Políticas de Segurança e Informação

GRUPO MUFFATO

Índice

1. Apresentação

Prezando pela transparência e confiança daqueles que possuem qualquer relação com o **Grupo Muffato**, implementamos a **Política de Segurança e Informação** para assegurar a proteção dos dados de nossos usuários, buscando zelar para que a experiência com a nossa empresa seja cada dia mais eficaz, bem como alinhar os procedimentos de utilização de informações com o código de ética do Grupo.

Temos por objetivo padronizar o processamento das informações interligadas na empresa, com o compromisso de garantir que cada procedimento seja realizado de forma adequada e segura.

2. Conceitos

Pensando em proporcionar uma leitura clara e objetiva, apresentamos a seguir os termos utilizados para os responsáveis e envolvidos pelo processamento dos seus dados:

DPO (Diretor de Proteção de Dados): profissional indicado para se responsabilizar pela proteção de dados na organização, zelando pela segurança das informações e atuando como canal de comunicação entre o usuário e a empresa.

Titular: qualquer pessoa natural que tenha seus dados pessoais tratados, como por exemplo, clientes, colaboradores e fornecedores.

Vale ressaltar que o Grupo Muffato realiza a coleta de dados apenas de indivíduos maiores de 18 anos, informações de crianças e adolescentes não fazem parte do nosso banco de dados.

Controlador: pessoa física ou jurídica de direito público ou privado que realizada o monitoramento e processamento dos dados.

Dado Pessoal: toda informação direta que possui ligação com a pessoa física, como por exemplo, documentos de identificação pessoais e eletrônicos, endereços etc.

Agentes de Tratamento: os Controladores e Operadores que, em conjunto, são denominados "Agentes de Tratamento". O "Controlador" é a pessoa física ou jurídica, de direito público ou privado, que tomará decisões referentes ao Tratamento de Dados Pessoais, enquanto o "Operador" é a pessoa física ou jurídica, de direito público ou privado, que realiza o Tratamento de dados pessoais em nome ou seguindo as instruções do Controlador.

3. Aplicação

Direta: Todos os colaboradores

Indireta: Usuários interligados ao Grupo Muffato (Fornecedores e Clientes).

4. Disposições gerais

4.1. Generalidades

Tem como responsabilidade preservar a integridade dos dados, garantir sua disponibilidade para as pessoas e os sistemas certos, além de estabelecer a confidencialidade das informações, principalmente das mais críticas para o negócio. A política também deve indicar como os dados são utilizados e descartados após perderem sua relevância para as empresas e os controles e proteções requeridos.

A adoção da Política de Segurança da Informação visa minimizar os riscos de falhas, danos e prejuízos que possam comprometer o Grupo Muffato.

As informações são analisadas e revisadas criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias, e após isso são repassadas a todos os colaboradores.

Todos os colaboradores deverão conhecer a Política de Segurança da Informação. A anuência quanto ao conteúdo se dá após a leitura e entendimento das diretrizes e assinatura individual do Termo de Aceite.
Os documentos referentes à Política de Segurança da Informação estão disponíveis no departamento de LGPD, bem como há uma cópia em cada loja da empresa para eventuais consultas.

A Política de Segurança da Informação foi elaborada em alinhamento com o Código de Ética do Grupo Muffato.

5. Comitê de Segurança da Informação

5.1. O Comitê de LGPD do Grupo Muffato possui as seguintes atribuições:

- Atualizar a norma corporativa de segurança da informação.
- Deliberar sobre assuntos relacionados à segurança da informação.
- Deliberar sobre comunicações e treinamentos no âmbito da segurança da informação.
- Mapear e implementar controles para a mitigação de riscos relacionados à segurança da informação.

5.2. O Comitê será composto pelos ocupantes dos seguintes cargos:

- Diretor Administrativo
- DPO
- Gerência Jurídica
- Gerência de TI
- Gerência de Marketing
- Gerência de E-commerce

As reuniões do comitê acontecerão semanalmente, ou sem prejuízo de reuniões extraordinárias quando houver necessidade.

