DEPARTAMENTO	SGSI		
POLÍTICA	Política de Segurança da Informação		
N° DO DOCUMENTO	POL-SGSI-001	**DATA DA EMISSÃO**	20/04/2022
CRIAÇÃO	Ana Isabel Sousa		
REVISÃO	00	**DATA DA REVISÃO**	12/08/2025
APROVAÇÃO	Andrea Melo		

HISTÓRICO DE ALTERAÇÕES DO DOCUMENTO

Item	Natureza das alterações	Versão	Data	Elaborado por	Aprovação Final
1	Atualização	00	12/08/2025	Ana Isabel Sousa	Andrea Melo

1. SUMÁRIO

1. OBJETIVO

A Política de Segurança da Informação é uma declaração formal da A MELO IT Governance acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, representantes, administradores e demais descritos neste instrumento.

2. ABRANGÊNCIA

Todos os colaboradores e prestadores de serviços que estejam a serviço e disponibilizam de ativos corporativos da A MELO IT Governance, independentemente de sua localização física (trabalho remoto).

3. MISSÃO

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da A MELO IT Governance.

4. TERMOS E DEFINIÇÕES

- **TI**: Tecnologia da Informação.
- **Software:** É a parte lógica, o conjunto de instruções e dados processados nos computadores e na nuvem.
- **Nuvem (Cloud Computing):** Modelo de computação que permite acesso onipresente, conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis (ex: Google Drive, servidores virtuais).
- **MFA (Multi-Factor Authentication)**: Autenticação de Múltiplo Fator, recurso de segurança que exige mais de uma forma de verificação para validar o acesso.
- **Backup**: Cópia de segurança dos dados para garantir sua restauração em caso de perda ou corrupção.
- **Mídias Removíveis:** Dispositivos de armazenamento portátil como Pen Drive, HD Externo, cartões de memória, entre outros.

- **Softwares de Mensageria:** Programas de comunicação instantânea (ex: WhatsApp, Slack, Teams, Google Chat).
- **Phishing/Engenharia Social:** Técnicas de manipulação psicológica para induzir usuários a revelarem informações confidenciais.

5. SEGREGAÇÃO DE ATIVIDADES E FUNÇÕES

No quadro de pessoal e de prestadores de serviços há a segregação de atividades e funções de forma que uma mesma pessoa não assuma simultaneamente responsabilidades das quais decorram interesses conflitantes. A delegação de atribuições deve ser formal, com responsabilidades claramente delimitadas.

5.1 Conscientização e Treinamento

A MELO IT Governance possui procedimentos para conscientizar os colaboradores e terceiros sobre a necessidade da segurança das informações. Os empregados são capacitados quanto à correta utilização dos recursos, especialmente no contexto de trabalho remoto.

6. SENHAS E AUTENTICAÇÃO

Senhas de caráter sigiloso, pessoal e intransferível são fornecidas aos colaboradores para acesso às contas corporativas (Google Workspace), sistemas internos e dispositivos.

6.1 Autenticação de Múltiplo Fator (MFA/2FA)

É obrigatória a ativação e utilização da Autenticação de Dois Fatores (2FA) para acesso a todas as contas corporativas, especialmente e-mail e Google Drive. O colaborador deve configurar o segundo fator através de aplicativo autenticador ou prompt no celular corporativo. A desativação deste recurso é proibida.

6.2 Diretrizes de Senhas

Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros.

As senhas não devem ser anotadas ou armazenadas em arquivos não criptografados (Word, Excel, Blocos de Notas).

Não devem ser baseadas em informações pessoais (datas de nascimento, nomes de familiares) ou sequências óbvias (ex: "123456", "empresa2025").

7. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SI

7.1 Colaboradores

Cabe a todos os colaboradores cumprir fielmente a Política de Segurança da Informação; proteger as informações contra acesso não autorizado; assegurar que os recursos tecnológicos (notebooks e contas de nuvem) sejam utilizados apenas para finalidades aprovadas; e comunicar imediatamente a A MELO IT Governance qualquer suspeita de fragilidade de segurança pelo email **comitesi@ameloconsultoria.com**

7.2 Lideranças e Gestores

Cabe à liderança assegurar que sua equipe possua acesso e conhecimento desta Política e comunicar imediatamente eventuais casos de violação.

