POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código: POL-QCO-002
Revisão: 6
Data: 03/02/2025
Aprovado por: Victor Gonzaga
Uso Interno

1. CONTEXTUALIZAÇÃO

A DMS é uma empresa referência em soluções inovadoras para logística global, destacando-se pelo aprimoramento contínuo de seus serviços tecnológicos e pela forte presença em filiais e parceiros distribuídos pelos cinco continentes.

A Política de Segurança da Informação tem como objetivo mitigar riscos, protegendo a DMS contra ameaças e vulnerabilidades, bem como contra impactos aos seus ativos que possam comprometer a confidencialidade, integridade e disponibilidade das informações.

2. OBJETIVO

A DMS tem como objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da Segurança da Informação, promovendo a melhoria contínua dos processos voltados à proteção de dados e informações. Dessa forma, busca prevenir, detectar e mitigar vulnerabilidades, reduzindo riscos de incidentes nos ambientes web e cloud. Com isso, a empresa assegura a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações essenciais para suas operações e para atender aos interesses de suas partes interessadas.

A Política de Segurança da Informação e Cibernética da DMS poderá ser avaliada e revisada periodicamente, a critério exclusivo da empresa, ou sempre que eventos e circunstâncias exigirem ajustes. O objetivo é garantir sua constante atualização, adequação e efetividade, reforçando a proteção dos ativos da organização.

3. ÁREAS DE RELACIONAMENTO (DESTINATÁRIOS)

A Política de Segurança da Informação da DMS aplica-se a todos os sócios, administradores, diretores, gerentes, prepostos, empregados, prestadores de serviços e demais terceiros autorizados que tenham acesso, sob qualquer título ou natureza, a dados, informações, recursos, ferramentas, sistemas, aplicações ou serviços de propriedade ou controle da empresa. Essa política abrange tanto as atividades realizadas internamente quanto aquelas executadas externamente que utilizem o ambiente de processamento da organização ou acessem informações pertencentes à DMS.

A divulgação da política às partes interessadas ocorre por meio do site da empresa, treinamentos de integração, programas de reciclagem e comunicações por e-mail, sendo reforçada pelo menos uma vez ao ano.

Além disso, esta política se estende aos colaboradores em regime de trabalho remoto, incluindo teletrabalho e home office. A DMS poderá, a seu critério, estabelecer políticas, processos e diretrizes específicas para garantir a segurança da informação nesses casos.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Confidencialidade: Garantir que as informações sejam acessíveis apenas a pessoas autorizadas, prevenindo acessos indevidos ou vazamentos.

Integridade: Assegurar que os dados, tanto armazenados quanto em trânsito, não sofram modificações não autorizadas, sejam elas intencionais ou acidentais.

Disponibilidade: Garantir que as informações estejam sempre acessíveis e utilizáveis quando

necessário, evitando interrupções que impactem as operações.

Conformidade: Cumprir requisitos legais, contratuais e regulatórios, assegurando que a DMS LOGISTICS esteja alinhada às normas vigentes e às expectativas das partes interessadas.

Capacitação: Incentivar a realização de treinamentos e programas de conscientização em Segurança da Informação, garantindo que todos os envolvidos compreendam seu papel na proteção dos dados da empresa.

5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A DMS LOGISTICS adota como política oferecer soluções logísticas de alta performance, baseadas na criatividade, otimização contínua das operações e aprimoramento dos sistemas de gestão da qualidade e segurança da informação. Nosso compromisso inclui a melhoria contínua dos processos de segurança de dados, garantindo a prevenção, detecção e mitigação de vulnerabilidades, especialmente em ambientes web e cloud. Dessa forma, asseguramos a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações essenciais para o funcionamento da DMS e para a proteção dos interesses de nossas partes interessadas.

A DMS se compromete a:

