# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Nós, do **GRUPO MAYER (MAYER SERVIÇOS DE APOIO EMPRESARIAL LTDA-ME,** inscrita no CNPJ/MF nº 10.610.085/0001-83, **MAYER GESTÃO E ADMINISTRAÇÃO EMPRESARIAL LTDA,** inscrita no CNPJ/MF nº 37.251.801/0001-30 e **MAYER TRENAMENTOS & CURSOS DE CAPACITAÇÃO PESSOAL LTDA,** inscrita no CNPJ/MF nº 40.619.593/0001-93), todas estabelecidas na Rua XV de Novembro, nº 297, 7º andar, Centro, CEP 80.020-310, Curitiba/PR e **MAYER GESTAO E ADMINISTRACAO EMPRESARIAL LTDA** (filial SP), inscrita no CNPJ sob o nº 37.251.801/0002-10, estabelecida na Avenida Pedro Severino Junior 289, Sala 10, Vila Guarani, CEP: 04310-060, São Paulo/SP, todas integrantes do **GRUPO MAYER**, levamos a segurança da informação a sério. Aqui veremos como as informações que estão sob os cuidados do **GRUPO MAYER** devem ser protegidas e asseguradas.

## 1. OBJETIVO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos negócios do **GRUPO MAYER**. Todo e qualquer usuário de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

## 2. ABRANGÊNCIA

Aplica-se a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam ao **GRUPO MAYER** e seus **CLIENTES**.

## 3. CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

**Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;

**Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;

**Integridade:** Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

## 4. DEFINIÇÕES

**Informação:** resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema.

**Ativos de Informação:** conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.

**Sistemas de informação:** de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.

**Segregação de funções:** consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.

**Grupo Gestor da Segurança da Informação:** grupo composto por administradores do **GRUPO MAYER** com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela empresa.

## 5. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida no desenvolvimento das atividades da empresa deve ser classificada de acordo com os níveis de confidencialidade abaixo:

**Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral. Por exemplo: informações disponíveis na página da Internet do **GRUPO MAYER**.

**Interna:** É toda informação que só pode ser acessada por funcionários do GRUPO MAYER. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da empresa, organização interna, mudanças de perímetros, e-mails e comunicados internos diversos.

**Confidencial:** É toda informação que pode ser acessada por colaboradores e parceiros do **GRUPO MAYER** especificamente autorizados. A divulgação não autorizada dessa informação pode causar impacto, da imagem ou operacional ao negócio da organização ou ao negócio do parceiro. Exemplo: Projetos de filiais de clientes, EVTL's e planos de expansão de clientes.

**Restrita:** É toda informação que pode ser acessada somente por um grupo restrito de colaboradores ou parceiros do **GRUPO MAYER** explicitamente indicados pelo nome ou por área a que pertencem. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Exemplos: Propostas comerciais, estratégias do **GRUPO MAYER**, dados da folha de pagamento.

Deve-se incluir em todo documento/e-mail/comunicado produzido ou alterado por nós, um selo de classificação das informações identificando em qual das categorias ele se enquadra: pública, interna, confidencial ou restrita.

## 6. RESPONSABILIDADES

De forma geral, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

I) Cumprir fielmente a Política de Segurança da Informação do **GRUPO MAYER**;

II) Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pelo **GRUPO MAYER**;

III) Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo **GRUPO MAYER**;

IV) Cumprir as leis e as normas que regulamentam a propriedade intelectual e a lei geral de proteção de dados;

V) Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;

VI) Não compartilhar informações confidenciais de qualquer tipo;

VII) Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

É dever de ***todos*** dentro do **GRUPO MAYER**:

I) Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para o GRUPO MAYER e deve sempre ser tratada profissionalmente.

II) É de responsabilidade do Gerente/Coordenador/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

São boas práticas:

I) Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;

II) Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

## 7. Grupo Gestor da Segurança da Informação do GRUPO MAYER

I) Missão

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

II) Equipe

Rodrigo José Mayer

Aline Aparecida Mendonça Mayer (DPO)

Anaisa da Silva

## 8. DIRETRIZES GERAIS

*I) DADOS PESSOAIS DE FUNCIONÁRIOS*

O **GRUPO MAYER** se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários serão considerados confidenciais e não serão usados para fins diferentes daqueles para os quais foram coletados.

