POLÍTICA DE USO ACEITÁVEL DE ATIVOS

Código: POL-TI-001
Revisão: 01
Data: 13/03/2023

1. PROPÓSITO

A Política de Uso de Ativos apresenta regras e critérios para acesso, uso e monitoramento dos ativos de tecnologia da DMS Logistics.

O objetivo é assegurar a proteção dos ativos de informação da DMS Logistcis contra ameaças internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus colaboradores a respeito. Sua aplicação protege os colaboradores, clientes, fornecedores e o ambiente corporativo de ações ilegais e/ou prejudiciais, intencionais ou não.

A DMS Logistics tem por meta estabelecer uma cultura corporativa em segurança compatível com o uso aceitável das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades da empresa.

Esta Política busca garantir a adequada e correta utilização dos ativos do escritório, entre eles, internet, rede interna, equipamentos físicos (hardware), software e recursos de tecnologia em geral. Estes ativos são destinados para uso relacionado às atividades empresariais da DMS Logistics nas atividades do seu negócio.

Além disso, busca-se viabilizar a gestão de ativos, a partir de uma visão integrada do seu ciclo de vida e levando em consideração os riscos e otimização de custos para alcançar a máxima eficácia, contribuindo de forma sustentável para alcançar as metas e objetivos da empresa.

2. ESCOPO

A Política de Uso de Ativos aplica-se a:

- Todos os ambientes físicos, incluindo-se a sede, filiais, unidades regionais, unidades de desenvolvimento, centros de processamento e quaisquer outros pertencentes ao patrimônio ou sob a custódia da DMS Logistics.
- Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela DMS Logistics, independentemente da localização geográfica;

- As regras e diretrizes se aplicam a todos os colaboradores em todos os níveis hierárquicos da empresa, visitantes e a terceiros que tenham contato com informações produzidas no âmbito de suas atuações. É fundamental ressaltar que as disposições são aplicáveis a todos os formatos de tratamento de dados pessoais possíveis, sejam meios digitais ou meios físicos.
- É responsabilidade de todos os clientes, colaboradores, stakeholders e usuários conhecer estas diretrizes e adotar as recomendações a seguir.

3. PRINCÍPIOS

São princípios básicos desta política:

- A preservação da imagem da empresa e de seus empregados;
- A criação, desenvolvimento e manutenção de cultura de segurança da informação;
- Que o nível, a complexidade e os custos das ações de Segurança da Informação sejam apropriados e adequados ao valor dos ativos da DMS Logistics, considerando os impactos e a probabilidade de ocorrência de incidentes.
- A preservação da responsabilidade solidária para dados de outras empresas que trafegam nos ativos da DMS Logistics.

4. DIRETRIZES GERAIS

4.1. RESPONSABILIDADE E COMPROMETIMENTO

O uso inapropriado dos ativos pode comprometer a segurança da DMS Logistics, expondo-a a ataques externos, comprometimento das redes, sistemas, equipamentos e problemas legais.

Colaboradores, estagiários, jovens aprendizes, clientes, fornecedores e todos que, de alguma maneira, prestarem serviços, tiverem parceria ou utilizarem, por qualquer motivo, os ativos e sistemas da DMS Logistics, em qualquer função ou nível hierárquico, são corresponsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários e dos ambientes a que tenham acesso, independente das medidas de segurança implementadas pelos responsáveis da gestão de segurança.

São responsáveis pelos ativos da DMS Logistics:

Gestor de Segurança da Informação

- Acompanhar, supervisionar, orientar e aprovar a configuração dos equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles técnicos necessários para garantir a segurança dos dados, sistemas, ativos e informações pessoais;
- Garantir que todos tenham acesso e conhecimento desta Política e demais normas e padrões de Segurança da Informação.
- Fiscalizar os procedimentos previstos nesta Política.

Colaboradores

- Cumprir e zelar pela materialização e realização eficaz desta Política;
- Notificar o Gestor de Segurança da Informação em caso de perda, roubo, uso inapropriado de ativos, dados, informações, equipamentos ou descumprimento das disposições desta Política.

4.2. CONTROLE DE ACESSO

O acesso aos sistemas da DMS Logistics é controlado e concedido apenas a colaboradores e visitantes autorizados.

As autorizações de acesso devem ser concedidas com base nos princípios da necessidade de conhecer (need to know) e privilégios mínimos (least privilege) para o desempenho das atividades profissionais.