1. Oferecer serviços de agenciamento de cargas aéreas e marítimas para importação e exportação com eficiência e alto desempenho.
2. Proteger os ativos de informação para reduzir vulnerabilidades e prevenir incidentes que possam comprometer a segurança da empresa.
3. Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações essenciais para as operações da DMS e para a proteção dos interesses de suas partes interessadas.
4. Realizar avaliação contínua dos riscos do negócio, garantindo a satisfação do cliente, conformidade com requisitos aplicáveis e viabilidade financeira.
5. Alinhar a gestão da segurança da informação às estratégias e processos da DMS, fortalecendo a governança corporativa.
6. Tratar as informações ao longo de todo o seu ciclo de vida de forma ética, responsável e em conformidade com as regulamentações aplicáveis.
7. Assegurar a proteção da informação em todas as suas fases: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.
8. Identificar, analisar, avaliar e tratar riscos associados aos ativos de informação por meio de avaliações periódicas e regulares.
9. Implementar mecanismos de proteção contra uso indevido, fraudes, perdas, sabotagens, ataques e erros, garantindo a segurança da informação durante todo seu ciclo de vida.
10. Monitorar continuamente os ativos de informação, utilizando processos, controles e tecnologias de prevenção e resposta a incidentes.
11. Promover a cultura de segurança da informação através de programas permanentes de sensibilização, conscientização e capacitação.
12. Assegurar que os requisitos de segurança da informação sejam mantidos na contratação

de serviços e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários.

13. Garantir que colaboradores e terceiros tenham acesso apenas às informações necessárias para o desempenho de suas funções, conforme determinado por contrato ou exigência legal.
14. Identificar e controlar o acesso individual de cada usuário e, em casos comprovados de uso indevido da informação corporativa, responsabilizar tanto o usuário quanto o administrador que concedeu o acesso.
15. Analisar ocorrências de tratamento inadequado de informações corporativas, responsabilizando os envolvidos sob os aspectos legal e disciplinar, e corrigindo vulnerabilidades sob o aspecto técnico.
16. Garantir a satisfação dos clientes, promovendo a conscientização sobre a qualidade e excelência dos serviços entre os colaboradores.
17. Investir na capacitação e desenvolvimento dos colaboradores, assegurando sua integração ao Sistema de Gestão da Qualidade e Segurança da Informação.
18. Aprimorar continuamente os processos e sistemas de qualidade e segurança da informação, garantindo maior eficiência e proteção.
19. Manter uma equipe qualificada, empreendedora e inovadora, onde os líderes atuam pelo exemplo e criam um ambiente favorável para o alcance das metas de qualidade.
20. Fomentar relações de benefício mútuo com fornecedores, estabelecendo comunicação transparente, alinhamento de objetivos e cooperação na melhoria de processos conjuntos.
21. Promover a alocação eficiente de recursos e atividades para garantir resultados consistentes em todos os níveis da organização.

A contratação, manutenção e implementação de sistemas, aplicativos, programas e demais recursos e ferramentas de informação da DMS deverão levar sempre em conta os riscos de segurança existentes e as respectivas medidas, controles e mecanismos de mitigação. A DMS 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.

6. OBRIGAÇÕES GERAIS

Todos os Colaboradores da DMS 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 e deve sempre ser tratada profissionalmente.

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 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 a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, de informações ou ainda da perda de equipamento:

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolva 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 sem a autorização expressa e escrita da equipe de segurança.

Para a execução das atividades e serviços, a DMS 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, tendo o Colaborador somente a posse precária sobre os mesmos. Em momento algum, a propriedade desses bens cedidos se transferiu 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. Sempre que solicitado pela DMS, os Colaboradores retornarão devolverão os aparelhos, equipamentos e recursos que tenham sido cedidos pela DMS 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, 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, 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.

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 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 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.

7. PROPRIEDADE INTELECTUAL

É de propriedade da DMS, todos os materiais, obras, “designs”, processos, fluxogramas, pesquisas,

análises, criações ou procedimentos desenvolvidos por qualquer Colaborador no exercício de suas atividades para a DMS, sem prejuízo da aplicabilidade do disposto na legislação brasileira.

8. 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.

9. DADOS 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. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da DMS, 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.

A DMS 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 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, de tempos em tempos.

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

10. PROGRAMAS ILEGAIS

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

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 responsabilidade sua.
- Sempre que sair da frente de sua estação, tenha certeza de 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.
- Caso seja necessário, o funcionário pode entrar em contato com a equipe técnica para solicitar suporte.

11. 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.

12. 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.

13. 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.

Assim, é importante que o funcionário não utilize o e-mail corporativo de maneira indevida, negligente ou maliciosa. [1]

14. OMPARTILHAMENTO 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 às autorizações de acesso do TI. Não são permitidos na empresa o compartilhamento de dispositivos móveis tais como pen drives e outros.

15. 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;
- 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.

16. 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 à 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;

- ✓ Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam estas 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.