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.

*II) PROGRAMAS ILEGAIS*

É terminantemente proibido a instalação ou desinstalação de qualquer software nos computadores do **GRUPO MAYER**. As máquinas são entregues para os usuários com um pacote de softwares homologados e configurados para o uso e que não pode ser modificado pelo usuário.

Periodicamente, o Grupo Gestor da Segurança da Informação do **GRUPO MAYER** e a **TECIT – Consultoria em Tecnologia Ltda** - fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

*III) ADMISSÃO/DEMISSÃO DE COLABORADORES – CONCESSÃO E REVOGAÇÃO DE ACESSOS*

O setor de RH do **GRUPO MAYER** deverá informar ao Setor de Tecnologia da Informação e o Grupo Gestor de Segurança da Informação toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas da empresa. O RH deverá questionar ao setor responsável pela contratação quais sistemas e repositórios de arquivos de trabalho o novo colaborador deverá ter direito de acesso. Essas informações deverão ser registradas e encaminhadas para o Grupo Gestor da Segurança da Informação, que ficará designado para o envio do e-mail de comunicado padrão para o setor de TI e para a TECIT – Consultoria em Tecnologia Ltda, a finalidade de solicitar a concessão ou revogação de acessos aos recursos computacionais.

O Setor de Tecnologia da Informação juntamente com a TECIT, fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo usuário no seu primeiro acesso.

No caso de desligamento, o setor de RH deverá comunicar o fato na mesma data ao Grupo Gestor da Segurança da Informação, ao Setor de Tecnologia da Informação e a TECIT, por meio do “e-mail padrão para concessão e revogação de acessos aos recursos computacionais” para que todos os acessos concedidos sejam revogados.

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 do **GRUPO MAYER.**

*IV) POLÍTICA DE SENHAS*

Já é padrão aplicado no **GRUPO MAYER** que as senhas tenham sempre no mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial.

Recomendamos que as senhas também sejam trocadas pelos usuários a cada 3 meses, não devendo se repetir as senhas definidas nos últimos 6 (seis) meses.

Sempre que um usuário é desligado da organização, todas as suas senhas e acessos são revogados no mesmo dia.

*V) ARQUIVOS DE TRABALHO*

Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do negócio, são mantidos nos servidores de arquivos do **GRUPO MAYER**, sistema de acesso controlado e restrito exclusivamente aos colaboradores do **GRUPO MAYER.**

São exemplos de arquivos de trabalho:

**Projetos, relatórios, análises técnicas, propostas comerciais, documentos obtidos com órgãos públicos e material de suporte para a produção destes documentos.**

O acesso ao local onde os arquivos estão armazenados fora das dependências do **GRUPO MAYER** é bloqueado e somente é possível através de ferramenta de VPN e exclusivamente nos computadores do **GRUPO MAYER**, computadores esses cuja retirada do escritório somente pode ocorrer com a devida permissão do Grupo Gestor da Segurança da Informação. Para a retirada do computador o colaborador deverá assinar o Termo de Responsabilidade de Equipamentos.

*VI) ARQUIVOS INDIVIDUAIS*

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para clientes. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas. A cópia de segurança destes arquivos é de responsabilidade dos próprios usuários.

Não é permitido aos usuários o uso ou armazenamento dos tipos de arquivos abaixo relacionados em suas estações de trabalho:

- Programas não licenciados ou não homologados para uso no **GRUPO MAYER**;
- Músicas, filmes, séries, programas de TV;
- Acesso a Redes Sociais e/ou contas de e-mail pessoal durante o horário de trabalho;
- Vídeos não relacionados à atividade profissional;
- Conteúdo pornográfico ou relacionado a sexo;
- Conteúdo relacionado ou que gere discriminação de qualquer tipo, constrangimento, bullying ou qualquer forma de discurso de ódio.

