Política de Segurança da Informação e Privacidade

Nome do documento Política de Segurança da Informação e Privacidade	**Tipo de documento** Política	**Classificação** Interna
Criada por Rodrigo Lopes (rodrigo@fwdcomputers.com) Bárbara Araújo (barbara.araujo@fwdcomputers.com)	**Data de criação** 05/10/2022	**Versão** 1
Revisada por Priscila França (pfranca@rmconsulting.com.br) Lorena Zucatelli (lorena@gilbertoalvares.adv.br)	**Data de revisão** 08/11/2022	**Revisão** 1
Aprovada por Rachel Maia	**Data de aprovação**	**Prazo para revisão** Anual

ÍNDICE

1. Declaração

1.1 A **RM Consulting** é uma consultoria especializada em educação corporativa, recrutamento e seleção, pesquisa e palestras, com diversidade, inclusão, desenvolvimento de liderança, aceleração de carreira, presidida por Rachel Maia, tem como missão gerar oportunidades de forma inclusiva e inovadora, impactar e influenciar pessoas e empresas. Para tal, compreende-se que sendo sua base diversidade e inclusão, dispondo de Censo de Equidade Racial, a informação através de métodos, critérios, estudos e conhecimentos específicos, é um ativo estratégico.

1.2 A RM Consulting considera também de inestimável valor os dados confidenciais ou pessoais de todos seus colaboradores, candidatos, parceiros e fornecedores tratados em suas atividades de negócio.

1.3 A correta gestão da informação, assegurando que esta esteja sempre disponível pelo tempo necessário para aqueles que dela precisam para o exercício de suas atividades em nome da organização é fundamental para a reputação da RM Consulting, e com isso para o crescimento da organização e sua percepção pelo mercado onde atua, bem como pelas partes interessadas e pelo público em geral.

1.4 Desta forma, a RM Consulting estabelece através desta Política de Segurança da Informação e Privacidade, como parte de seu Sistema de Gestão Organizacional, alinhado às melhores práticas e normas internacionalmente aceitas, seu objetivo de garantir níveis adequados para assegurar a confidencialidade, integridade e disponibilidade das informações tratadas pela organização e sob sua responsabilidade.

2. Glossário

2.1 Visando o melhor entendimento de todos aqueles que devem tomar conhecimento desta Política de Segurança da Informação e Privacidade, fica estabelecida aqui a definição para os seguintes termos:

Termo / Conceito	Definição / Exemplo
Segurança da Informação	Correta aplicação de controles para proteção da confidencialidade, integridade e disponibilidade da informação em qualquer formato (físico ou digital) segundo sua relevância para o cumprimento dos objetivos de negócio e responsabilidades legais da organização. Os esforços de Segurança da Informação da RM CONSULTING são orientados pelas Normas Técnicas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e pelo NIST Cybersecurity

	Framework; sem prejuízo de outros modelos, controles e melhores práticas que possam ser consultados e considerados.
Segurança Cibernética	Aplicação de medidas técnicas com objetivo de proteger a informação armazenada por meio digital em servidores, computadores, smartphones, sistemas, e-mails e bancos de dados, armazenados localmente ou em nuvem.
Privacidade e Proteção de Dados Pessoais	Referidas neste documento de forma simplificada como "Privacidade". Consiste no compromisso da organização com o direito humano fundamental à Privacidade do indivíduo, traduzido na aplicação de medidas técnicas e administrativas para proteção de dados pessoais e sensíveis conforme requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD). Os esforços de Privacidade e Proteção de Dados da RM Consulting são orientados pela Norma Técnica ABNT NBR ISO/IEC 27701:2019, além da própria LGPD; sem prejuízo de outros modelos, controles e melhores práticas que possam ser consultados e considerados.
Lei Geral de Proteção de Dados Pessoais (LGPD)	Lei nº 13.709/2018, é a legislação federal brasileira que estabelece regras para tratamento de dados de pessoas naturais por meios físicos ou digitais, aplicada a profissionais liberais, empresas, órgãos públicos e organizações não governamentais; com objetivo de assegurar que organizações adotem processos e medidas para preservar o Direito à Privacidade e proteger os dados pessoais e sensíveis durante todo seu ciclo de vida.
Dado	Parte sem significado da informação.
Informação	Dado colocado em um contexto, com significado. Também referenciada nesta Política como **ativo de informação**.
Proprietário da informação	Responsável pela classificação, compartilhamento e divulgação da informação conforme diretrizes estabelecidas nesta Política, requisitos legais e objetivos de negócio da organização.
Ativo	Qualquer coisa com valor para a organização. **Exemplos de ativos tangíveis**: pessoas e suas competências, equipamentos, softwares e informações. **Exemplos de ativos intangíveis**: reputação e imagem da organização.
Confidencialidade	Princípio que preza que uma informação deve estar acessível apenas para aqueles aos quais seja necessário tal acesso para a execução de suas atividades em nome da organização.
Integridade	Princípio que preza que dados e informações devem ser mantidos íntegros, válidos, livres de adulteração e não corrompidos.
Disponibilidade	Princípio que preza que dados e informações devem estar disponíveis para indivíduos e sistemas que deles precisam para cumprir com suas atividades e tarefas em nome dos objetivos de negócio da organização.
Autenticidade	Princípio adotado para a confirmação da identidade dos usuários antes que seja liberado o acesso a sistemas, e-mails e recursos computacionais, minimizando os riscos de acessos e utilizações não autorizadas. A autenticidades requer que se valide a autorização de usuários, dispositivos, serviços, conexões; para acessar, transmitir e