6. Base legal para o processamento dos dados

A lei nos permite realizar a coleta de dados desde que o usuário dê o aceite ao consentimento. Logo, se os seus dados estão sendo tratados pelo Grupo Muffato, é provável que em algum momento suas informações tenham sido inseridas em nossa rede através de formulários de cadastros nas lojas, Shopfato, Max, ClubeFato, Delivery, Crediffato, Auto Posto Super Muffato e Conexão à rede wi-fi.

Recolhemos apenas as informações essenciais, sendo elas:

- Dados pessoais (nome, endereço, e-mail e telefone);
- Preferência de contato;
- Pesquisa de dados nos sites do Muffato.

Qualquer dúvida sobre o processamento de dados realizado pela empresa pode ser esclarecida em nosso site:

www.supermuffato.com.br/lgpd-lei-geral-de-protecao-de-dados

7. Comunicação e Transparência

Atendendo à necessidade de nossos usuários e clientes de exercerem seus direitos em relação às suas informações pessoais, bem como sanar suas dúvidas sobre como usamos suas informações pessoais, disponibilizamos a seguir o contato do nosso encarregado de Dados:

Encarregado de Dados (DPO): Marcelo Machado de Paiva

Contato: dpo@grupomuffato.com.br

7.1. Compartilhamento de dados

Nós partilhamos as informações quando necessário, a fim de proporcionar aos nossos usuários uma experiência mais eficaz na utilização dos serviços fornecidos pela empresa. **Seus dados serão compartilhados apenas nos seguintes casos:**

- Hospedagem de páginas Web;
- Serviços de e-mail de marketing;
- Concursos e promoções;
- Auditoria;

- Análise de dados;
- Serviços de apoio ao cliente;
- Relatórios de satisfação dos clientes e para fins de pesquisas.

Asseguramos que nossos parceiros e afiliados estão empenhados na garantia de proteção de dados e quaisquer informações pertinentes

8. Uso do correio eletrônico e redes Sociais

Serviço de uso permitido: ferramenta de e-mail padrão corporativo pacote office 365. O conjunto de ferramentas fornecidas pelo Grupo Muffato deve ser utilizado exclusivamente para as atividades profissionais e corporativas durante jornada pré estabelecida em contrato de trabalho.

Em caso de acesso remoto, o controle será feito por meio de usuário e senha. A solicitação de acesso ao correio eletrônico deverá ser realizada por meio de chamado técnico via Central de Serviços de TI.

Quando houver o desligamento, o TI é comunicado e realiza o cancelamento da caixa de e-mail.

8.1. Criação de caixa de e-mail temporária:

Do endereçamento aos Grupos de Usuários, os seguintes cuidados devem ser tomados:

• As mensagens devem ser objetivas e o conteúdo relevante para todos os destinatários;

• O remetente da mensagem deve avaliar criteriosamente quais grupos pode incluir no endereçamento e conhecer a composição de cada um;

• Não será permitido manter ativas as caixas postais de colaboradores desligados do Grupo;

• Se necessário, o baackup da caixa postal de colaboradores desligados deverá ser solicitado via chamado à TI, sempre com a aprovação da gerência responsável;

• O tempo para a retenção de informações das caixas de e-mail é de 05 anos para usuários ativos e de 90 dias para usuários desligados ou excluídos, sendo a política de retenção aplicada para todos os domínios, não sendo possível a aplicação em tempo diferente por domínio;

• O acesso ao correio eletrônico deve ser feito pelo Office 365;

• A recomendação de armazenamento da caixa de e-mail depende da licença aplicada do usuário, podendo ser o armazenamento nos tamanhos E1 (de 50 GB), E3 (de 100 GB), E5 (de 100 GB) e F3 (de 2 GB).