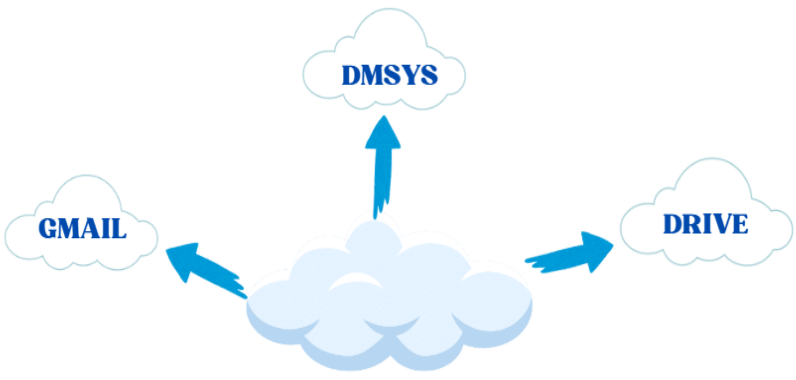
- Lembrando novamente que o uso da internet estará sendo auditado constantemente assim como o usuário.
- O funcionário será responsável pelo uso dos aparelhos, equipamentos, recursos, ferramentas e serviços disponibilizados pela DMS LOGISTICS para a realização de suas atividades.

17. 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.

18. BACKUP, SEGURANÇA E CONFIABILIDADE

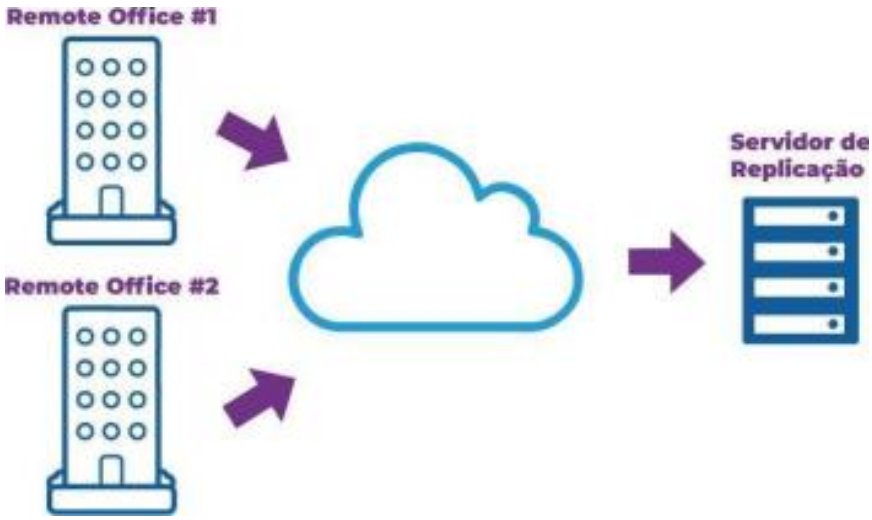


O gerenciamento do banco de dados é responsabilidade exclusiva do Setor de Ti, assim como a manutenção, alteração e atualização de equipamentos e programas.

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 dados armazenados na nuvem são replicados para um servidor adicional, garantindo que, mesmo em caso de falha ou indisponibilidade da nuvem, as informações permaneçam protegidas e acessíveis.



19. ADMISSÃO, AFASTAMENTO E DEMISSÃO DE COLABORADOR

19.1. IDENTIFICAÇÃO DA NECESSIDADE

O setor de Recrutamento e Seleção de Pessoal da DMS LOGISTICS deverá informar ao setor de Informática,[2] 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.

19.2. ACESSOS A E-MAILS E PLATAFORMAS CORPORATIVO - 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.

19.3. 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.

19.4. 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.

19.5. PENALIDADES

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

20. INFORMAÇÃO E COMUNICAÇÃO

Todos os destinatários dessa Política devem comunicar à Direção e ao setor de Qualidade

qualquer situação de risco identificada, conforme as diretrizes estabelecidas, para que as medidas necessárias sejam tomadas.

Para isso poderão ser utilizados os seguintes canais de comunicação:

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

Os colaboradores devem comunicar imediatamente qualquer situação, fato ou evento, incluindo suspeitas ou tentativas que envolvam, por exemplo:

(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 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.

21. TERMO E DEFINIÇÕES

Informação sensível: Todos os dados que precisam ser protegidos.

- 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 assegurar 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
- 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.

22. 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 à total disposição para saneamento de dúvidas e auxílio técnico.

23. 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 submetidas 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 ao conhecimento de todos do Grupo DMS.

24. 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.