A liderança, junto com os colaboradores podem sugerir melhorias e modificações desta Política para melhor adequação.

7.3 Encarregado de Dados Pessoais

Cabe ao Encarregado de DP estar envolvido em todos os assuntos relacionados a dados pessoais da organização garantindo a conformidade com a Lei Geral de Proteção de Dados e com as políticas internas referentes à privacidade.

8. DIRETRIZES DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

A informação é um ativo que tem valor para a organização e necessita ser adequadamente protegida, garantindo a continuidade dos negócios.

A segurança da informação é caracterizada pela preservação da:

- **Confidencialidade**: Acesso somente a pessoas autorizadas.
- **Integridade**: Salvaguarda da exatidão e completeza da informação.
- **Disponibilidade**: Acesso à informação quando necessário.

A organização efetua o tratamento dos dados em todo o seu ciclo de vida, cumprindo a legislação aplicável (LGPD), garantindo o uso legal, transparente e mantendo os dados apenas pelo tempo necessário.

9. PROPRIEDADE INTELECTUAL

É de propriedade da A MELO IT Governance todos os designs, criações, códigos, processos ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo profissional. Os softwares e aplicações utilizados pela equipe possuem licenças, não sendo permitido utilização de softwares piratas.

10. ENGENHARIA SOCIAL

A Engenharia Social visa obter informações sigilosas através da exploração da confiança.

- **Diretos**: Contato direto (telefonemas, mensagens) solicitando dados.
- **Indiretos**: E-mails falsos (Phishing), links maliciosos ou ofertas tentadoras.
- **Recomendação**: Desconfie de solicitações urgentes ou fora do padrão, verifique sempre o remetente e jamais forneça senhas ou códigos de MFA por telefone ou chat.

11. CLASSIFICAÇÃO DA INFORMAÇÃO

É responsabilidade da liderança estabelecer critérios relativos ao nível de confidencialidade da informação:

- **Pública**: Informação dedicada à divulgação ao público em geral.
- **Confidencial**: Informação crítica (financeira, estratégica, dados de clientes). A divulgação não autorizada pode causar sérios impactos. Restrita a grupos específicos.
- **Restrita**: Informação acessível apenas por usuários explicitamente indicados.

Os rótulos da classificação são realizados no Google Drive que possui os marcadores para a devida classificação quando o documento for aprovado.

Ver o documento PR-SGSI-002-00 Controle e Classificação da Informação.

12. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL (TRABALHO REMOTO)

Cuidado ao tratar de assuntos da empresa em ambientes compartilhados (coworkings, cafés ou em casa com visitas presentes).

Evite mencionar nomes de clientes e dados sensíveis em videochamadas se houver pessoas não autorizadas no mesmo ambiente físico.

Utilize fones de ouvido para evitar que terceiros ouçam o conteúdo de reuniões confidenciais.

13. SEGURANÇA NO AMBIENTE DE TRABALHO REMOTO (HOME OFFICE)

Considerando que a A MELO IT Governance opera em modelo remoto, a segurança física dos equipamentos é de responsabilidade direta do colaborador.

- **Bloqueio de Tela**: É obrigatório bloquear a tela do computador sempre que se ausentar, mesmo que em casa, para evitar acessos acidentais ou indevidos.
- **Ambiente de Vídeo:** Durante reuniões, verifique o entorno para garantir que não haja exposição de dados sensíveis ou informações privadas no fundo do vídeo.
- **Zelo pelo Equipamento:** Equipamentos corporativos não devem ser deixados em veículos ou locais públicos sem supervisão.

Mais orientações na POL-SGSI-002-00 - Política de BYOD.docx

14. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

14.1 Diretrizes Gerais

Todo acesso às informações é controlado via autenticação individual. As permissões de acesso aos diretórios na nuvem devem ser revistas periodicamente.

14.2 Diretrizes Específicas

14.2.1 Sistemas e Backup em Nuvem

A MELO IT Governance utiliza soluções em nuvem. A redundância e o backup são geridos primariamente através das políticas de retenção das ferramentas contratadas (ex: Google Workspace). O colaborador não deve impedir as atualizações automáticas ou sincronizações do sistema.

14.2.2 Estações de Trabalho (Notebooks)

As estações de trabalho possuem códigos internos ou identificadores. Tudo que for executado na estação é de responsabilidade do colaborador. É proibido desativar recursos de segurança (antivírus, firewall local) instalados pela empresa.