	receber determinadas informações. Os mecanismos básicos para a autenticação são **logins e senhas**, mas também podem ser utilizados recursos como a autenticação biométrica ou a autenticação por meio de tokens. A combinação de 2 ou mais fatores de autenticação, como por exemplo: senha e confirmação de um token no smartphone do usuário, é chamado de **autenticação multifatorial (MFA)**.
Não Repúdio:	Princípio baseado no conceito jurídico de **irretratabilidade,** assegura que uma pessoa ou entidade **não possa negar** a autoria de seus atos. Por exemplo: negar a utilização de uma informação fornecida, transações realizadas em um sistema de informação ou computador, acessos e transações realizadas na Internet etc. Na Gestão de Segurança da Informação, isso significa ser **capaz de provar** o que foi feito, por quem e quando foi feito, impossibilitando a negação das ações por parte de seus respectivos executores.
Vulnerabilidade	Ponto fraco de um ativo ou controle de segurança que possa ser explorado por uma ameaça e desta forma causar danos.
Ameaça	Causa potencial de um incidente indesejado, que possa resultar em danos a um ativo, sistema ou a uma organização.
Ameaças humanas intencionais	Extravio de informações, ataque hacker, roubo etc.
Ameaças humanas não intencionais	Pen drive infectado, usuário clica em um link malicioso por acidente, perda de um laptop ou smartphone etc.
Ameaças não humanas	Incêndio, inundação, falha no ar-condicionado, queda de energia etc.
Risco	Potencial que uma ameaça tem de explorar vulnerabilidades de um ativo ou grupo de ativos e, desta forma, causar danos à organização. Os riscos devem ser calculados segundo sua probabilidade (ocorrência) X consequência (impacto).
Controle	Medida administrativa, técnica ou física integrada aos processos da organização com objetivo de mitigar riscos. Tais como políticas, processos, softwares e sistemas de segurança, melhores práticas etc.
Incidente	Evento indesejável e/ou inesperado que pode comprometer os objetivos de negócio explorando um risco à confidencialidade, integridade ou disponibilidade das informações.
Medidas físicas	Crachás para identificação de colaboradores e visitantes, geradores e sistemas para alimentação ininterrupta de energia (UPS), extintores de incêndio, câmeras de segurança, controle de acesso, trituradores de papel etc.
Medidas técnicas	Controle de identidades, autenticação multifatorial (MFA), soluções antimalware, backup, criptografia, firewall, sistemas para detecção de intrusos, sistemas para recuperação de desastres, sistemas para prevenção contra extravio e perda de dados, atualização e correção de sistemas etc.
Medidas administrativas	Políticas de Segurança da Informação e Privacidade, inventário de ativos, programa de treinamento e capacitação de colaboradores, seguros de

