seus Colaboradores com o disposto nesta política de segurança e cibernética.

Todo e qualquer usuário de recursos computadorizados da companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- Exponha a DMS LOGISTICS a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, de informações ou ainda da perda de equipamento;
- Envolver a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolver o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Não é permitida a retirada de quaisquer aparelhos, equipamentos, informações das instalações da DMS LOGISTICS sem a autorização expressa e escrita da equipe de segurança.

Para a execução das atividades e serviços, a DMS LOGISTICS poderá disponibilizar aos seus Colaboradores, a seu critério único, determinados aparelhos, equipamentos e recursos, a título de comodato. Os aparelhos, equipamentos e recursos cedidos permanecerão, a todo o tempo, sob a propriedade da DMS LOGISTICS, tendo o Colaborador somente a posse precária sobre os mesmos. Em momento algum, a propriedade desses bens cedidos se transferirá para os Colaboradores. Os Colaboradores deverão zelar, a todo o tempo pela guarda, correto manuseio e a manter os bens cedidos em adequado e normal estado de conservação, considerando o desgaste natural decorrente do uso normal e adequado dos mesmos. É vedada a utilização dos bens cedidos para finalidade diversa daquela a que se destinam. Os bens cedidos deverão ser mantidos em local adequado, apropriado e seguro, observadas as recomendações e orientações da DMS LOGISTICS. Sempre que solicitado pela DMS LOGISTICS, os Colaboradores retornarão devolverão os aparelhos, equipamentos e recursos que tenham sido cedidos pela DMS LOGISTICS para a execução das atividades. Os Colaboradores que, no exercício de suas atividades, tenham em sua posse e utilizem ativos da DMS, deverão proceder à sua devolução e cessar o uso de quaisquer ferramentas, recursos e serviços disponibilizados pela DMS, após o término do contrato de trabalho, prestação de serviços ou fundamento legal aplicável.

Os terceiros que venham a ter acesso aos sistemas de informação da DMS LOGISTICS, sejam fornecedores, clientes ou outros, deverão ter acesso às normas de segurança de informação aplicáveis, e concordar com os seus termos e condições, para assegurar e garantir a segurança de informação da DMS LOGISTICS, antes do acesso ser concedido, incluindo, normas de confidencialidade.

Esses fornecedores devem adotar sempre as melhores práticas de mercado em matéria de segurança de informação e serão, regularmente, monitorados para garantir o cumprimento e conformidade com os requisitos de segurança da informação aplicáveis. Os contratos devem incluir provisões adequadas para garantir a segurança das informações e sistemas da DMS



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 8 de 21
Título: Política de Segurança da Informação	

LOGISTICS.

Os Colaboradores deverão ser, regularmente, treinados e capacitados em matérias de segurança de informação, relativamente à natureza e tipo de ameaças, medidas de segurança existentes e necessidade de comunicação de suspeitas e indícios de problemas. A DMS LOGISTICS é comprometida em fornecer treinamento e capacitação mandatórios a todos os Colaboradores para assegurar a segurança da informação.

A disposição definitiva e permanente de mídias, softwares, sistemas e outros aparelhos e equipamentos da DMS LOGISTICS deverá ser precedida da eliminação e destruição de quaisquer dados e informações contidas nesses ativos. O mesmo procedimento será aplicável no caso de defeito ou falha desses ativos.

## 9. PROPRIEDADE INTELECTUAL

É de propriedade da DMS LOGISTICS, todos os materiais, obras, “designs”, processos, fluxogramas, pesquisas, análises, criações ou procedimentos desenvolvidos por qualquer Colaborador no exercício de suas atividades para a DMS LOGISTICS, sem prejuízo da aplicabilidade do disposto na legislação brasileira.

## 10. POLÍTICA DE USO

- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.
- Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.
- Relate à equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

## 11. DADOS DOS COLABORADORES. APARELHOS DOS COLABORADORES.

Todos os Dados Pessoais de Funcionários que porventura sejam armazenados serão considerados dados confidenciais.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da DMS LOGISTICS. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da DMS LOGISTICS, sem prévia e expressa autorização por parte da diretoria.

A presente Política é aplicável ainda a aparelhos e equipamentos pessoais de Colaboradores que venham a ser utilizados para o exercício das respectivas atividades e serviços, naquilo que couber, contanto que devidamente autorizados e permitidos pela DMS LOGISTICS.