Fica a critério do colaborador excluir as mensagens que não forem mais necessárias, porém, deve-se ter ciência de que o armazenamento dos e-mails é local no computador, portanto, não é possível recuperar tais arquivos em caso de problemas no HD ou de arquivos corrompidos;

• É de responsabilidade do colaborador gerenciar a sua pasta de Lixo eletrônico (spams);

• As assinaturas de correio eletrônico devem obrigatoriamente respeitar os modelos oficiais;

• Não é permitido utilizar o e-mail corporativo para o envio de e-mails em massa, que ultrapassem o número de 30 e-mails por minuto, sendo o tamanho máximo do e-mail de 35 MB. Em caso de necessidade do envio para divulgação ou publicidade das entidades, deve ser utilizada ferramenta própria para marketing. Essa ação visa tratar a inserção dos domínios Grupo Muffato em listas negras dos provedores de internet e pode prejudicar a utilização e causar interrupção dos serviços de e-mail por longos períodos;

• Todas as caixas de e-mail do Grupo Muffato podem ser auditadas a qualquer momento sem aviso prévio, após a solicitação do setor de auditoria e do gerente de TI.

9. Critério de utilização de redes sociais

As mídias sociais são ferramentas que auxiliam o Grupo Muffato a divulgar os seus serviços e promover cooperação com os clientes, colegas e com o mundo em geral.

Os colaboradores devem utilizar as mídias sociais de forma adequada, pois todas as mensagens publicadas no ambiente da rede corporativa estão diretas ou indiretamente ligadas ao nome do Grupo Muffato. Assim, os colaboradores devem respeitar os seguintes princípios:

- Mantenha-se na sua área de especialização e forneça uma perspectiva individual exclusiva sobre o que está acontecendo no Grupo Muffato e no mundo;

- Divulgue comentários respeitosos e significativos, evitando spams, comentários ofensivos e não relacionados ao tema;

- Sempre pare e pense antes de postar. Considerando isso, responda aos comentários de forma oportuna, e quando for apropriado;

- Respeite informações, conteúdos proprietários e confidencialidade;

- Quando não concordar com a opinião de outras pessoas, seja educado;

- Siga o Código de Ética do Grupo Muffato;

O colaborador não possuirá autorização para acesso às contas das mídias sociais que representam as instituições em caso de desvinculação do quadro de colaboradores do Grupo Muffato, ficando sob a responsabilidade da área de Marketing a gestão dos acessos.

O colaborador é responsável por proteger a boa imagem, o bom nome e a boa reputação da empresa, bem como, a dos colegas que nela trabalham. Assim, serão repudiadas as postagens em redes sociais com conteúdo que desqualifique, constranja ou ofenda a empresa e/ou qualquer pessoa a ela vinculada.

Não é permitido o uso dos serviços disponibilizados para:

- Denúncias ou campanhas contra pessoas, autoridades constituídas, empresas, entidades, organizações e os poderes constitucionais;

- Anúncios de compra e venda de produtos e serviços pessoais;

- Propaganda de atividades pessoais e de participação em eventos socioculturais;

- Atividades de caráter político-partidário;

- Divulgação de mensagens de utilidade pública, feitas por colaboradores sem atribuição para tal;

- Mensagens de autoajuda ou de cunho religioso;

• Listas de adesão ou de manifestação de solidariedade, exceto as autorizadas pela do Grupo Muffato;

• Transportar arquivos de som e vídeo (MP3, MPEG etc.) exceto quando estes atenderem às necessidades de serviço;

• Mensagens sobre datas comemorativas, festividades e celebrações em geral, exceto as autorizadas pela Direção do Grupo Muffato;

• Transmissão, recebimento e/ou armazenamento de mensagens contendo programas de computador que possam ser considerados nocivos ao ambiente de rede do Grupo Muffato;

• Correntes e pirâmides que circulam na Internet, quaisquer que sejam suas finalidades;

• Envio, transmissão ou distribuição para endereços externos ao Grupo Muffato de informações de propriedade das instituições, tais como, mensagens internas, confidenciais, dados, segredos comerciais, financeiros ou tecnológicos, a não ser que expressamente autorizado pelo superior;

• Violação do Código de Ética do Grupo Muffato;

• Veiculação de conteúdo ilícito como pedofilia, apologia às drogas e terrorismo;

• Veiculação de conteúdo pornográfico.

Além da relação acima, qualquer tipo de conteúdo sem vinculação estrita às atividades profissionais.

10. Acesso e uso da internet Acesso externo seguro (VPN)

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a registro e monitoramento em total conformidade legal.