Os Dirigentes, colaboradores e terceiros são responsáveis pelo uso e sigilo de suas credenciais de acesso. Não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta e/ou dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

O acesso pode ser monitorado, registrado ou bloqueado sem prévio aviso.

4.3. PROPRIEDADE E USO DE ATIVOS

Todo dado, código e informação coletada, criada, tratada e armazenada, seja em ambiente cloud ou em dispositivos físicos, são de propriedade da DMS Logistics.

O uso dos ativos da DMS Logistics é direcionado para a execução dos objetivos de negócio da empresa. Os equipamentos, dados e informações devem ser utilizados apenas para esse fim, sendo expressamente vedado o uso de dados e informações pessoais, sejam de colaboradores, clientes ou terceiros para outros fins.

É permitido o acesso à Internet, de acordo com regras específicas, tratadas em tópico próprio nesta Política. Ela estabelece as regras para o seu acesso e uso no ambiente corporativo.

4.4. DIRETRIZES SOBRE O USO DE ATIVOS

A instalação de equipamentos, recursos computacionais, sistemas e serviços para uso na rede ou nas dependências do DMS Logistics é controlada é permitida mediante autorização formal, concedida pelo gestor de Segurança da Informação.

- A DMS Logistics poderá implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexão com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderão ser usadas para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Todos os sistemas são acessados mediante autenticação. Cada usuário deve estar devidamente identificado por uma identidade única e intransferível, possibilitando que seja vinculado e responsabilizado por seus atos dentro da organização. Para acessar o sistema, deve ser feita uma solicitação para o departamento de Segurança da Informação. Apenas após a autorização e liberação pelo departamento de Segurança da Informação, será possível acessar o Sistema DMS Logistics.

- Cada usuário deve estar devidamente identificado por uma identidade única e intransferível, possibilitando que seja vinculado e responsabilizado por seus atos dentro da organização.

- Cabe ao usuário assegurar que seu ID e senha não sejam utilizados por terceiros, impedindo que estes sejam utilizados para a obtenção de acesso não autorizado aos sistemas da DMS Logistics.

Garantir que os dispositivos de sua responsabilidade estejam devidamente bloqueados durante sua ausência. Os equipamentos serão bloqueados após uma inatividade de 10 minutos. Entretanto, sempre que o usuário se ausentar de sua estação de trabalho, ela deverá ser bloqueada;

Não deixar à mostra login e senha;

As senhas não devem ser deixadas em notas adesivas coladas no computador ou embaixo dele, nem podem ser deixadas escritas em local acessível;

As senhas de acesso devem ser fortes;

As senhas não devem ser armazenadas em texto puro;

O recurso de duplo fator de autenticação (MFA) deve ser utilizado.

- Não é permitida a instalação e execução de softwares não autorizados.

Todos os computadores seguem uma configuração padrão de segurança. Se for necessária alguma alteração, ela deverá ser avaliada e autorizada pelo Gestor de SI.

As senhas padrão deverão ser alteradas após a instalação dos softwares.

Não emprestar ou compartilhar, em nenhuma hipótese, suas credenciais de acesso. Dar acesso a terceiros não autorizados pelo Gestor de SI é terminantemente proibido. Os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis tanto o titular das credenciais quanto aquele que as utilizar indevidamente.

Dispositivos externos, quando conectados à rede da DMS Logistics, devem ser primeiramente autorizados pelo Gestor de SI antes de serem conectados.

Os usuários devem estar classificados em um grupo de privilégio, com acesso somente às funcionalidades necessárias para a execução do seu trabalho, com base nos princípios da necessidade de conhecer (need to know) e privilégios mínimos (least privilege).

Todas as permissões e métodos de acesso devem ser solicitados via ticket aberto e registrado no Jira, e previamente analisados e autorizados pela equipe da DMS Logistics Tecnologia.

Os usuários devem estar atentos antes de abrirem anexos enviados por e-mail, especialmente aqueles promocionais ou enviados por desconhecidos.

4.5. USO DA INTERNET

O uso do serviço de Internet deve estar em conformidade com perfis pré definidos, respeitando o armazenamento das informações e sua autenticidade.

Os serviços corporativos de correio eletrônico, mensagens instantâneas, Intranet e Internet devem ter seu uso orientado para as atividades de interesse do DMS Logistics.