	responsabilidade empresarial e contra ameaças cibernéticas, termos de confidencialidade etc.
Dado confidencial	Qualquer dado ou informação cuja revelação deva ser controlada por envolver conteúdo classificado pela organização como de acesso confidencial ou restrito, o qual deve estar acessível apenas a pessoas prévia e explicitamente autorizadas, que precisem conhecer tal dado para execução de suas atividades a favor da organização. Convém que o acesso a dados confidenciais da organização esteja protegido por Acordos de Confidencialidade e Não Divulgação, conforme cláusula 13.2.4 da Norma ABNT NBR ISO/IEC 27002:2013.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável. Qualquer informação relacionada a um indivíduo que possa identificá-lo, mesmo que para isso precise ser combinada com outras informações. **Exemplo:** nome, sobrenome, data de nascimento, CPF, RG, CNH, sexo, endereço, e-mail, telefone etc.
Dado pessoal sensível	Referido neste documento de forma simplificada como “dado sensível”, são Informações de caráter íntimo, muito pessoal e que podem levar à discriminação do indivíduo. **Exemplo:** dados sobre a saúde (prontuários, exames, laudos cirúrgicos etc.) genéticos, biométricos, referente a origem racial ou étnica, convicção religiosa ou política, e referentes a vida sexual.
Dado pseudo-anonimizado	Dados que estão aparentemente anonimizados, mas podem identificar o titular caso alguma informação seja complementada. **Exemplo:** informações que combinadas possam levar a identificação do indivíduo.
Dado anonimizado	Qualquer dado relacionado a um indivíduo, mas que não possa identificá-lo. **Exemplo:** dados expostos genericamente em uma pesquisa.
Titular de dados	Pessoa física natural, ou seja, o indivíduo que é titular dos dados.
Tratamento de dados	Toda e qualquer operação realizada com um dado pessoal, desde simplesmente acesso, até coleta, produção, recepção, classificação, utilização, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, modificação, comunicação, transferência etc.
Agentes de tratamento	Pessoas físicas ou jurídicas, de direito público ou privado, que tratam dados pessoais ou sensíveis. Segundo a LGPD, os agentes de tratamento se dividem em controladores e operadores e uma mesma organização pode ser controladora de determinados dados e operadora de outros.
Controlador	Aquele que toma decisões referente ao tratamento dos dados pessoais. **Exemplo:** a RM Consulting é controladora dos dados de colaboradores.
Operador	Aquele que trata dados pessoais por orientação do controlador. **Exemplo:** sistemas como o Microsoft 365 contratados pela RM Consulting para gerenciar e-mail e servidor de arquivos.
Encarregado de Dados ou Data	Profissional ou empresa designado para orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à

Protection Officer (DPO)	proteção de dados pessoais; responsável por disseminar a cultura de proteção de dados conscientizando os colaboradores e desenvolvendo um programa de governança em privacidade. É responsável também por atender solicitações dos titulares de dados e por interagir com a ANPD, inclusive comunicando incidentes.
Autoridade Nacional de Proteção de Dados (ANPD)	É uma autarquia federal, criada com o objetivo elaborar diretrizes nacionais para proteção de dados pessoais, bem como elaborar regulamentações e estudos complementares, fiscalizar o cumprimento da LGPD e punir eventuais infrações.

3. Escopo e objetivos

1.1. Esta Política de Segurança da Informação e Privacidade deve ser aplicada a todas as partes da RM Consulting e gerenciar o tratamento de ativos de informação através de todo o seu ciclo de vida.

1.2. Todas as partes da RM Consulting tratam informações, seja de forma verbal, através de vários tipos de mídias físicas ou plataformas tecnológicas. Políticas de Segurança da Informação e Privacidade aqui incluem todos os processos, papeis, modelos, arquitetura da informação, políticas, termos, regras e regulamentos, os quais em conjunto com esta Política, possam ser considerados necessários para assegurar que a informação seja tratada de forma a atender as necessidades e objetivos de negócio da organização, assim como obrigações legais e contratuais as quais está sujeita.

1.3. Esta Política de Segurança da Informação e Privacidade é extensível a toda a organização e devem ser governados por ela, todo os colaboradores, parceiros e fornecedores, enquanto em exercício de atividades através ou em nome da RM Consulting, assim como sistemas, softwares, comunicações e instalações contratadas ou pertencentes à organização.

1.4. Toda a informação criada/coletada, armazenada, acessada/utilizada, modificada, compartilhada arquivada ou descartada por qualquer pessoa ou sistema em nome do RM Consulting deve ser classificada, protegida e disponibilizada corretamente e com níveis adequados segurança.

1.5. Todos os ativos – sejam eles pessoas, processos, tecnologias, sistemas ou informações – devem ser governados por um rigoroso processo de gerenciamento de riscos e estar sujeitos a implementação de controles que assegurem as melhores práticas de Segurança da Informação e Privacidade.

1.6. Todos os dados pessoais tratados pela RM Consulting devem respeitar bases legais claramente previstas na Lei Geral de Proteção de Dados, assim como os princípios de finalidade, adequação, minimização, transparência, segurança, qualidade e prestação de contas.

1.7. Deve ser claro o objetivo de proteger dados confidenciais ou pessoais, em qualquer forma física ou digital, para tal compreende-se que Segurança da Informação e Privacidade devem estar integradas por padrão e no desenho de todos os processos, sistemas, documentos e relações, sendo assim vistas como estratégicas para o prestígio, relevância e crescimento da RM Consulting no mercado onde atua.

1.8. Deve estar claro o compromisso com o cumprimento de obrigações legais e contratuais impostas a organização. Esta responsabilidade se aplica à RM Consulting em sua coletividade e deve ser compartilhada por todos aqueles que estão direta ou indiretamente ligados à ela, ou que em nome dela estejam sujeitos a estas obrigações na execução de suas tarefas e atividades profissionais.