• Todas as solicitações de acesso à internet, inclusão e retirada de sites do perfil de acesso deverão ser solicitadas obrigatoriamente por meio do sistema de chamados e aprovados pelo gestor do solicitante.

• Os colaboradores não poderão em hipótese alguma utilizar os recursos do Grupo Muffato para fazer o download ou a distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

• Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao Grupo Muffato ou de dados de sua propriedade aos seus parceiros e clientes sem expressa autorização do responsável pelo software ou pelos dados.

• Os colaboradores não poderão utilizar os recursos do Grupo Muffato para deliberadamente propagar qualquer tipo de vírus, cavalo de troia, spam, assédio ou perturbação.

• Para garantir a segurança e a integridade dos serviços, não é permitida a utilização de acessos secundários à Internet (ADSL, 3G, 4G e cable modem, entre outros), em equipamentos conectados à rede do Grupo Muffato, sem o conhecimento e a autorização formal de uso emitida pelo setor Tecnologia da Informação via chamado aprovado pelo gestor.

As solicitações de mudanças do grupo de acesso à internet deverão ser solicitadas para o TI, após a aprovação conforme tabela de alçada vigente por meio do sistema de chamados;

10.1. Solicitação de acesso

• Todo colaborador, quando cadastrado na rede, recebe o acesso à internet.

• Toda solicitação de cadastramento ou mudança de perfil de acesso à Internet deverá ser realizada por meio de chamado técnico via Central de Serviços de TI.

É necessária a aprovação do Gerente da área para a liberação dos seguintes serviços:

• Acesso a sites bloqueados;
• Acesso às portas específicas;
• Serviços de comunicação;
• Serviço de File Transfer Protocol (FTP);

O colaborador deverá abrir um chamado junto ao sistema de chamados e aguardar a aprovação do Gerente de área. Após a aprovação, o chamado será direcionado à TI, que irá analisar a solicitação e liberar o acesso, caso não traga nenhum risco a organização.

• A exclusão do colaborador da internet é realizada pela Tecnologia da Informação, de forma automática mediante o desligamento do colaborador do Grupo Muffato. Em caso de transferências de áreas, a solicitação deve vir através de comunicação recebida pelo Recursos Humanos ou por chamado, realizada pelo próprio setor do colaborador.

• É de responsabilidade do superior direto a solicitação de exclusão do acesso à Internet de um colaborador, seja ele colaborador por prazo determinado, indeterminado ou terceiro. A solicitação de exclusão deverá ser realizada através do sistema de chamados.

• O acesso à internet para visitantes externos utilizando os recursos corporativos é concedido mediante a solicitação e autorização da área ou unidade do Grupo Muffato.

• Os recursos de VPN serão utilizados somente para acessos externos, ou seja, quando o colaborador estiver fora da rede do Grupo Muffato.

• A liberação do acesso externo aos recursos corporativos do Grupo Muffato está habilitada aos colaboradores e terceiros prestadores de serviços ao Grupo Muffato.

• Todas as liberações de acesso ao VPN obrigatoriamente deverão ser solicitadas via chamado pelo sistema de chamados e, posteriormente, deverão ser aprovadas pelo gestor do colaborador solicitante ou do gestor do contrato.

• A TI realizará a liberação do acesso ao colaborador ou terceiro somente após as devidas aprovações.

Quando solicitado o acesso ao VPN de terceiros prestadores de serviços, obrigatoriamente deverá ser informada a data de início e término do acesso, sendo que se necessário por mais de 30 dias, o solicitante deverá solicitar a prorrogação de acesso à TI via chamado, informando a data inicial e final.

O uso dos recursos da VPN deverá ser utilizado para fins estritamente profissionais, de forma a cumprir as normas e procedimentos de segurança, ficando sob responsabilidade do colaborador a utilização adequada dos recursos de VPN.

10.2. Controle de acesso aos dados

O controle de acesso visa garantir a proteção das informações dos serviços do Grupo Muffato e Terceiros autorizados. Para fins de rastreabilidade, o controle de acesso deve prever a identificação do colaborador, local, data e horário de acesso.

É de responsabilidade do gestor da área controlar todos os acessos aos sistemas de informação disponíveis do Grupo Muffato, indicando por meio de chamado qualquer necessidade de alteração, exclusão ou mudança de função.