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 9 de 21
Título: Política de Segurança da Informação	

A DMS LOGISTICS poderá estabelecer, a seu critério único, políticas, processos e diretrizes de segurança de informação específicas, destinadas a regular o acesso e utilização de dados, informações, ferramentas, recursos e serviços da DMS LOGISTICS em aparelhos pessoais dos Colaboradores, fornecedores e usuários autorizados, entre elas, os requisitos, modelos, marcas autorizadas. Essas políticas, processos e diretrizes específicas poderão ser alteradas pela DMS LOGISTICS, de tempos em tempos.

Sempre que solicitado pela DMS LOGISTICS, os Colaboradores disponibilizarão os seus aparelhos e equipamentos pessoais para: (i) implementação de medidas de segurança, tais como, atualizações de sistemas, serviços e aplicativos de segurança para proteção e salvaguarda dos dados, informações, sistemas e recursos da DMS LOGISTICS; (ii) monitoramento e averiguação da conformidade dos Colaboradores com as políticas, processos e práticas da DMS LOGISTICS; (iii) realização de testes e auditorias de segurança ao ambiente, recursos, sistemas, aplicações e redes da DMS LOGISTICS; (iv) cópias e backups das informações, dados, serviços e atividades da DMS LOGISTICS contidos nos aparelhos e equipamentos pessoais dos Colaboradores; e (v) remoção, eliminação e desinstalação de dados, informações, serviços, recursos, ferramentas da DMS LOGISTICS dos aparelhos e equipamentos pessoais dos Colaboradores, em particular, com o término da relação contratual aplicável.

## 12. PROGRAMAS ILEGAIS

É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na DMS LOGISTICS.

Os usuários não podem, em hipótese alguma, instalar este tipo de “software” (programa) nos equipamentos da DMS, mesmo porque somente o pessoal da área de TI tem autorização para instalação de programas previamente autorizados dentro da política de segurança da organização. Semestralmente, o Setor de TI fará verificações nos dados dos servidores, Drives e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Todos os colaboradores assinam um termo de responsabilidade e uso dos equipamentos e sistemas da DMS, nesse termo é detalhado que:

- Cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretará em responsabilidade sua.
- Sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou o console.
- Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança.
- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;
- Todos os dados relativos à empresa devem ser mantidos no drive da DMS, onde existe um sistema de backup diário e confiável.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 10 de 21
Título: Política de Segurança da Informação	

- Caso seja necessário, o funcionário pode entrar em contato com a equipe técnica para solicitar suporte.

### **13. PERMISSÕES E SENHAS**

Todo usuário para acessar os dados da rede da DMS LOGISTICS, deverá possuir um login e senha previamente cadastrados pelo setor de TI.

Quem deve fornecer os dados referente aos tipos de acessos e programas de cada colaborador é o responsável direto, que deve preencher uma ficha e entregá-la ao departamento de RH. Quando da necessidade de cadastramento de um novo usuário para utilização da “rede”, sistemas ou equipamentos de informática da DMS, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, por meio de comunicado interno ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

O setor de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 30 (trinta) dias. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações etc.) deverão comunicar ao Setor de TI quem será o seu substituto quando de sua ausência da DMS, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de TI.

### **14. ESTAÇÕES DE COMPUTADOR DE TRABALHO DOS COLABORADORES**

Todas as estações de computador de trabalho possuem usuário administrador, para garantir que não seja feita nenhuma alteração nas configurações do computador.

Os usuários são proibidos pela conta do administrador de fazer downloads e instalação de aplicativos não autorizados.

### **15. MONITORAMENTO DE E-MAILS**

O e-mail corporativo é acessado por ferramentas disponibilizadas pela DMS LOGISTICS, não existindo qualquer expectativa de privacidade como ocorre com o e-mail de uso pessoal e privado do Colaborador. O e-mail corporativo trata-se de uma ferramenta de propriedade da DMS LOGISTICS.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 11 de 21
Título: Política de Segurança da Informação	

Assim, é importante que o funcionário não utilize o e-mail corporativo de maneira indevida, negligente ou maliciosa

## 16. COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de pastas nos computadores, desktops e demais dispositivos móveis da empresa. Todos os dados deverão ser armazenados no Drive da DMS, e a autorização para acessá-los deverá ser fornecida pelo pessoal do TI. Periodicamente, o Setor de TI fará verificações nos dados dos drives e/ou nos computadores dos usuários, visando garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede.

Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso do TI. Não são permitidos na empresa o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

## 17. MESA E TELA LIMPA

- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa, devem ser armazenados em gavetas ou armários trancados quando não estiverem em uso, principalmente fora do horário de expediente.
- Informações em meio físico classificadas como sensíveis, confidenciais, restritas ou críticas para o da DMS devem ser armazenadas e trancadas em local seguro e separado.
- Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados no desktop, notebook, monitor, quadros de aviso ou paredes.
- Não anotar informações classificadas como restrita, confidencial, sensível em locais onde a informação possa ficar exposta, como quadros de avisos, murais e quadro branco.
- Em períodos de ausência da estação de trabalho, documentos em meio físico devem ser retirados das mesas e de outras áreas de superfície;
- Documentos de uso interno ou confidenciais em meio eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso a pessoas não autorizadas;
- Todos os documentos impressos devem ser destruídos antes de serem descartados no lixo. Documentos classificados como confidencial e restrito devem ser destruídos utilizando máquina desfragmentadora ou incinerados.
- Evitar imprimir documentos que possam ser lidos no desktop e notebook.
- Sempre fazer logoff quando sair sua mesa bloqueando a tela do Desktops e notebooks.
- Não deixar logado impressoras, desktops e notebooks quando estiver ausente do escritório.
- Objetos pessoais devem estar sempre guardados, seja em seu armário ou em sua bolsa.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 12 de 21
Título: Política de Segurança da Informação	

- Sua senha é pessoal e intransferível, por isso não repasse a ninguém.
- Ao final do expediente, ou quando for se ausentar, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários e desligar o desktop ou notebook.
- Não colocar em cima da mesa copos com água, sucos, café, etc.

## 18. ACESSO À INTERNET

- Dentro das instalações da DMS é fornecido acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;
- O acesso à internet pode ser fornecido tanto através da rede corporativa da DMS, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pela DMS;
- Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do gestor.
- O uso recreativo da internet não deverá se dar no horário de expediente.
- Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pela DMS está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;
- Durante o monitoramento do acesso à internet, a DMS se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;
- Durante o acesso à Internet fornecido pela DMS não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:
  - Qualquer espécie de exploração sexual;
  - Qualquer forma de conteúdo adulto, erotismo, pornografia;
  - Qualquer tipo de Pornografia infantil;
  - Qualquer forma de ameaça, chantagem e assédio moral ou sexual;
  - Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;
  - Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 13 de 21
Título: Política de Segurança da Informação	

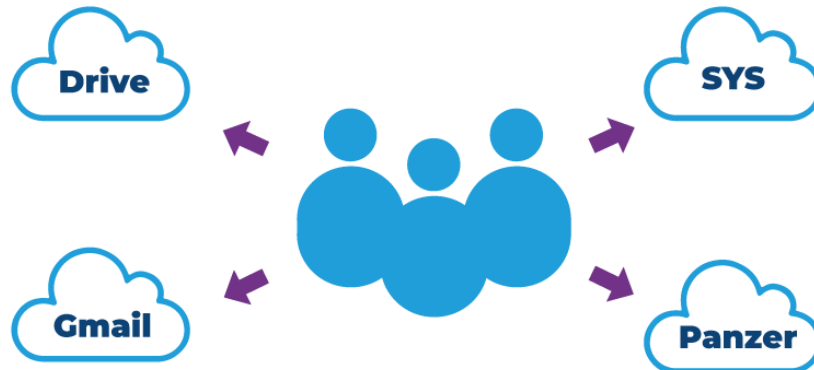
- Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;
- A prática e/ou a incitação de crimes ou contravenções penais;
- A prática de propaganda política nacional ou internacional;
- A prática de quaisquer atividades comerciais desleais;
- O desrespeito a imagem ou aos direitos de propriedade intelectual da DMS LOGISTICS;
- A disseminação de códigos maliciosos e ameaças virtuais;
- Tentativa de expor a infraestrutura computacional da DMS a ameaças virtuais;
- Divulgação não autorizada de qualquer informação da DMS LOGISTICS classificada como confidencial, restrita ou de uso interno;
- Uso de sites ou serviços que busquem contornar controles de acesso à internet.
- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc).
- É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança.
- Lembrando novamente que o uso da internet estará sendo auditado constantemente assim como o usuário.
- O funcionário será responsável pelo uso dos aparelhos, equipamentos, recursos, ferramentas e serviços disponibilizados pela DMS LOGISTICS para a realização de suas atividades.

## **19. COMPORTAMENTO CORPORATIVO EM MÍDIAS E REDES SOCIAIS**

Quando no uso de suas mídias e redes sociais particulares, colaboradores, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

- Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à DMS, seus colaboradores, terceiros contratados e prestadores de serviço.