4. Diretrizes e responsabilidades

4.1 Com objetivo de promover o alinhamento estratégico dos interesses da RM Consulting com as melhores práticas de Segurança da Informação e Privacidade, necessárias para o cumprimento dos objetivos de negócio da organização, assim como requisitos legais e obrigações contratuais aos quais está sujeita, fica decidida a formação do Comitê Gestor de Segurança da Informação e Privacidade ("CGSIP") com participação da Gestora Administrativa, Encarregada de Dados (DPO), e Representante da Consultoria de Segurança da Informação.

4.2 O conteúdo desta Política de Segurança da Informação e Privacidade – incluindo seu escopo, objetivos, regras e construção – apenas poderá ser modificado por deliberação do CGSIP e deverá ser revisado sempre que necessário, com o intervalo máximo de 12 meses a partir da aprovação.

4.3 A comunicação sobre a Política de Segurança da Informação e Privacidade deve ocorrer de imediato após sua aprovação ou atualização, e nenhum colaborador deve ser considerado apto a exercer suas atividades em nome da RM Consulting sem conhecimento e ciência formal desta. Toda a comunicação deve estar de acordo com o Plano de Comunicação e Conscientização em Segurança da Informação e Privacidade, que estabelece a estratégia da organização para assegurar que todos os colaboradores estejam cientes de suas responsabilidades, bem como dos processos, tecnologias e ferramentas com os quais contam para que possam contribuir na missão da RM Consulting em assegurar a Confidencialidade, Integridade e Disponibilidade dos dados tratados em seu nome.

4.4 A comunicação sobre esta Política de Segurança da Informação e Privacidade é de responsabilidade de todos os gestores junto a suas respectivas equipes. Questionamentos e dúvidas devem ser prontamente endereçados ao Comitê Gestor de Segurança da Informação e Privacidade em *dpo@rmconsulting.com.br*

4.5 Empresas contratadas pela RM Consulting devem incluir em seus contratos um Termo de Confidencialidade compatível com os serviços que prestarão, formalizando o comprometimento de

seus sócios, prepostos, colaboradores e subcontratados com a confidencialidade quanto ao tratamento de dados pertencentes à RM Consulting.

4.6 Empresas contratadas pela RM Consulting, operadores de dados pessoais e dados pessoais sensíveis, devem formalizar em seus contratos e estar aptas a demonstrar sua conformidade com a Lei Geral de Proteção de Dados Pessoais, inclusive, quando se fizer necessário, através de auditorias específicas realizadas pela RM Consulting ou por empresa terceirizada contratada para esta finalidade.

4.7 Deve ser avaliado pelo CGSIP a necessidade de que empresas contratadas e seus prepostos tomem conhecimento e recebam treinamento sobre esta Política de Segurança da Informação e Privacidade como requisito para o exercício de suas atividades junto a RM Consulting.

4.8 Todos os membros, colaboradores, parceiros e fornecedores tratam informações pertencentes à RM Consulting ou em seu nome e devem tomar ciência e assinar um Termo de Confidencialidade compatível com as informações às quais terão acesso, formalizando suas responsabilidades, inclusive após o encerramento do contrato em questão.

4.9 Todos os colaboradores tratam dados confidenciais e/ou pessoais em nome da RM Consulting e para tal lhe são concedidos recursos tecnológicos para o exercício das suas atividades, tais como: contas de e-mail, acesso a sistemas, computadores e smartphones. Todos estes recursos estão sujeitos a monitoramento contínuo e auditoria sem aviso prévio por parte da equipe de TI da RM Consulting ou consultoria externa contratada para esta finalidade. Portanto desaconselhamos a utilização destes recursos para o manuseio, armazenamento ou comunicação de informações de caráter pessoal do próprio colaborador.

4.10 Fica estabelecido que **TODOS OS COLABORADORES** são responsáveis por:

- **a.** conhecer integralmente o conteúdo e realizar suas atividades de trabalho segundo as regras estabelecidas nesta Política de Segurança da Informação e Privacidade, considerando também outras políticas e termos específicos apresentados no contexto de suas atividades e ativos aos quais possuem acesso.
- **b.** Compreender que Segurança da Informação e Privacidade são responsabilidades de todos na organização e por isso todos devem estar atentos enquanto utilizam ativos e tratam informações pertencentes ou em nome da RM Consulting, observando as regras da organização estabelecidas nesta Política de Segurança da Informação e Privacidade, bem como em outras políticas, termos específicos e boas práticas de mercado.
- **c.** Compreender que é seu dever conhecer e cumprir leis e normas que regulamentam aspectos como Privacidade e Proteção de Dados Pessoais e Propriedade Intelectual no exercício de suas atividades profissionais em nome da RM Consulting.
- **d.** Cumprir com os treinamentos e programas de conscientização em Segurança da Informação e Privacidade promovidos pela RM Consulting, como por exemplo: Treinamento sobre LGPD e Treinamento sobre Defesa Cibernética Pessoal.