Todo colaborador deverá possuir conta de acesso lógico com as seguintes regras:

- Colaborador: nome.último sobrenome;

- Colaboradores homônimos: último sobrenome.nome
- Terceiro: nome. último sobrenome.nome da empresa;

- Terceiros homônimos: nome da empresa.nome. último sobrenome;

- Administradores de domínios: admin. último sobrenome;

- Usuários de serviços de sistemas: nome do sistema.service;

- Para cadastramento de contas de terceiros e visitantes, o responsável deverá gerar chamado técnico por meio da Central de Serviços de TI, com as seguintes informações: nome completo, empresa, Cidade, CPF, cargo, CNPJ, departamento responsável, número para contato; prazo de validade da conta e grupo de acesso;

- A TI deverá possuir controle da relação das contas de serviço e seus responsáveis.

Para evitar roubo ou deturpação das informações, e para possibilitar rastreabilidade no processo de controle de acesso, é definido que toda senha é pessoal, intransferível e deve ser mantida sob sigilo pelo próprio colaborador. Em caso de situações comprovadas de acesso e manipulação indevida da informação, o colaborador será sujeito a advertência ou medidas disciplinares cabíveis. No início do período de férias, as senhas do colaborador serão expiradas, sendo automaticamente solicitadas novas senhas no seu retorno.

Todos os colaboradores devem se cadastrar e manter atualizados os dados no Sistema de Gestão de Acessos (SGA) para futuras alterações de senhas e desbloqueio de contas de rede e e-mail. O acesso a esse sistema deve ser efetuado por meio do seguinte link: (endereço)

Para reset de senhas de rede e e-mail em caso de expiração ou de bloqueio por excesso de tentativas incorretas, o colaborador deve obrigatoriamente contatar o gestor imediato responsável por solicitar a alteração da senha. Por segurança, a TI não fará a alteração e o desbloqueio desse recurso por telefone. Em casos especiais, as solicitações de reset e alteração de senhas devem ser solicitadas apenas por meio da Central de Serviços de TI.

• Para todos os colaboradores, será obrigatória a troca de senha a cada 45 dias.

• No primeiro acesso, o colaborador deve trocar a senha temporária.

• O login será bloqueado automaticamente após 10 (dez) tentativas de acesso inválidas, ou seja, com a senha errada.

• O período de bloqueio em caso de tentativas de acesso inválidas é de 5(cinco) minutos.

As senhas deverão ter no mínimo 9 dígitos.

• A reutilização de senhas obedecerá ao ciclo mínimo de 24 (vinte e quatro) trocas, ou seja, as últimas vinte e quatro não poderão ser reutilizadas.

• Na criação ou troca de senhas, devem ser adotadas senhas fortes, buscando sempre utilização de senhas complexas que não remetam a informações pessoais e que contenham caracteres especiais, números e letras maiúsculas e minúsculas, dificultando a quebra da senha.

• O acesso lógico externo à rede corporativa é facultado aos colaboradores e terceiros autorizados que estejam fora do local de trabalho (Unidades Corporativas), em horário de expediente, e que necessitem de acesso pela Internet a informações e serviços do Grupo Muffato com fins estritamente profissionais.

• O acesso aos recursos lógicos do Grupo Muffato deverá ser restringido enquanto o colaborador estiver em período de gozo das férias ou em licença.

11. Dispositivos móveis

11.1. Dispositivos móveis de visitantes | Utilização

Dispositivo móvel de visitantes é o equipamento eletrônico móvel de propriedade particular dos visitantes do Grupo Muffato.

Entende-se como visitantes, empresas e pessoas que visitem a unidade corporativa ou as unidades operacionais do Grupo Muffato, por pequenos períodos, de 01(uma) hora até 15(quinze) dias e que não possuam vínculo por meio de contrato firmado direta ou indiretamente com as instituições. Todo aquele que possui vínculo deverá necessariamente receber uma identificação para acesso à rede, deixando de ser visitante e se tornando um colaborador.