25. DOCUMENTOS DE REFERÊNCIA

- **Lei nº 9.279/1996** – Regula os direitos e obrigações relativos à Propriedade Industrial, garantindo a proteção de patentes, marcas, desenhos industriais e concorrência desleal.
- **Lei nº 13.709/2018 (LGPD)** – Define regras para a proteção de dados pessoais, regulando o tratamento, coleta, armazenamento e compartilhamento de informações, visando garantir a privacidade e os direitos dos titulares.
- **Lei nº 13.853/2019** – Modifica a LGPD, aprimorando suas disposições e criando a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização e aplicação das normas de proteção de dados.
- **NBR ISO/IEC 27001:2022** – Norma internacional que estabelece requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), garantindo a proteção contra riscos, ameaças e vulnerabilidades.
- **NBR ISO 9001:2015** – Define critérios para um Sistema de Gestão da Qualidade (SGQ), visando a melhoria contínua dos processos e a satisfação do cliente.

26. AUTORIDADE E RESPONSABILIDADES

- **Diretores:** São responsáveis por analisar, revisar e aprovar esta Política sempre que necessário. A Política entra em vigor a partir de sua aprovação pela Diretoria, revogando quaisquer documentos em contrário.
- **Gestor de TI e Infraestrutura:** Deve cumprir as diretrizes estabelecidas, manter a Política atualizada regularmente para assegurar que qualquer mudança no direcionamento da DMS LOGISTICS seja incorporada e esclarecer dúvidas sobre seu conteúdo e aplicação.
- **Gestores**: São responsáveis por definir critérios para o nível de confidencialidade das informações (relatórios e mídias) geradas em suas áreas, classificando-as como Pública, Interna, Confidencial ou Restrita.
- **Colaboradores:** Devem observar e garantir o cumprimento desta Política, acionando o Gestor de TI e Infraestrutura sempre que houver dúvidas ou situações de conflito com as diretrizes estabelecidas. Além disso, é essencial que cada colaborador compreenda a importância da segurança da informação em suas atividades diárias e participe dos

programas de conscientização promovidos pela empresa.

Os Diretores da DMS poderão, a seu exclusivo critério, estabelecer um comitê especializado para avaliar, revisar, implementar e fiscalizar esta Política de Segurança da Informação e Cibernética, garantindo sua efetividade e alinhamento com as necessidades da empresa.

Em caso de dúvidas ou questionamentos sobre esta Política, os colaboradores devem entrar em contato com o Gestor de TI e Infraestrutura por meio dos canais oficiais:

A DMS compromete-se a promover, desenvolver, atualizar e implementar, de forma contínua e regular, políticas, processos e práticas complementares para fortalecer sua segurança da informação e cibernética. Essas iniciativas incluem, mas não se limitam a: (i) política de continuidade de negócio, destinada a garantir as atividades de negócio críticas e essenciais da DMS; (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.

27. 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.
03	28/03/2023	Revisão e Padronização do documento
04	15/04/2023	Padronização do documento.
05	15/02/2024	Revisão da documentação.
06	03/02/2025	Ajustes no layout e revisão do documento.

28. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	Wellington Ferreira
Revisado por:	Natalie Corrêa, Aghata Oliveira, Leonardo Sabbadim, Paulo Gomes,

	Anna Caroline Silva.	
Aprovador por:	Eduardo Reis	
Nível de Confidencialidade:	**X**	**Informação Pública**
		Informação Interna
		Informação Confidencial
		Informação Sigilosa

ANEXO I
TERMO DE COMPROMISSO COM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Declaro, para todos os fins, que recebi um exemplar da Política de Segurança da Informação da DMS LOGISTICS, cujo conteúdo está redigido em linguagem clara e de fácil compreensão. Dessa forma, declaro estar plenamente ciente das minhas responsabilidades e comprometo-me a cumpri-la integralmente, respeitando todas as suas diretrizes.

Além disso, tenho ciência de que devo observar e seguir a Política de Segurança da Informação em todas as situações e circunstâncias relacionadas, direta ou indiretamente, às minhas atividades na DMS LOGISTICS.

Reconheço ainda que o descumprimento de qualquer um dos termos estabelecidos nesta política poderá resultar na instauração de uma sindicância administrativa para apuração de eventuais irregularidades. Caso sejam constatadas infrações, a DMS LOGISTICS poderá adotar as medidas cabíveis, tanto na esfera administrativa quanto judicial, visando a reparação de possíveis prejuízos, seja no âmbito cível, trabalhista ou penal.

Por estar de acordo com todos os termos aqui expressos, firmo a presente declaração.

Local e data	
Nome completo	
CPF	
Assinatura	