*VII) COMPARTILHAMENTO DE PASTAS E DADOS*

O compartilhamento de pastas e arquivos de trabalho cujo conteúdo seja classificado como sendo de informação CONFIDENCIAL ou RESTRITA somente é possível através das ferramentas oficiais da empresa e para os motivos previstos pelo escopo do trabalho. As ferramentas oficiais são:

- Ferramenta de e-mail padrão;
- MS Teams;
- WhatsApp Business em conta corporativa;
- Planilhas do Google Drive;
- We transfer e File transfer.

Considera-se que o compartilhamento de pastas e arquivos somente é autorizado para os casos previstos e necessários para a realização do trabalho. Sendo vedado o compartilhamento para quaisquer outros motivos.

Considera-se ainda que o compartilhamento de arquivos e pastas por outras ferramentas não é justificado e, portanto, deve ser evitado.

*VIII) CÓPIAS DE SEGURANÇA, RECUPERAÇÃO E INTEGRIDADE DOS SISTEMAS E DE SEUS BANCOS DE DADOS*

Cópias de segurança dos sistemas, repositórios de arquivos de trabalho, bancos de dados e configurações dos equipamentos e servidores de rede são de responsabilidade exclusiva do Setor de Tecnologia da Informação em acordo com o Grupo Gestor da Segurança da Informação.

É proibida a realização de cópias de segurança de informações pertinentes ao trabalho além das ferramentas previstas aqui, bem como da posse e do transporte de informações sensíveis para fora da empresa por quaisquer motivações que não sejam previstas e necessárias para a correta execução do trabalho definido para cada colaborador.

*IX) USO DA INTERNET*

O uso da Internet e o histórico da navegação pode ser monitorado pelo Grupo Gestor da Segurança da Informação, através do uso de sistema de registro de navegação que informa qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) de sites restritos, como por exemplo, redes sociais, é atribuição da administração da empresa, a partir da solicitação de seu Gerente/Supervisor.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

É proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a site através de computador/telefone celular da empresa:

- Estações de rádio;
- De jogos on-line;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos relacionados aos negócios do **GRUPO MAYER**, que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso de telefone pessoal, WhatsApp particular, e-mail particular ou outras ferramentas que não são de propriedade do **GRUPO MAYER** para a realização do trabalho de cada colaborador é proibido.

Em caso de perda, furto ou roubo do aparelho celular titular da conta do aplicativo WhatsApp, e/ou ataque hacker, sequestro de conta entre outras modalidades de invasão cibernética, o proprietário ou detentor do número do telefone deverá acionar imediatamente o Setor de Tecnologia da Informação e o Grupo Gestor de Segurança da Informação para as providências cabíveis.

Qualquer acesso às redes sociais que não seja relacionado com a área de interesse da empresa não é permitido e, sendo assim, passível de punição.

O acesso a estações de rádio ou ao Spotify é permitido somente para uso via telefone celular particular, através de conexão estabelecida na rede wi-fi do **GRUPO MAYER**, desde que isso não prejudique a qualidade e o prazo das entregas e sempre com fone de ouvido.

*Da mesma forma, recomenda-se sempre o bom senso e a brevidade quando ao acesso e à utilização de telefone celular durante o expediente. Lembramos ainda que é proibido fotografar ou filmar a tela de seu computador ou da tela de colegas bem como o compartilhamento de imagens que possam divulgar alguma informação de cliente ou da própria Mayer para fora do ambiente de trabalho.*

*X) USO DO CORREIO ELETRÔNICO – ("e-mail") e das ferramentas de comunicação instantânea (WhatsApp e MS Teams)*

O correio eletrônico fornecido pelo **GRUPO MAYER** é um instrumento de comunicação interna e externa para a realização dos negócios da empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do **GRUPO MAYER**, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos no "Código de Ética e Conduta"

O uso do correio eletrônico é de uso exclusivo de cada usuário, sendo o mesmo responsável por toda mensagem enviada pelo seu endereço.

Da mesma forma é proibido o compartilhamento de conta de e-mail profissional bem como de senha de acesso a computador e à rede.