Equipamentos de visitantes não devem ser utilizados para fins profissionais, portanto acesso a arquivos e pastas nas unidades de rede não serão autorizados. Para acessar a internet por meio da estrutura tecnológica do Grupo Muffato com dispositivo móvel pessoal, o responsável pelo visitante deve solicitar a aprovação formal do diretor de sua unidade ou área de lotação.

É expressamente proibida a utilização do modem USB 3G do Grupo Muffato em dispositivos móveis de visitantes.

11.2. Dispositivos de armazenamento removíveis | Utilização

Dispositivos de armazenamento removíveis (pendrives, HDs externos, DVDs-RW e cartões de memória, entre outros) são facilitadores de transporte de dados. Todavia, deve-se notar que eles podem se tornar vetores que facilitam desvios de informação e disseminação de vírus, se não forem utilizados com cuidado e idoneidade.

A autorização para a utilização de dispositivos de armazenamento removíveis, bem como a garantia da segurança da informação que será manipulada, é de decisão restrita dos Gerentes de área. Periodicamente, o Comitê de LGPD fará uma análise das liberações desses dispositivos para avaliar se as autorizações estão dentro da normalidade ou se estão aumentando o nível de risco da empresa.

Caso o Comitê identifique algum aumento no risco, deliberará sobre a manutenção ou não do acesso.

A cópia de dados corporativos do grupo Muffato por parte de terceiros, parceiros e visitantes só é permitida com autorização da diretoria da área.

12. Utilização de aparelho celular

Durante o horário de trabalho, os colaboradores devem se dedicar exclusivamente às atividades relacionadas às suas funções e aos negócios do Grupo Muffato, sendo expressamente proibido o uso de telefones e celulares.

A Diretoria poderá autorizar expressamente o uso de aparelhos de celular para determinados colaboradores em razão da função exercida. Contudo, sua utilização deverá ser de forma moderada e sem abusos, de modo a não interferir na realização do trabalho.

Os colaboradores que utilizam seus telefones pessoais para trabalho deverão aceitar e obedecer a todas as políticas de segurança das aplicações da empresa que forem utilizadas, tais como políticas de uso e acesso, restrições de conteúdo e horários de uso, entre outras.

13. Mesa limpa

Recomenda-se aos colaboradores nunca deixar documentos expostos nas mesas. Orienta-se que, sempre que o usuário sair do seu posto de trabalho, guarde os documentos que eventualmente estejam nas mesas para que outros não tenham acesso às informações confidenciais.

14. Usa da rede de comunicação de dados

As solicitações para adição, instalação e manutenção dos recursos de rede de dados deverão ser feitas através de abertura de chamado técnico via Central de Serviços de TI. Tais perfis podem ser modificados com base em justificativa encaminhada via chamado formal pela área interessada à TI.

• Equipamentos de visitantes não poderão ter acesso aos arquivos e pastas corporativas do Grupo Muffato.

• A conexão com a rede wireless está sendo disponibilizada somente dentro das dependências físicas das Unidades do Grupo Muffato e em área delimitada.

• Não é permitida a utilização da (e a conexão à) rede wireless por terceiros (fornecedores ou visitantes).

• O acesso a dados corporativos só será autorizado mediante solicitação via chamado à Central de Serviços de TI, realizada pelo responsável da área/unidade solicitante.

• É vedada a instalação de qualquer equipamento do tipo Access Point, 3G e 4G ou similar em qualquer uma das áreas ou unidades do Grupo Muffato sem o conhecimento e autorização do Comitê de LGPD, que deverá ser obtida através de abertura de chamado técnico via Central de Serviços de TI, quando serão verificadas as seguintes características: funcionalidade, segurança e disponibilidade de recurso.

• Os dados corporativos e de trabalho devem ser armazenados nas unidades compartilhadas da rede, sendo assim possível recuperar os dados perdidos,

• Não é permitido o compartilhamento local do computador.

Durante o processo de manutenção ou auditoria das unidades compartilhadas de rede, a TI providenciará:

• Relação por nome em uma tabela, que será enviada à chefia direta do colaborador;

• Posterior remoção dos arquivos nas unidades compartilhadas, caso não existam justificativas autorizadas.

• A organização em pastas e o gerenciamento das informações armazenadas em compartilhamentos públicos são atribuições de cada diretoria de área ou unidade.