e. Adotar senhas fortes para que suas contas de acesso para e-mails, sistemas e estações de trabalho sejam mantidas dentro de um nível aceitável de segurança. Não compartilhar suas senhas com qualquer pessoa, em nenhuma hipótese, e utilizar autenticação multifatorial (MFA) sempre que este recurso estiver disponível.

f. Conhecer e aplicar em sua rotina de trabalho as regras para classificação, rotulagem, manuseio e descarte de ativos de informação conforme estabelecido na *Política de Ciclo de Vida e Classificação da Informação*. E adotar precauções extras quando compartilhar qualquer informação em redes sociais ou blogs, considerando sempre se a RM Consulting pode ser prejudicada por uma informação que caia em mãos erradas.

g. Seguir recomendações estabelecidas pela RM Consulting para o tratamento de dados pessoais ou sensíveis dos colaboradores, parceiros e fornecedores; e consultar o Encarregado de Dados (DPO) sempre que houver dúvidas sobre riscos advindos de um determinado tratamento de dado pessoal ou sensível.

h. Armazenar seus documentos na assinatura do Microsoft 365, sobretudo no Microsoft Sharepoint e Microsoft OneDrive, da RM Consulting ou outro diretório caso especificado explicitamente, conforme regras específicas da organização para que sejam realizados backups e demais processos com objetivo de assegurar a integridade e disponibilidade de dados e informações.

i. Tratar informações pertencentes à RM Consulting apenas através de e-mails e sistemas fornecidos para esta finalidade, exceto quando autorizados formal e explicitamente a proceder de maneira diferente.

j. Utilizar de forma apropriada, dentro das normas aprovadas, equipamentos e recursos tecnológicos fornecidos pela RM Consulting, informando sobre qualquer não conformidade conhecida ou comportamento suspeito em seus computadores, smartphones, sistemas e e-mails.

k. Instalar ou utilizar somente softwares e sistemas previamente autorizados, apenas dentro das especificações aprovadas pelo Departamento de Tecnologia da Informação. Não instalar softwares e sistemas licenciados para a RM Consulting em equipamentos pessoais sem autorização prévia.

l. Adotar, inclusive quando fora de instalações pertencentes à organização, medidas cabíveis para proteger as informações da RM Consulting - em formato físico ou digital - contra acesso, modificação, destruição ou divulgação indevidos ou não autorizados.

m. Não abrir e-mails ou outro tipo de mensagem de procedência ou com assuntos duvidosos, como por exemplo: solicitações cadastrais por parte de bancos, Receita Federal, Tribunal de Justiça e Serasa.

n. Comunicar qualquer problema, suspeita ou solicitação relacionados à Segurança da Informação e Privacidade apenas através do dpo@rmconsulting.com.br e-mail aprovado pela RM Consulting para esta finalidade.

o. Reportar de imediato caso desconfie de um vazamento de dados ou qualquer incidente de Segurança da Informação e Privacidade que possa afetar ativos e interesses da RM Consulting.

4.11 Fica estabelecido que **O COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ("CGSIP"),** sem prejuízo das regras impostas a todos os colaboradores, é responsável por:

a. Conduzir o tratamento da temática de Segurança da Informação e Privacidade como um todo na RM Consulting, zelando pelo alinhamento do Sistema de Gestão de Segurança da Informação e Privacidade aos objetivos de negócio da organização.

b. Assegurar o provisionamento de recursos humanos e financeiros necessários para salvaguardar os interesses da RM Consulting nas questões de Segurança da Informação e Privacidade.

c. Atribuir os papeis e responsabilidades relacionados à Segurança da Informação e Privacidade a pessoas competentes e capazes de cumprir com as tarefas a elas atribuídas, comprometendo-se a buscar consultoria especializada em qualquer assunto, tecnologia ou ferramenta que considerar necessário.

d. Realizar a devida diligência no processo de recrutamento e contratação de colaboradores com objetivo de assegurar que os responsáveis por funções ligadas a Segurança da Informação e Privacidade possuam competência – baseada em educação, treinamento e experiência - compatível com o exercício de suas atividades.

e. Apontar o Encarregado de Dados (DPO) da RM Consulting e assegurar que este possua autonomia, recursos tecnológicos e humanos para o exercício de suas funções.

f. Coordenar o programa de Gestão de Riscos em Segurança da Informação e Privacidade da RM Consulting, responsabilizando-se: (i) pela definição de critérios objetivos para classificação e aceitação de riscos; (ii) periodicidade e escopo para realização de avaliações de riscos; (iii) aprovação, aplicação e validação de planos de tratamento de riscos.

g. Monitorar, medir a eficácia e revisar controles implementados, avaliações e planos para tratamento de riscos da RM Consulting, com objetivo de eliminar não-conformidades e continuamente melhorar a pertinência, adequação e eficácia do Sistema de Gestão de Segurança da Informação e Privacidade da organização.

h. Analisar criticamente todo o Sistema de Gestão de Segurança da Informação e Privacidade para que este seja mantido pertinente e relevante quanto aos objetivos de negócio da RM Consulting e aos requisitos legais e contratuais impostos à organização.

i. Coordenar a revisão desta Política de Segurança da Informação e Privacidade com periodicidade máxima de um ano, envolvendo equipes e colaboradores; e fazendo uso de aconselhamento especializado sempre que considerar necessário.