14.2.3 Política de Mesa Limpa e Tela Limpa

Documentos digitais sensíveis não devem ficar expostos na Área de Trabalho (Desktop) desnecessariamente.

Não salvar senhas em post-its digitais ou blocos de notas visíveis.

Ao compartilhar a tela em reuniões, feche janelas ou abas que contenham informações confidenciais de outros projetos ou clientes.

Não deixe materiais físicos nas mesas de trabalho que possuam dados de clientes e informações confidenciais pertencentes a A MELO IT Governance. Sempre guarde em gavetas evitando exposição.

14.2.4 Utilização de Equipamentos Particulares

O uso de equipamentos particulares para acesso a dados corporativos só é permitido mediante aprovação da empresa e desde que respeitados os requisitos de segurança (antivírus atualizado, sistema operacional original e uso de MFA).

Mais orientações na POL-SGSI-002-00 - Política de BYOD.docx

14.2.5 Diretrizes para Computação em Nuvem e Google Drive

A A MELO IT Governance adota o Google Drive como ferramenta oficial de armazenamento.

- **Centralização**: Todos os arquivos de trabalho devem ser criados e salvos diretamente nos Drives Compartilhados da empresa.
- **Proibição Local**: É proibido manter arquivos corporativos críticos apenas localmente na máquina sem sincronização.
- **Nuvem Pessoal**: É estritamente proibido o uso de nuvens pessoais (Dropbox, Google Drive pessoal, etc.) para armazenamento de dados da empresa.
- **Compartilhamento**: O compartilhamento de links deve ser restrito às pessoas que necessitam do acesso ("Restrito a pessoas com o link" ou "Apenas convidados"), evitando links públicos indexáveis.

14.2.6 Instalação de Softwares

Qualquer software necessário para o serviço deve ser homologado pela liderança. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) ou craqueados nos computadores utilizados para trabalho. Como os computadores são particulares em sua maioria, seguindo a Politica POL-SGSI-002-00 - Política de BYOD.docx a orientação é não ter softwares que possam prejudicar de alguma forma as informações da A MELO IT Governance.

Os sites, considerando filtragem de web e navegação segura, são realizados nos dispositivos controlados pela A MELO IT Governance pela ferramenta Kaspersky.

14.2.7 Diretrizes de Conectividade e Internet

- **Redes Wi-Fi**: Evite o uso de redes Wi-Fi públicas abertas para acessar dados críticos. Em casa, certifique-se de que seu roteador Wi-Fi utiliza senha forte e criptografia (WPA2/WPA3).
- **Uso da Internet**: A internet deve ser utilizada para fins corporativos e enriquecimento profissional. O acesso a sites com conteúdo impróprio ou ilícito é proibido.
- **Downloads**: É vedado o download de arquivos suspeitos ou softwares desconhecidos que possam comprometer a segurança da máquina e que comprometam as informações da empresa.

14.2.8 Mídias Removíveis e USB

O uso de mídias removíveis (Pen Drives, HDs Externos) não é estimulado, devendo-se priorizar a nuvem. Caso utilizado, o dispositivo deve ser verificado por antivírus antes da abertura dos arquivos.

14.2.9 Recomendações sobre o E-Mail

Utilizar o e-mail corporativo apenas para fins profissionais.

Não abrir anexos de remetentes desconhecidos ou com extensões suspeitas (.exe, .bat, .src).

Não utilizar o e-mail para cadastro em sites de entretenimento ou compras pessoais não relacionadas ao trabalho.

14.2.10 Antivírus e Atualizações

Os sistemas operacionais e softwares de antivírus devem ser mantidos sempre atualizados e configurados para varredura automática.

14.2.11 Uso de Softwares de Mensageria

O uso de mensageiros (WhatsApp, Telegram) deve ser feito com cautela. É proibido o envio de arquivos contendo dados sensíveis, senhas ou bases de dados de clientes através de mensageiros pessoais. Utilize os canais oficiais e seguros da empresa para troca de arquivos.

15. VIOLAÇÕES E SANÇÕES

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento por justa causa e eventuais processos cíveis ou criminais, conforme a gravidade do incidente e a legislação vigente.

16. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado, sujeita a revisões periódicas.