• Os limites definidos de espaço poderão ser alterados para mais ou para menos de acordo com necessidade técnica.

• Alterações individuais de aumento de limites poderão ser solicitadas através da abertura de chamado técnico via Central de Serviços de TI, sendo avaliadas tecnicamente e autorizadas caso não haja restrições sendo limitadas a 5 GB por solicitação.

• As solicitações de acesso à rede deverão ser realizadas por meio de chamado técnico via Portal de chamados da TI.

• Cada departamento possui uma pasta com seu respectivo nome no servidor de arquivos;

• O acesso às pastas e arquivos armazenados na unidade Departamental é liberado apenas aos colaboradores pertencentes ao departamento em questão.

As unidades compartilhadas da rede devem ser utilizadas para armazenamento de dados de fins estritamente profissionais, nos seguintes tipos:

• Apresentações e textos;

• Áudio (MP3, MP4 e WAV, entre outros);

• Imagens (JPG e BMP, entre outras);

• Softwares (aplicativos);

• Vídeos (AVI e MPEG, entre outros).

Para o compartilhamento de arquivos entre setores, existe uma pasta na rede interna chamada Público, a qual apenas os colaboradores do grupo possuem acesso.

O acesso às pastas e arquivos armazenados na unidade Compartilhado é liberado mediante solicitação via chamado no Portal de chamados da TI. Essa solicitação deve ser aprovada pelo(s) gestor(es) responsáveis pela pasta. Caso seja necessária a criação de uma nova pasta na unidade Compartilhado, o solicitante deverá informar os colaboradores que terão acesso, e o(s) gestor(es) responsáveis pela pasta, na solicitação via portal de chamados da TI.

Arquivos gravados na pasta Público podem ser acessados por qualquer pessoa e serão apagados toda sexta-feira por meio de rotina automática.

15. Gravação telefônica

A Central Telefônica poderá registrar todas as ligações recebidas e efetuadas de todos os ramais e linhas instaladas. No entanto, em função de obrigatoriedade normativa, algumas áreas do Grupo Muffato podem ter seus ramais ligados a um sistema de gravação de voz. A escuta por qualquer funcionário só poderá ser realizada com a aprovação da área de Compliance ou de seus Diretores.

16. Trabalho remoto

São elegíveis ao trabalho remoto todos os colaboradores, a critério exclusivo do Grupo Muffato, desde que:

• Obrigatoriamente assinem o termo de aditivo de contrato de trabalho remoto;

• Não precisem, necessariamente, estar no escritório para trabalhos que exijam sua presença, como audiências;

• Não possuam reuniões agendadas com clientes, fornecedores ou parceiros sobre assuntos considerados estritamente confidenciais para o caso ou para o escritório; ou que o cliente, fornecedor ou parceiro não possa ou não aceite que elas ocorram remotamente;

• Que tenham tido liberação formal do Departamento de Recursos Humanos ou de sua diretoria imediata e conheçam e sigam rigorosamente essas Políticas de Segurança da Informação, além das políticas de trabalho já impostas pelo Departamento de Recursos Humanos.

16.1 Horários

O colaborador deverá indicar disponibilidade no sistema ou enviar mensagem para a equipe avisando que está em sua mesa trabalhando remotamente. Nesse período, ele deve estar disponível para ligações, comunicações via chat e reuniões virtuais em situação de disponibilidade equivalente a quando está presente no escritório. (Quando sair para uma pausa ou almoço, marque na ferramenta de comunicação "volto já" no status).

• Divulgue a janela de horários de disponibilidade para contatos regulares;

• A carga horária de trabalho de quem está trabalhando remoto deve ser equivalente à carga de trabalho de quem está no escritório, não podendo extrapolar os limites de seu contrato de trabalho.

Não é necessário que o colaborador que esteja em Home Office cumpra os horários de quem não está. No entanto, é fundamental e obrigatório estar 100% disponível dentro do horário comercial, em consonância com seu horário contratual.

Semanalmente, os trabalhos de Home Office devem ser combinados entre as equipes e/ou colaboradores que estejam trabalhando em conjunto.