4.12 Fica estabelecido que os **GESTORES/LÍDERES DE DEPARTAMENTOS,** sem prejuízo das regras impostas a todos os colaboradores, são responsáveis por:

a. estar cientes e informar ao CGSIP sobre questões relativas à Segurança da Informação e Privacidade que impactem as atividades e processos de seu departamento.

b. Assegurar que nenhum colaborador atuando em seu departamento exerça suas funções e atividades sem o conhecimento e ciência formal desta Política de Segurança da Informação e Privacidade.

c. Formalizar ao Departamento de Tecnologia da Informação sobre contratações, promoções, mudanças de atividade em toda a organização, com objetivo de assegurar que cada colaborador possua sempre apenas o acesso necessário pelo tempo necessário para o exercício de suas funções.

d. Formalizar ao Departamento de Tecnologia da Informação, sempre que possível com antecedência de dois dias úteis, sobre o desligamento de colaboradores, para que acessos aos sistemas e recursos tecnológicos utilizados pelos mesmos sejam desativados/excluídos.

e. Responder, quando for de seu conhecimento, às dúvidas apresentadas por colaboradores atuando em seus respectivos departamentos. E encaminhar ao CGSIP, através do e-mail dpo@rmconsulting.com.br , as dúvidas e questionamentos que não se considerem aptos a responder.

f. Notificar de imediato ao CGSIP sobre qualquer comportamento suspeito relacionado à Segurança da Informação e Privacidade por parte de um colaborador atuando em seu departamento.

g. Seguir instruções do CGSIP sobre sanções e punições que devam ser aplicados aos colaboradores atuando em seu departamento, conforme processo disciplinar estabelecido nesta Política.

h. Não contratar ou utilizar, nem permitir que sejam contratados ou utilizados em seu departamento, sistemas e softwares que não tenham sido previamente aprovados pelo Departamento de Tecnologia da Informação da RM Consulting.

4.13 Fica estabelecido que a **CEO** sem prejuízo às reponsabilidades de todos os colaboradores e gestores de departamento, é responsável por:

a. apontar membros do Comitê Gestor de Segurança da Informação e Privacidade e assegurar que este disponha de recursos humanos e financeiros para exercer suas atividades.

b. Supervisionar os esforços de Segurança da Informação e Privacidade da RM Consulting e zelar pelo alinhamento destes esforços à missão e aos objetivos de negócio da organização.

4.14 Fica estabelecido que a **DIRETORA ADMINISTRATIVA**, sem prejuízo às reponsabilidades de todos os colaboradores e gestores de departamento, é responsável por:

a. Coordenar os esforços de comunicação e conscientização sobre Segurança da Informação e Privacidade, assegurando os gestores recursos necessários para comunicar não apenas esta Política de Segurança da Informação e Privacidade, mas também processos, papeis, modelos, arquitetura da informação, políticas, termos, guias, regras e regulamentos. Liderando os esforços para que colaboradores não exerçam suas funções sem o devido conhecimento e, quando cabível, ciência formal destes instrumentos.

b. Realizar no processo seletivo a verificação de antecedentes dos candidatos (“background check”) proporcional às atividades que vão desempenhar, com objetivo de mitigar riscos relacionados aos acessos que estes terão a informações confidenciais e pessoais pertencentes ou tratadas pela RM Consulting.

c. Respeitar as bases legais e melhores práticas mapeadas pela assessoria jurídica especializada para o tratamento de dados pessoais de colaboradores contratados, conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais.