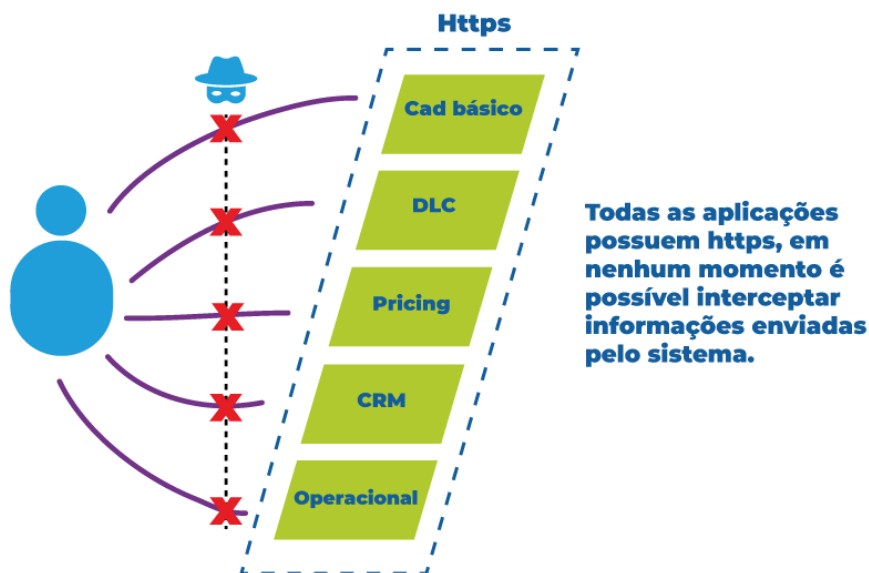
## 20. BACKUP, SEGURANÇA E CONFIABILIDADE



O gerenciamento do banco de dados é responsabilidade exclusiva do Setor de Ti, assim como a manutenção, alteração e atualização de equipamentos e programas.

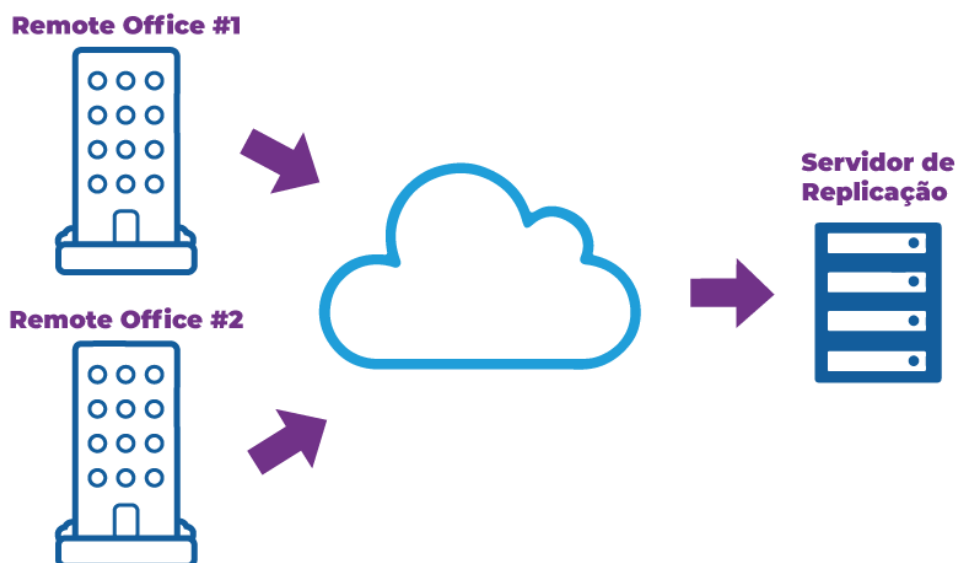
O usuário só tem acesso ao servidor através do nosso ip local.

Os backups são feitos automaticamente na nossa nuvem e no servidor, sendo assim não há risco de perda de dados.



Todos os nossos dados da nuvem são replicados para um outro servidor, sendo assim, mesmo que haja algum tipo de problema na nuvem, nossos dados ainda estarão salvos no servidor.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 15 de 21
Título: Política de Segurança da Informação	



## 21. ADMISSÃO, AFASTAMENTO E DEMISSÃO DE COLABORADOR

### 21.1. IDENTIFICAÇÃO DA NECESSIDADE

O setor de Recrutamento e Seleção de Pessoal da DMS LOGISTICS deverá informar ao setor de Informática, toda e qualquer movimentação de admissão, suspensão, interrupção e demissão de seus colaboradores, para que os mesmos possam ser cadastrados ou excluídos nos sistemas da DMS. Isto inclui o fornecimento de sua senha e registro do seu nome como usuário nos sistemas, pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à DMS, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso aos sistemas. No caso de demissão, o setor de RH deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído dos sistemas da DMS.

Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da DMS LOGISTICS. Nenhum colaborador, poderá ser contratado, sem ter expressamente concordado com esta política.



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 16 de 21
Título: Política de Segurança da Informação	

## **21.2. ACESSOS A E-MAILS E PLATAFORMAS CORPORATIVAS - AFASTAMENTO**

Durante o período de afastamento da empresa, o setor de TI suspenderá os acessos do colaborador aos sistemas informatizados e e-mails e fará o redirecionamento automático dos e-mails, para outro membro da equipe e mantemos nossos clientes e parceiros informados do afastamento do colaborador no período determinado conforme decisão do Gestor responsável.

## **21.3. RETORNO AO TRABALHO**

Após ser aprovado o retorno ao trabalho, o RH deve informar ao setor de TI a liberação aos acessos do colaborador aos sistemas informatizados e e-mails e suspender o redirecionamento automático dos e-mails.

## **22. PROMOÇÃO E TRANSFERÊNCIA DE COLABORADOR**

Quando um colaborador for promovido ou transferido de setor ou gerência, o setor de RH deverá comunicar o fato ao Setor de TI, para que sejam feitas as adequações necessárias para os acessos do referido funcionário aos sistemas informatizados da DMS.

## **23. PENALIDADES**

O não cumprimento política de Segurança da Informação da DMS LOGISTICS poderá acarretar na aplicação de medidas e sanções, incluindo, mas não se limitando, o desligamento do colaboradores de acordo com a natureza e gravidade da ocorrência.

## **24. INFORMAÇÃO E COMUNICAÇÃO**

Todos os destinatários desta Política, ao identificar uma situação de risco relacionada à esta Política, e demais normas de conteúdo similar, têm a responsabilidade de comunicar o fato à Direção e ao Departamento de Qualidade da DMS.

Para isso poderão ser utilizados os seguintes canais de comunicação:

- Canal Disque Denúncia: [ouvidoria@dmslog.com](mailto:ouvidoria@dmslog.com) (caso queria fazer uma denúncia anônima);
- Chamado através do DMSYS.

A título exemplificativo, os Colaboradores deverão informar, o quanto antes, de qualquer situação, fato ou evento, incluindo mera suspeita ou tentativa, envolvendo, entre outros:

(i) uso, acesso, transmissão, divulgação, compartilhamento, ou qualquer outro tipo de tratamento não autorizado de dados e informações de propriedade ou sob o controle da DMS LOGISTICS;

(ii) qualquer iniciativa, interna ou externa, destinada a interferir, prejudicar, comprometer a segurança, disponibilidade, autenticidade confidencialidade e integridade dos dados e



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 17 de 21
Título: Política de Segurança da Informação	

informações, ou funcionamento e desempenho de aparelhos, equipamentos, recursos, ferramentas, serviços e medidas de segurança da DMS LOGISTICS;

(iii) perda, dano, falha, defeito de aparelhos, equipamentos de propriedade ou sob o controle da DMS, ou até mesmo, aparelhos e equipamentos pessoais dos colaboradores, por meio dos quais tenham acesso a dados e informações de propriedade ou sob o controle da DMS LOGISTICS;

(iv) qualquer inconformidade que venha a ser identificada relativamente a esta Política e demais aplicáveis aos Colaboradores, tais como, acordos de confidencialidade, prestação de serviços, contratos de trabalho, entre outros; e

(v) quaisquer outras situações, fatos ou eventos que, pela sua natureza, possam representar um risco em matéria de segurança de informação e cibernética para a DMS LOGISTICS.

## 25. TERMO E DEFINIÇÕES

- Informação sensível: Todos os dados que precisam ser protegidas.
- Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.
- Acesso: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados
- Armazenamento: ação ou resultado de manter ou conservar em repositório um dado
- Arquivamento: ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência
- Avaliação: ato ou efeito de calcular valor sobre um ou mais dados
- Classificação: maneira de ordenar os dados conforme algum critério estabelecido
- Coleta: recolhimento de dados com finalidade específica
- Comunicação: transmitir informações pertinentes a políticas de ação sobre os dados
- Controle: ação ou poder de regular, determinar ou monitorar as ações sobre o dado
- Difusão: ato ou efeito de divulgação, propagação, multiplicação dos dados
- Distribuição: ato ou efeito de dispor de dados de acordo com algum critério estabelecido
- Eliminação: ato ou efeito de excluir ou destruir dado do repositório
- Extração: ato de copiar ou retirar dados do repositório em que se encontrava

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 18 de 21
Título: Política de Segurança da Informação	

- Modificação: ato ou efeito de alteração do dado
- Processamento: ato ou efeito de processar dados
- Produção: criação de bens e de serviços a partir do tratamento de dados
- Recepção: ato de receber os dados ao final da transmissão
- Reprodução: cópia de dado preexistente obtido por meio de qualquer processo
- Transferência: mudança de dados de uma área de armazenamento para outra, ou para terceiro
- Transmissão: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.
- Utilização: ato ou efeito do aproveitamento dos dados.
- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

## 26. A EMPRESA E A POLÍTICA DE SEGURANÇA

Todas as normas aqui estabelecidas visam proteger a instituição contra acessos indevidos aos sistemas informatizados.

Ao receber a cópia da Política de Segurança, o colaborador compromete-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e navegação na internet podem estar sendo monitorados.

A equipe de segurança encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

## 27. SITUAÇÕES NÃO CONTEMPLADAS

Esta Política apresenta diretrizes gerais, sendo que algumas situações específicas podem não estar contempladas.

O que se espera nesses casos é que cada um aja com responsabilidade, prudência e consciência ética, avaliando o melhor caminho a seguir com a certeza de que a solução adequada será sempre regida pelo bom-senso e pelos valores que prezamos.

Quaisquer questões não especificadas neste documento e relacionadas aos temas ética e conduta, deverão ser submetidos para avaliação da Diretoria.

Cabe a área de Recursos Humanos manter este documento atualizado, em conformidade com o divulgado pelo grupo internacionalmente, levando seu conteúdo a conhecimento de todos do Grupo DMS.

Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 19 de 21
Título: Política de Segurança da Informação	

## 28. VIGÊNCIA

Este Código entra em vigor na data de sua publicação, revogando e substituindo qualquer comunicação anterior sobre o assunto e permanecerá vigente por prazo indeterminado.

## 29. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	18/10/2018	Emissão do documento.
01	28/09/2020	Revisão geral para incluir novos compromissos com o meio ambiente, saúde e segurança dos colaboradores e segurança da informação e codificação no documento.
02	22/04/2021	Revisão geral para alterar o termo web e clouds por web e cloud e modificar o template do documento.

## 30. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	Wellington Ferreira	
Revisado por:	Natalie Corrêa	
Aprovador por:	Eduardo Reis	
Nível de Confidencialidade:	X	Informação Pública
		Informação Interna
		Informação Confidencial
		Informação Sigilosa



Política	
Código: POL-SGI-003	Revisão: 02
Data: 01/12/2020	Páginas: 20 de 21
Título: Política de Segurança da Informação	

## **Anexo I – Termo de Compromisso com a Política de Segurança da Informação**

Declaro, para todos os fins, que recebi um exemplar de Política de Segurança da Informação da DMS LOGISTICS, a qual estava em linguagem clara e de fácil compreensão, de modo que assumo que estou ciente da minha responsabilidade e me comprometo a cumpri-la e a respeitá-la integralmente.

Declaro ainda, que estou ciente quanto à observância em todas as situações e circunstâncias que estejam diretas ou indiretamente vinculadas às minhas atividades na DMS LOGISTICS.

Da mesma forma, estou ciente que o descumprimento de qualquer um dos termos contidos na presente Política de Segurança da Informação, ensejará a formação de uma sindicância administrativa, que será constituída para a apuração de eventuais irregularidades.

Ato contínuo, ante a constatação de irregularidades, declaro que estou ciente que a DMS poderá promover as medidas cabíveis, tanto na esfera administrativa, como na judicial, visando reparar todos os prejuízos causados, seja na esfera penal, cível ou trabalhista.

Por fim, por estar de acordo, assino o presente instrumento.

Local e data	
Nome completo	
CPF	
Assinatura	



**NUNCA COLOCAMOS EM RISCO A  
QUALIDADE E NEM A ÉTICA NOS NEGÓCIOS**

*WE NEVER COMPROMISE ON QUALITY AND  
BUSINESS ETHICS*

**[WWW.DMSLOG.COM](http://WWW.DMSLOG.COM)**