Os colaboradores e visitantes autorizados poderão usar a conexão de internet para:

- Realizar tarefas de trabalho
- Fazer pesquisas e coletar informações que possam melhorar seu trabalho

4.6. PERFIS DE ACESSO À INTERNET

Os colaboradores e visitantes que utilizarem a conexão da DMS Logistics deverão acessar o Sistema com suas contas corporativas com o uso de dispositivos seguros e autorizados.

Deve-se utilizar sempre senhas fortes, com o uso de letras, números e caracteres especiais.

Ficam estabelecidos os seguintes perfis para o acesso à Internet:

Padrão: Permite o acesso a todos os sites da Internet, inclusive os que veiculam material contendo áudio e vídeo, redes sociais e blogs.

Todos os colaboradores da DMS Logistics, aprendizes e estagiários devem ser cadastrados no perfil "Padrão".

Investigação: Permite o acesso irrestrito, em caráter temporário, a todos os sites da Internet. O perfil "Investigação" poderá ser atribuído a um colaborador por ato formal para atuação em processos de Tratamento e Resposta a Incidentes em Redes Computacionais.

- O relatório dos acessos deverá constar do documento que compõe o resultado do processo investigativo.
- O prazo de vigência da atribuição deste perfil será o mesmo definido para a conclusão do processo investigativo.

4.7. RESTRIÇÕES E CONDUTAS

É proibido a todos os perfis de acesso, exceto para o perfil "Investigação", o acesso e navegação a:

- Sites que contenham material pornográfico ou obsceno;
- Sites que contenham material ilegal;
- Sites de jogos;
- Sites que representem risco à Segurança da Informação.

Ficam vedadas as seguintes condutas quando da utilização da Internet:

- Envolver-se em atividades que contrariem os interesses da DMS Logistics, que violem suas Políticas ou a legislação vigente no País;
- Praticar atos de comercialização de produtos, em proveito próprio ou de terceiros, que não sejam de interesse da DMS Logistics;
- Violar direitos pessoais, autorais e/ou intelectuais, revelar segredos industriais e/ou comerciais, fazer cópia ou divulgar código-fonte, violar patentes, instalar ou distribuir softwares "piratas" ou outros que não estejam licenciados para uso legal pela DMS Logistics;
- Copiar, utilizar, compartilhar ou divulgar dados pessoais de colaboradores, stakeholders sem expressa autorização da DMS Logistics;
- Praticar atos de invasão de contas e dispositivos de terceiros, sejam pessoas físicas ou jurídicas;

- Utilizar os ativos da DMS Logistics para envolvimento em atividades criminosas, como hackeamento ilegal, fraude, compra/venda de bens e serviços ilegais, prática de terrorismo, pornografia, pedofilia ou participação em movimentos religiosos, políticos ou de qualquer viés extremista;
- Valer-se de recursos ou dispositivos para acesso a computadores ou redes externas à DMS Logistics com o objetivo de obter informações não autorizadas ou provocar a interrupção ou a degradação de serviços de rede;
- Utilizar modem ou dispositivo de rede que interligue a rede interna da DMS Logistics a outras redes ou à Internet;
- Visitar websites potencialmente perigosos que possam comprometer os dispositivos ou acesso à rede;
- Baixar arquivos ou programas da Internet que contrariem as diretrizes desta ou das demais Políticas da DMS Logistics.
- Baixar filmes, músicas, revistas, livros, softwares e outros materiais que sejam objeto de direitos autorais de terceiros.
- Ademais, é proibido aos colaboradores o uso do correio eletrônico da DMS Logistics para as seguintes atividades:
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Empresa;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o DMS Logistics ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do DMS Logistics estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do DMS Logistics;

- Contenham ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- Tenha conteúdo considerado impróprio, obsceno ou ilegal.

É vedado:

- Instalar ou remover softwares dos equipamentos da DMS Logistics sem prévia autorização do Gestor de SI;
- Impedir ou desativar qualquer atualização dos softwares ou hardwares recomendada pela equipe de Segurança da Informação;
- Instalar, desinstalar ou desabilitar qualquer software ou hardware, tornando-o total ou parcialmente inoperante;
- Realizar qualquer tipo de manutenção nos equipamentos do escritório sem o auxílio da área responsável;
- Alterar as configurações de rede e do Sistema Integrado de Entrada e Saída - BIOS das máquinas, bem como realizar qualquer alteração que possa causar algum dano futuro;
- Comprometer equipamento pertencente à DMS Logistics, por uso inadequado ou de forma intencional;
- Tornar vulnerável a segurança dos ativos de informática portáteis, entre eles, HD externo, notebook, data show, pen drive;