4.15 Fica estabelecido que a **CONSULTORIA RESPONSÁVEL POR SEGURANÇA DA INFORMACÃO,** sem prejuízo às reponsabilidades de todos os colaboradores e gestores de departamento, é responsável por:

- **a.** Coordenar os esforços para que a RM Consulting possua medidas de segurança cibernética capazes de proteger os dados confidenciais e pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação indevida ou qualquer outro tratamento inadequado ou ilícito.
- **b.** Prover aconselhamento ao Comitê Gestor de Segurança da Informação e Privacidade e ao Encarregado de Dados (DPO) sobre questões pertinentes a Tecnologia da Informação e Segurança Cibernética, que possam impactar os esforços de Segurança da Informação e Privacidade do RM Consulting no contexto de seus objetivos de negócio e obrigações legais e contratuais.
- **c.** Elaborar, gerenciar e manter atualizados inventários de ativos de hardware e software de Tecnologia da Informação pertencentes à RM Consulting.
- **d.** Elaborar e manter um plano eficiente e eficaz de Gestão de Mudanças para os ativos de Tecnologia da Informação da RM Consulting com objetivo de evitar falhas advindas de softwares desatualizados ou equipamentos obsoletos.
- **e.** Elaborar e manter atualizados e relevantes processos, políticas e termos de uso que tenham por objetivo assegurar o uso adequado de ativos relacionados à Tecnologia da Informação.
- **f.** Recomendar ao Comitê que a RM Consulting conte, através de colaboradores ou prestadores de serviços especializados, com todas as competências para implementar e manter os recursos tecnológicos, maximizando sua eficácia e pertinência aos critérios previstos para tratamento e aceitação de riscos da organização.
- **g.** Gerenciar sistemas de controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos dos usuários em qualquer sistema ou ativo de propriedade ou controlado pela RM Consulting.
- **h.** Reportar com transparência ao CGSIP sobre: (i) vulnerabilidades técnicas que possam impactar a resiliência da RM Consulting contra ataques cibernéticos e medidas recomendadas para mitigá-las. (ii) Incidentes e violações de segurança cibernética nos ativos de Tecnologia da Informação da organização, atuando conforme o Plano de Resposta a Incidentes de Segurança Cibernética aprovado.
- **i.** Elaborar, validar, manter atualizado e relevante, fazendo uso de aconselhamento especializado quando necessário, um Plano para Recuperação de Desastres compatível com os requisitos de confidencialidade, integridade e disponibilidades dos sistemas e ativos de informação da RM Consulting.

4.16 Fica estabelecido que a **ENCARREGADA DE DADOS (DPO)**, sem prejuízo às reponsabilidades de todos os colaboradores, é responsável por:

- **a.** Manter seus conhecimentos relevantes e atualizados sobre: (i) a Lei Geral de Proteção de Dados Pessoais (LGPD); (ii) melhores práticas e modelos de Segurança da Informação e Privacidade; (iii) Legislações que impactem a regulação sobre Proteção de Dados Pessoais nos negócios operados pela RM Consulting; (iv) aspectos que possam impactar direitos e liberdades dos titulares de dados na operação da RM Consulting.

b. Agir com autonomia quanto a proteção dos interesses dos titulares de dados tratados pela RM Consulting e comunicar de maneira formal ao Comitê Gestor de Segurança da Informação e Privacidade sempre que, por qualquer razão, perceber cerceada tal autonomia.

c. Monitorar se as regras internas de Privacidade e Proteção de Dados e as obrigações previstas na LGPD estão sendo observadas por colaboradores, gestores, terceiros e demais partes interessadas, enquanto no tratamento de dados pessoais em nome da RM Consulting.

d. Mensurar a efetividade do Programa de Privacidade da RM Consulting por meio de indicadores próprios, avaliações periódicas e pelo acompanhamento de canais de denúncia estabelecidos para atender às requisições dos titulares de dados.

e. Atuar como ponto de contato entre a RM Consulting e a Autoridade Nacional de Proteção de Dados (ANPD), comprometendo-se a assegurar que a RM Consulting responda às requisições ou medidas necessárias, também buscando orientações proativamente sempre que considerar pertinente.

f. Atuar como ponto de contato entre a RM Consulting e titulares de dados, assegurando que as requisições destes sejam atendidas dentro do prazo legal e da melhor forma possível;

g. Atuar como disseminador da cultura de Privacidade e Proteção de Dados na RM Consulting, prestando aconselhamento sobre melhores práticas e avaliando o impacto de decisões e operações cotidianas quanto ao tratamento de dados pessoais;

h. Avaliar e aconselhar sobre a necessidade de realizar ou atualizar um Relatório de Impacto a Proteção de Dados (RIPD) em relação a alguma atividade desempenhada pela RM Consulting;

i. Prover aconselhamento ao Comitê Gestor de Segurança da Informação e Privacidade e aos Gestores de Departamento sobre questões envolvendo relacionadas a Privacidade e Proteção de Dados e sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) como um todo.

j. Informar ao CGSIP sobre a necessidade de buscar aconselhamento Jurídico, em Segurança da Informação ou em Segurança Cibernética sempre que considerar necessário para a realização de suas atividades, tendo em vista os interesses e objetivos de negócio da RM Consulting e a proteção dos dados pessoais ou sensíveis dos titulares de dados.

4.17 As violações, mesmo que por mera omissão ou tentativa não consumada, desta Política, bem como demais normas e procedimentos de Segurança da Informação e Privacidade, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, demissão regular, demissão por justa causa, processos nas esferas cível e criminal.

4.18 As aplicações de sanções e punições serão deliberadas pelo Comitê Gestor de Segurança da Informação e Privacidade (CGSIP), devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho. Podendo o CGSIP, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

4.19 No caso de terceiros contratados ou prestadores de serviço, o CGSIP deve analisar a violação ocorrida e deliberar sobre a efetivação de sanções e punições previstas em contrato, bem como sobre ações judiciais cabíveis.

4.20 No caso de violações que infrinjam a Legislação vigente, impliquem em atividades ilegais, incorram ou possam incorrer em dano à RM Consulting, o infrator deverá ser responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes, sem prejuízo às demais sanções e punições previstas nesta Política de Segurança da Informação e Privacidade.

4.21 As diretrizes estabelecidas nesta Política de Segurança da Informação e Privacidade, além de demais normas e procedimentos adotados pela RM Consulting não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui aqui rol enumerativo, cabendo ao usuário da informação adotar, sempre que pertinente, outras medidas que considerar cabíveis, além daquelas aqui previstas, para proteger as informações da RM Consulting. Inclusive comunicando proativamente sobre tais medidas ao Comitê Gestor de Segurança da Informação e Privacidade (CGSIP).

5. Normas, termos e procedimentos internos complementares

5.1 Esta Política de Segurança da Informação e Privacidade não esgota em si todos os instrumentos que direcionam e regulamentam o tratamento de informações na RM Consulting, embora deva ser considerado como documento de referência principal para questões de Segurança da Informação e Privacidade na organização.

5.2 Documentos que compõem os esforços de Segurança da Informação e Privacidade da RM Consulting, sem prejuízo de outras políticas, termos e normas não especificadas aqui, são:

- **a.** Relatório de Avaliação e Plano de Tratamento de Riscos em Segurança da Informação e Privacidade
- **b.** Termo de Confidencialidade e Responsabilidade
- **c.** Política de Ciclo de Vida e Classificação da Informação
- **d.** Plano de Resposta a Incidentes
- **e.** Plano para Recuperação de Desastres
- **f.** Plano para Continuidade de Negócios
- **g.** Mapeamento do Tratamento de Dados Pessoais

5.3 Caso haja conflito entre diretrizes estabelecidas nesta Política de Segurança da Informação e Privacidade e qualquer outra política interna, termo ou documento, deve prevalecer o que está determinado nesta política.

6. Melhoria contínua

6.1 O CGSIP deve monitorar, medir, analisar e avaliar o desempenho e a eficácia do Sistema de Gestão de Segurança da Informação e Privacidade, levando em conta o que precisa ser monitorado, método que deve ser aplicado para o monitoramento, quando os resultados devem ser analisados e quem deve analisar e avaliar estes resultados, mantendo toda a documentação relativa ao processo.

6.2 O CGSIP deve coordenar a revisão e atualização desta Política, bem como demais políticas, normas, termos, procedimentos e processos pertinentes à Segurança da Informação e Privacidade, sempre que considerar necessário, não excedendo a periodicidade máxima de doze meses.

6.3 O CGSIP deve planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos e resultados de auditorias anteriores.

6.4 Todas as partes interessadas ligadas à RM Consulting devem analisar criticamente e buscar melhorar continuamente a pertinência das regras estabelecidas pelo Sistema de Gestão de Segurança da Informação e Privacidade, bem como seu alinhamento contínuo aos objetivos de negócio da organização, levando em conta fatores como:

a. Situação das análises críticas anteriores.
b. Mudanças nas questões internas e externas.
c. Mudanças no contexto do mercado de atuação da organização.
d. Mudanças em legislações vigentes aplicáveis a organização.
e. Resultados da avaliação de riscos e situação plano de tratamento de riscos.
f. Resultados de auditorias e seus comentários.
g. Não conformidades e ações corretivas aplicadas.
h. Técnicas, produtos ou processos que possam melhorar o desempenho do Sistema de Gestão de Segurança da Informação e Privacidade da organização.

7. Controle de Versões

Versão/Revisão	Data	Responsáveis	Ações
1.0 (versão 1)	05/10/2022	Rodrigo Lopes Bárbara Araújo	○ Criação da Política de Segurança da Informação e Privacidade (PSIP).
1.1 (versão 1, revisão 1)	08/11/2022	Priscila França Lorena Zucatelli	○ Ajustes gerais em toda a PSIP quanto a especificidades da RM Consulting.

			○	Ajustes de departamentos e responsabilidades.
1.1 (versão 1, revisão 1)	28/11/2022	Rachel Maia	○	Aprovação