Não é permitido o cadastro de contatos pessoais nos sistemas de mensagens instantâneas (ao utilizar a conta profissional); e nem a utilização de contas pessoais.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem do GRUPO MAYER e/ou de outras empresas;
- Sejam incoerentes com as políticas estabelecidas no "Código de Ética e Conduta";
- Não é recomendado o uso de e-mail gratuitos (Yahoo, Hotmail, Gmail), uma vez que não possuímos ferramentas de gestão para acompanhar o uso destas contas nem garantir a manutenção e o funcionamento delas.

O GRUPO GESTOR DA SEGURANÇA poderá acessar a qualquer momento e sem a necessidade de aviso prévio às contas de e-mail e ferramentas de comunicação instantâneas de posse do GRUPO MAYER, ficando sempre claro que elas não são de propriedade dos colaboradores.

O Grupo Gestor da Segurança da Informação poderá, visando evitar a entrada de vírus nos computadores do GRUPO MAYER, bloquear o recebimento de e-mails provenientes de e-mails gratuitos.

*XI) NECESSIDADES DE NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS*

O Grupo Gestor da Segurança da Informação é responsável pela definição de compra, substituição e instalação de todo e qualquer "software" e "hardware".

Qualquer necessidade de novo "software" ou "hardware" deverá ser discutida com os responsáveis pelo Grupo Gestor da Segurança da Informação. Não é permitida a compra, o uso mesmo que a título de teste ou o desenvolvimento de "softwares" diretamente pelos usuários.

*XII) USO DE EQUIPAMENTOS DE PROPRIEDADE DA EMPRESA*

Os usuários que estiverem de posse de qualquer equipamento (desktop, notebook, celular ou tablet) de propriedade do **GRUPO MAYER** devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido;
- O usuário não deve instalar ou remover nenhum programa do equipamento recebido, também não deve alterar a configuração de nenhum programa previamente instalado.

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc;
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto obrigatoriamente serão necessárias as ações abaixo:

- Registre a ocorrência em uma delegacia de polícia;
- Comunique o fato o mais rápido possível ao seu superior imediato e ao Setor de Tecnologia da Informação;
- Envie uma cópia do boletim de ocorrência para o RH.

*XIII) RESPONSABILIDADES DOS GERENTES/COORDENADORES/SUPERVISORES*

Os gerentes, coordenadores e supervisores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da empresa, cabendo a eles verificarem se eles estão acessando exatamente os sistemas e as áreas de dados compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e salvando seus documentos individuais nos locais previstos, conforme estabelecido nesta política.

O Grupo Gestor da Segurança da Informação fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinado sistema e/ou informação;
- Quem acessou determinada sistema e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinado sistema ou informação;
- Que informação ou sistema determinado usuário acessou;
- Quem tentou acessar qualquer sistema ou informação sem estar autorizado.

*XIV) SISTEMA DE TELECOMUNICAÇÕES E TELEFONIA*

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos do **GRUPO MAYER**, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Setor de Tecnologia da Informação, de acordo com as definições da administração da empresa.

*XV) USO DE ANTIVÍRUS*

Todo arquivo obtido através da Internet ou recebido de entidade externa o **GRUPO MAYER** deve ser verificado por programa antivírus.

Todas as estações de trabalho possuem software antivírus instalado. A sua atualização será automática, agendada pelo Grupo Gestor da Segurança da Informação, via rede.

Da mesma forma as estações de trabalho são programadas para receber as atualizações de segurança dos programas e sistema operacional instalados, sendo vedado qualquer ação que impeça as atualizações.

O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

*XVI) VIOLAÇÃO DA POLÍTICA DE SEGURANÇA*

É qualquer ato que:

- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou 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;
- Viole a Política de Privacidade de Dados do GRUPO MAYER e legislação pertinente (Lei nº 13.709/2018 – Lei Geral de Proteção de Dados).

*XVII) PENALIDADES*

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações:

- Advertência formal;
- Suspensão;
- Rescisão do contrato de trabalho;
- Outra ação disciplinar e/ou processo civil ou criminal.

Vigência

O disposto no presente documento entrará em vigor na data de publicação do comunicado que o anunciar.

Curitiba, 15 de maio de 2022.