- Tomar qualquer conduta que comprometa a segurança da rede ou de equipamentos de informática da DMS Logistics;
- Falsificar endereços e/ou contas de login com objetivo de se ocultar dos sistemas de segurança da DMS Logistics;
- Obter acesso não autorizado a qualquer servidor, rede ou conta, burlando os sistemas de segurança, a fim de conseguir acesso ou privilégios indevidos;
- Compartilhar, sem prévia autorização, documentos ou arquivos com terceiros;
- Impedir o funcionamento pleno e adequado dos ativos por meio da alteração de parâmetros e configurações dos softwares;
- Utilizar ou propagar softwares como vírus, cavalos de tróia, keyloggers, ou programas que controlem outros computadores através dos recursos disponibilizados pela DMS Logistics.

4.8. MONITORAMENTO

Para garantir as regras mencionadas nesta Política, a DMS Logistics. se reserva no direito de:

- Implantar sistemas de monitoramento nos dispositivos corporativos, correio eletrônico, conexões à Internet e outros componentes da rede. A informação gerada por estes sistemas de monitoramento pode ser usada para identificar usuários e respectivos acessos efetuados;
- Inspecionar arquivos que estejam na rede interna ou no dispositivo corporativo, visando assegurar o rígido cumprimento desta Política.

A rotina de verificação de aplicação dos protocolos previstos nesta política e naqueles presentes na de segurança da informação, ocorrerá semestralmente envolvendo as pessoas e organizações vinculadas a DMS Logistics, por meio de disponibilização de assinatura de termos vinculantes e treinamentos, entre outras medidas adequadas.

Ao fazer uso dos ativos fornecidos pela DMS Logistics ou agindo em seu nome, os colaboradores concordam com as disposições relacionadas à segurança da informação e documentos correlatos, tendo ciência de que seus atos podem ser monitorados pela área responsável e pelo Gestor de SI.

4.9. EDUCAÇÃO E CONSCIENTIZAÇÃO

Esta Política e seus documentos agregados devem ser divulgados para criar e manter uma cultura corporativa em Segurança da Informação e Comunicações. De forma a reduzir os riscos à segurança da informação, todos os colaboradores devem ser informados quanto ao uso adequado e seguro dos recursos

tecnológicos e das informações do DMS Logistics a que tenham acesso.

É responsabilidade dos colaboradores, estagiários e jovens aprendizes conhecer e cumprir as diretrizes, regras e ações definidas por esta Política, assim como pelas suas normas e procedimentos agregados.

4.10. VIOLAÇÕES E PENALIDADES

O não cumprimento dos princípios e diretrizes desta Política, suas normas e procedimentos agregados, sujeita o infrator às penalidades previstas em lei e nos regulamentos internos do DMS Logistics.

4.11. ATUALIZAÇÃO

A Política de Uso de Ativos deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

5. ANEXO A - NORMAS DE USO DE DISPOSITIVOS MÓVEIS (BYOD)

Dispositivos móveis como smartphones, tablets e computadores são importantes ferramentas para a DMS Logistics em suas atividades corporativas. Contudo, podem representar um risco significativo para a segurança de dados quando, sem a adoção de aplicativos e procedimentos de segurança, são usados como canal de acesso não autorizado aos dados da empresa e à sua infraestrutura de tecnologia. Isso pode levar a vazamento de dados e infecção dos sistemas.

Por isso, a DMS Logistics possui requisitos para proteger seus recursos de tecnologia da informação, visando proteger seus clientes, sua propriedade intelectual e sua reputação. Este documento estabelece uma série de práticas para o uso seguro de dispositivos móveis e aplicativos.

5.1. ESCOPO

Esta normativa aplica-se a:

- Todos os ambientes físicos, incluindo-se a sede, filiais, unidades regionais, unidades de desenvolvimento, centros de processamento e quaisquer outros pertencentes ao patrimônio ou sob a custódia da DMS Logistics.
- Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela DMS Logistics;
- Todos os empregados, estagiários, jovens aprendizes e colaboradores de qualquer natureza jurídica do DMS Logistics.
- Todos os dispositivos móveis, sejam propriedades do DMS Logistics ou de

seus colaboradores, inclusive smartphones, tablets e computadores que tenham acesso às redes, dados e sistemas da companhia. A lista inclui, mas não se limita, a:

A. Desktops, notebooks, tablets;

B. Smartphones;

C. Cartões de memória, pen-drives;

D. HDs externos.

- Aplicativos utilizados por colaboradores em seus dispositivos móveis pessoais que armazenem ou acessem dados corporativos, como aplicativos de armazenamento em nuvem, de comunicação e mensagens instantâneas.

5.2. USO DE DISPOSITIVOS MÓVEIS

A DMS Logistics não fornece dispositivos móveis tais como celulares e tablets aos seus colaboradores. O modelo adotado para essa situação é o BYOD (Bring Your Own Device). No entanto, autorizamos o uso dos aplicativos que abaixo estão relacionados, com o devido monitoramento e auditoria, sem, entretanto, violar a privacidade da pessoa física dos nossos colaboradores, seguindo as orientações da Lei n° 12.965/2014 (Marco Civil da Internet). Seu uso deve estar em consonância com:

- A Política de Segurança da Informação da DMS Logistics;
- Contrato de Confidencialidade assinado pelo colaborador;

Regras para BYOD - Bring Your Own Device

Antes de seu primeiro uso em qualquer rede ou infraestrutura de TI do DMS Logistics, todo dispositivo móvel deverá ser registrado com a Equipe de SI. A DMS Logistics manterá uma lista de todos os dispositivos aprovados para uso.

Dispositivos que não estejam registrados e aprovados não poderão ser conectados à infraestrutura de tecnologia da companhia. Se o dispositivo preferencial de algum usuário não estiver na lista, deverá ser solicitada sua inclusão à Equipe de SI.

A conectividade de todos os dispositivos móveis será gerenciada pela Equipe de SI da DMS Logistics. Embora a equipe não seja capaz de monitorar todos os dispositivos externos - como notebooks, tablets ou smartphones pessoais - que possam necessitar de conectividade com as redes da companhia, espera-se que os usuários adotem os mesmos protocolos de segurança

quando utilizarem dispositivos que não sejam propriedade da DMS Logistics.

5.3. REQUISITOS TÉCNICOS

- Os dispositivos deverão utilizar os sistemas operacionais mais atualizados, para garantir que tenham atualizações de segurança mais recentes;
- Os dispositivos devem armazenar todas as senhas salvas pelo usuário em uma ferramenta de criptografia de senhas;
- Os dispositivos devem ser configurados com senhas seguras e que estejam de acordo com as instruções de segurança para senhas. As senhas não poderão ser as mesmas utilizadas em outras credenciais dentro da empresa;
- Apenas dispositivos autorizados pela Equipe de TI terão permissão para se conectar diretamente à rede interna corporativa.
- Os dispositivos estarão sujeitos às regras de compliance em relação a questões de segurança, como criptografia e senhas, estabelecidas pela Equipe de TI.

5.4. REQUISITOS DE USUÁRIO

- Usuários devem fazer upload em seus dispositivos apenas de dados que sejam essenciais para sua atividade corporativa;
- Se o usuário suspeitar de acesso não autorizado a dados da companhia através de seus dispositivos móveis, deverá reportar o incidente imediatamente à Equipe de TI, de acordo com os procedimentos estabelecidos;
- Usuários não devem instalar softwares pirateados ou conteúdo ilegal em seus dispositivos;
- Aplicativos devem ser provenientes apenas de fontes e plataformas oficiais. Se houver dúvida se um aplicativo provém de uma fonte confiável, o usuário deverá entrar em contato com a Equipe de TI.
- Os usuários devem checar semanalmente e atualizar ao menos uma vez por mês os sistemas e aplicativos em seus dispositivos.
- Os dispositivos não devem ser conectados a computadores que não possuam anti malwares atualizados e habilitados, ou que não cumpram os requisitos da DMS Logistics.
- Os dispositivos devem estar criptografados de acordo com os padrões da

companhia.

- Usuários devem ser cautelosos ao utilizar em conjunto contas pessoais e corporativas em seus dispositivos. Devem garantir que dados da companhia sejam enviados apenas através de e-mail corporativo.
- Todos os usuários devem garantir medidas de segurança física dos dispositivos, enquanto se encontram em sua posse e enquanto estiverem longe de seu alcance momentaneamente.

Os requerimentos acima poderão ser checados regularmente e se qualquer dispositivo não estiver de acordo com o estabelecido, poderá resultar em perda de acessos a ferramentas e redes da empresa, assim como limpeza dos dados corporativos dentro dos dispositivos.

Usuários não devem tentar modificar ou desabilitar as configurações de segurança aplicadas pela Equipe de TI para o uso do dispositivo

A Equipe de SI se reserva o direito de recusar a conexão de qualquer dispositivo móvel às redes e infraestrutura de tecnologia da DMS Logistics. Essa medida será adotada sempre que a Equipe de TI perceber que os dispositivos estão sendo utilizados de maneira a colocar os sistemas, usuários, dados e clientes em risco.

Casos não contemplados no presente documento serão submetidos a avaliação de risco e ao Comitê Gestor de Segurança da Informação da DMS Logistics.

5.5. FERRAMENTAS CORPORATIVAS COM USO PERMITIDO NOS DISPOSITIVOS MÓVEIS DOS COLABORADORES:

- GSuite
- Discord
- WhatsApp

5.6. GSUITE

- Suíte de ferramentas corporativas do Google.
- Gmail - E-mail corporativo
- Drive - Armazenamento e compartilhamento de arquivos
- Hangouts / Meet - Vídeo Conferências (Reuniões Virtuais)
- Calendar - Agenda de Compromissos ativos

Em caso de roubo e/ou perda do dispositivo móvel do colaborador, o departamento

de segurança da informação é acionado, e um dos membros deste departamento irá remover os dados dos dispositivos móveis do funcionário.

Ressaltam-se que apenas dados da DMS Logistics contidos nos aplicativos GSuite serão apagados. Mais informações em https://support.google.com/a/answer/7542661?hl=pt-BR.

Outra ação tomada imediatamente neste tipo de incidente será o reset da senha do e-mail corporativo. O colaborador deverá cadastrar uma nova senha e reconfigurar o mecanismo do MFA (Multi-Factor Authentication). O MFA é mandatório para todos os e-mails corporativos da DMS Logistics.

Abaixo as evidências do processo de administração remota dos recursos do GSuite da DMS Logistics:

EVIDÊNCIAS SOLICITADAS A DMS LOGISTICS EM 15/02/2023 .

5.7. DISCORD

O Discord é utilizado pelos colaboradores para a comunicação geral entre os times, sem o tráfego de dados sensíveis.

5.8. WHATSAPP

Todos dos colaboradores passaram por Workshops de Segurança da Informação, onde foi instruído e orientado individualmente como manter seu WhatsApp mais seguro, seguindo as diretivas de segurança do WhatsApp (https://faq.whatsapp.com/pt_br/general/26000245), como:

- Ativação do código de confirmação em duas etapas para adicionar uma camada extra de segurança à sua conta.
- Definir um endereço de e-mail autêntico para reduzir o risco de ficar sem acesso à sua conta, caso você esqueça seu PIN (https://faq.whatsapp.com/pt_br/general/26000021).
- Nunca compartilhar o código de confirmação de seis dígitos com ninguém, nem com pessoas que você conhece ou organizações nas quais confia.
- Definir um PIN para proteger seu celular.

O Whatsapp é um meio de comunicação dos funcionários da DMS Logistics e em caso de perda ou roubo do dispositivo móvel do colaborador, o mesmo é removido temporariamente dos grupos de WhatsApp que ele faça parte que possuam algum vínculo com o DMS Logistics..

5.9. IMPLEMENTAÇÃO E ATUALIZAÇÃO

Esta normativa deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

6. DISPOSIÇÕES FINAIS

Para a DMS Logistics , a privacidade e confiança são fundamentais para a nossa relação com você. Estamos sempre nos atualizando para manter os mais altos padrões de segurança.

Por isso, nossa Política de Uso Aceitável de Ativos pode ser alterada a qualquer tempo. Assim, deve-se estar atento quanto às atualizações publicadas.

Ao continuar com a utilização de ativos, você concorda com a nossa Política de Uso Aceitável de Ativos.

Em caso de dúvidas, entre em contato conosco pelo canal: (email)

Esta Política de Uso Aceitável de Ativos foi atualizada pela última vez em 28 de fevereiro de 2023.

7. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	28/02/2023	Emissão do documento.
01	13/03/2023	Revisão e padronização do documento.

8. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	CyberSecurity Team	
Revisado por:	Leonardo Sabbadim	
Aprovador por:	Victor Gonzaga	
Nível de Confidencialidade:	X	**Informação Pública**
		Informação Interna
		Informação Confidencial
		Informação Sigilosa

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

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM