

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Versão 2024.10

SUMÁRIO

I.	INTRODUÇÃO	3
1.	OBJETIVO.....	3
2.	ESCOPO.....	3
3.	BASE REGULATÓRIA.....	4
II.	DIRETRIZES PARA SEGURANÇA DE INFORMAÇÃO	5
1.	CONTROLES DE ACESSO A INFORMAÇÕES CONFIDENCIAIS	5
2.	BARREIRAS E CONTROLE DE INFORMAÇÕES.....	6
3.	DETENTORES DA INFORMAÇÃO, MANUTENÇÃO DE REGISTROS E LOGS	7
4.	PROTEÇÃO DA BASE DE DADOS.....	9
5.	POLÍTICA PARA DISPOSITIVOS PESSOAIS	9
6.	CONSIDERAÇÕES SOBRE DADOS PESSOAIS	10
7.	TESTES E TREINAMENTOS DE SEGURANÇA DA INFORMAÇÃO	11
8.	TRATAMENTOS DE INCIDENTES	12
9.	DAS SANÇÕES	12
10.	PLANO DE CONTINUIDADE DE NEGÓCIO (“PCN”)	13
III.	SEGURANÇA CIBERNÉTICA.....	14
1.	OBJETIVO.....	14
2.	PRINCÍPIOS.....	14
3.	RESPONSABILIDADES.....	15
4.	IDENTIFICAÇÃO/AVALIAÇÃO DE RISCOS (<i>RISK ASSESSMENT</i>)	17
5.	AÇÕES DE PREVENÇÃO E PROTEÇÃO	17
6.	PROCEDIMENTOS NA CONTRATAÇÃO DE TERCEIROS.....	19
	CONTROLE DE VERSÕES	21
	REFERÊNCIAS	22

I. INTRODUÇÃO

1. Objetivo

A Política de Segurança da Informação e Cibernética (“Política”) estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade das informações de posse temporária, de propriedade da Drýs Capital Ltda. (“Drýs” ou “Gestora”), permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade.

A segurança da informação tem se tornado um dos tópicos de maior relevância para as organizações, em que informações proprietárias, sigilosas e essenciais para a continuidade do negócio estão sob ameaça crescente de perda ou roubo, com riscos decorrentes de prejuízos significativos financeiros e não financeiros. Dessa forma, a confidencialidade, integridade e disponibilidade da informação são pilares diretamente ligados ao tema de Segurança.

Com o objetivo de mitigar esses riscos, essa Política tem como finalidade estabelecer princípios e diretrizes de proteção de dados pessoais e informações sigilosas contra ameaças cibernéticas.

2. Escopo

Todos os sócios, funcionários, estagiários e prestadores de serviços (“Colaboradores”) e partes interessadas da Drýs que tenham acesso concedido às informações de posse temporária ou de propriedade da Gestora, em qualquer meio (físico e/ou eletrônico), ou aos sistemas e recursos computacionais estão sujeitos a essa Política, exceto quando houver contrato estabelecido com cláusulas de proteção e sigilo.

A responsabilidade em relação à segurança da informação deve ser comunicada aos Colaboradores no início de vínculo, devendo estes assinarem o Acordo de Confidencialidade, conforme estabelecido pela Gestora.

3. Base Regulatória

Resolução CVM 175 de 23/12/2022 e alterações posteriores

<https://conteudo.cvm.gov.br/legislacao/resolucoes/resol175.html>

Dispõe sobre as normas específicas para os fundos de investimento registrados junto à CVM.

Código ANBIMA de Administração e Gestão de Recursos de Terceiros de 15/07/2024

Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros

https://www.anbima.com.br/pt_br/autorregular/codigos/administracao-de-recursos-de-terceiros.htm

Estabelecem os princípios, regras e procedimentos para as atividades de Administração Fiduciária, Gestão de Recursos de Terceiros e Gestão de Patrimônio Financeiro dos Fundos de Investimento e das Carteiras Administradas, que deverão ser observados pelas Instituições Participantes no desempenho de suas atividades.

II. DIRETRIZES PARA SEGURANÇA DE INFORMAÇÃO

A Drýs adota as seguintes diretrizes de segurança da informação, que visam garantir um nível adequado de proteção ao seu ambiente de negócios:

- As informações da Drýs, dos clientes e público em geral devem ser tratadas de forma ética e sigilosa, de acordo com as leis vigentes e normas internas.
- As informações devem ser utilizadas de forma transparente e apenas para as finalidades alinhadas.
- Os procedimentos e os controles deverão abranger todo o processo de autenticação, criptografia, prevenção e detecção de intrusão, com a realização de testes periódicos.
- O acesso dos usuários às informações e ambiente da Drýs deverá ser único, pessoal e intransferível.
- Somente deve ser concedido acesso aos recursos imprescindíveis para o pleno desempenho das atividades do usuário autorizado.
- A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível. Ela deve ser mantida de forma secreta, sendo proibido o seu compartilhamento.
- Devem ser reportados eventuais fatos ou ocorrências que possam colocar a Gestora em risco.
- As responsabilidades se aplicam a todos os Colaboradores, que deverão declarar entendimento e ciência conforme programa de Compliance.

1. Controles de Acesso a Informações Confidenciais

Para fins desta Política, entende-se como Informação Confidencial toda informação resguardada contra a revelação pública não autorizada, ou seja, informações eletrônicas, escritas ou faladas da qual o Colaborador tiver acesso dentro da Gestora, incluindo: dados da Drýs, seus sócios, diretores, clientes e Colaboradores, bem como de relatórios de órgãos reguladores, autorreguladores e do poder público, dados de inspeções e fiscalizações, materiais de marketing e demais informações de propriedade da Gestora.

Todo acesso a diretórios e sistemas de Informações Confidenciais da Drýs deve ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pela área de Compliance.

O controle do acesso a sistemas de informações da Drýs levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil;
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora; e
- Manutenção de documentos digitais por prazo não inferior a 6 (seis) anos.

Ainda, como medidas de prevenção:

- Habilitação de relatos de ameaças pelos usuários: fornecimento de canal seguro para análise de ameaças recebidas;
- Comunicação: divulgação sobre ocorrências e formatos recentes de fraudes e incidentes;
- Treinamento sobre ameaças digitais e vazamento de informações;
- Validação: realização de testes periódicos para avaliação da prontidão dos colaboradores e equipes de suporte.

2. Barreiras e Controle de Informações

Os Colaboradores detentores de Informações Confidenciais ou informações não públicas relevantes (“Informações Sigilosas”), em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

- Os Colaboradores devem evitar circular em ambientes externos à Drýs com cópias (físicas ou digitais) de arquivos contendo Informações Sigilosas, salvo se necessárias ao desenvolvimento do projeto e no interesse do cliente. Nesses casos, as cópias devem ser criptografadas ou mantidas através de senha de acesso;
- O descarte de Informações Sigilosas em meio digital deve ser feito de forma a impossibilitar sua recuperação, com orientação da equipe de segurança e infraestrutura;
- As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Drýs ou do próprio cliente;

- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes etc.;
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;
- A senha de acesso do Colaborador aos sistemas da Drýs é pessoal e intransferível, conforme já destacado nas diretrizes acima;
- O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de Compliance sempre que necessário. O uso do e-mail corporativo para fins pessoais por parte Colaboradores será admitido desde que não haja impacto no desempenho de suas funções ou riscos adicionais para a Gestora.

3. Detentores da Informação, Manutenção de Registros e Logs

O Diretor de Compliance deve manter o registro dos Colaboradores que detenham Informações Sigilosas, identificando o tipo de informação detida, informando aos Sócios sobre possíveis restrições e prevenir situações que possam suscitar um provável conflito de interesses ou uso indevido de informações, minimizando ameaças aos negócios e à imagem da Drýs.

Cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e outros ativos de informação será atribuído a um responsável identificável como pessoa física. Os usuários individuais (login) dos Colaboradores internos são de responsabilidade de cada usuário, enquanto os usuários (login) de terceiros são de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação.

A Gestora possui sistemas de monitoramento em Cloud e correio eletrônico para auditoria do ambiente. As informações geradas por esses sistemas poderão ser usadas para identificar usuários e respectivos acessos efetuados, bem como arquivos acessados e manipulados. O monitoramento dos controles de segurança adotará a abordagem baseada em risco, intensificado, assim, de acordo com o nível de risco.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Diretoria de Compliance;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitara o usuário às sanções administrativas e legais cabíveis, observado o disposto na seção 9 desta Política.

4. Proteção da Base de Dados

Os recursos computacionais da Gestora devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora tenha atuação.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (backups) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso deverá ser limitado somente a pessoas autorizadas pela área de Compliance.

No âmbito de infraestrutura e ambiente, são adotados (as):

- Ferramentas para proteção ativa contra ameaças digitais – firewall, antivírus, antimalware, antiphishing e antispam;
- Múltiplas camadas de segurança para a segregação e gerenciamento de permissões de acesso (DMZ);
- Sistemas Críticos com Redundância;
- Contingenciamento de Energia;
- Sistemas de Backup;
- Segurança Física (Acesso, Monitoramento, Rede);
- Atualizações Automáticas, sem bloqueio ou interferência do usuário;
- Manutenção Preventiva.

5. Política para Dispositivos Pessoais

Os Colaboradores devem comunicar à área de Compliance sua opção por utilizar seus dispositivos pessoais (BYOD – *bring your own device*), como smartphones e laptops, para acessar a rede corporativa, sistemas internos e bancos de dados.

Os dispositivos BYOD devem ser constantemente monitorados pela Drýs para garantir a segurança dos dados e prevenir possíveis violações da política de segurança e incidentes.

A área de Compliance irá auditar o dispositivo e poderá instalar ferramentas de monitoramento e remoção remota de informações em caso de perda ou roubo do dispositivo. O uso do dispositivo pessoal será aprovado somente se o Colaborador concordar com as seguintes condições:

- Acompanhar treinamentos de segurança promovidos periodicamente pela área de *Compliance*;
- Aprovar a gestão de soluções móveis da Drýs, que contém, dentre seus principais termos, os seguintes pontos:
 - Ações para bloqueamento remoto,
 - Remoção completa de arquivos,
 - Restauração aos padrões de fábrica,
 - Monitoramento constante de atividades realizadas no dispositivo;
- Possuir disco rígido criptografado (para laptops);
- Possuir solução antivírus ou malware;
- Seguir os procedimentos definidos nesta Política em casos de incidentes como roubo ou extravio do dispositivo pessoal;
- Utilizar sempre a versão mais atualizada do sistema operacional e efetuar todas as atualizações do fabricante;
- Utilizar autenticação de múltiplos fatores (2FA) em todos os sistemas da Drýs;
- Não utilizar logins pessoais para qualquer tarefa relacionada à Drýs;
- Não emprestar o dispositivo para terceiros, inclusive membros da família;
- Não instalar aplicativos não oficiais ou não homologados pela Drýs;
- Evitar o uso de redes de Wi-Fi públicas;
- Evitar links ou anexos de e-mails de fontes não confiáveis;
- Retornar o dispositivo à área de Compliance, no caso de desligamento, para sanitização.

6. Considerações sobre Dados Pessoais

Em atendimento à Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais ("LGPD"), destaca-se que toda informação relacionada a pessoa natural identificada ou identificável ("Dados Pessoais") e dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado

referente à saúde ou à vida sexual, dado genético ou biométrico, vinculados a uma pessoa natural (“Dados Pessoais Sensíveis”) eventualmente coletados pela Drýs têm finalidades específicas e pré-determinadas para seu tratamento, sendo certo que todos os critérios e diretrizes de confidencialidade e sigilo previstos nesta Política se estendem a eles.

Ainda, a Drýs adota os melhores esforços técnicos e administrativos para garantir que todos os processos de armazenamento, compartilhamento, acesso e eliminação dos Dados Pessoais e Dados Pessoais Sensíveis por ela tratados estejam adequados à LGPD e melhores práticas do mercado

7. Testes e Treinamentos de Segurança da Informação

Para garantir a implementação de ambiente adequado, a Drýs se reserva o direito de:

- Implantar softwares e sistemas que podem monitorar e gravar os acessos e uso de Internet através da rede e das estações de trabalho da empresa, respeitado o direito à intimidade e ao sigilo das comunicações, nos termos do art. 5º, X e XII, da Constituição Federal;
- Inspeccionar qualquer arquivo, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta Política;
- Efetuar verificações e/ou auditoria coordenada por área interna ou contratada em sistemas, estações e rede sem aviso prévio.

A área de Tecnologia e Segurança é responsável pela implementação de testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades, incluindo a adoção de novas tecnologias. Além disso, anualmente, serão realizados testes de invasão e varreduras para detectar vulnerabilidades em sistema, softwares e infraestrutura da Gestora. No caso de detecção de falha ou uso em desconformidade com o estabelecido nesta Política, serão aplicados bloqueios de acesso e/ou planos de ação corretivos.

A apresentação sobre o programa de segurança da informação fará parte do treinamento inicial e periódico da Gestora, assegurando que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações previstas nesta Política, minimizando a ocorrência de incidentes de segurança.

8. Tratamentos de Incidentes

Em caso de suspeita ou incidente de violação das normas de segurança da informação identificado pelo Colaborador, a área de Tecnologia e Segurança deverá ser notificada imediatamente com o objetivo de realizar análise e levantamento dos sistemas e informações afetadas. Ademais, a documentação completa do incidente deverá ser registrada e enviada para avaliação do Compliance.

Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da Drýs.

Os incidentes de segurança da informação identificados ou relacionados com a Drýs possuem caráter sigiloso.

9. Das Sanções

O não cumprimento das normas estabelecidas nessa Política, seja isolada ou cumulativamente, poderá acarretar, de acordo com a infração cometida, as seguintes sanções:

- Comunicação informando o descumprimento ao Compliance e reporte ao Comitê de Compliance.
- Advertência ou Suspensão para casos graves ou na hipótese de reincidência de infrações de menor gravidade.
- Desligamento para casos graves ou reincidência de advertências/suspensões.

10. Plano de Continuidade de Negócio (“PCN”)

Com o objetivo de assegurar a continuidade dos negócios, manter a integridade de suas operações e de forma a assegurar que os interesses dos clientes não sejam prejudicados, em eventos que impliquem na impossibilidade da operação normal, em suas instalações principais, a Drýs conta com uma série de procedimentos para execução do Plano de Continuidade de Negócio (“PCN”).

Na eventual ocorrência de qualquer evento que impossibilite o acesso ou permanência nas dependências da Drýs, os Colaboradores devem imediatamente contatar o grupo “Drýs Geral” ou seu gestor direto para orientação.

A Gestora conta com procedimento interno que descreve os elementos do Plano de continuidade e de resposta a incidentes, que aborda os seguintes elementos:

- Queda de Energia.
- Backup e Armazenamento.
- Queda dos links de acesso à Internet.
- Contingência de E-Mails.
- Contingência de Serviços de Telefonia.
- Acesso VPN.
- Equipe Externa.
- Falha de segurança cibernética grave.

III. SEGURANÇA CIBERNÉTICA

1. Objetivo

A Política tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

As diretrizes aqui abordadas buscam seguir as melhores práticas de mercado, bem como estarem de acordo com as leis e regulamentação aplicáveis.

2. Princípios

O objetivo das regras sobre segurança cibernética da Drýs é, primordialmente, assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Drýs devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Drýs, observadas as regras de sigilo e confidencialidade constantes do Capítulo de segurança da informação.

A Drýs exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores,

reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

3. Responsabilidades

O Diretor de Compliance é o principal responsável dentro da Drýs para tratar e responder questões de segurança cibernética (“Responsável pela Segurança Cibernética”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Segue abaixo uma lista, não exaustiva, dos deveres e responsabilidades de Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar ao Comitê os riscos residuais.
- Acordar sobre os serviços prestados por terceiros contratados e os procedimentos de resposta aos incidentes.
- Acompanhar a configuração dos equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos.
- Avaliar os controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Assegurar que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Drýs em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Drýs, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Drýs.
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Drýs, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de Segurança Cibernética.

3.1 Alçadas

A alçada superior se dará através do Comitê de Compliance e a inclusão dos tópicos relacionados à supervisão e monitoramento das diretrizes de segurança cibernética conforme previsto nesta política.

O Comitê poderá ser acionado de forma extraordinária quando necessário e contará obrigatoriamente com a presença do Responsável pela Segurança Cibernética. As decisões deverão ser registradas em ata e documentadas pela área de Compliance.

O Responsável pela Segurança Cibernética, em conjunto com o Comitê de Compliance, realizará a revisão e atualização desta Política periodicamente, no mínimo bianualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada.

3.2 Demais Atribuições

Cabe a todos os Colaboradores conhecer e adotar as disposições desta Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da Drýs, o Colaborador deverá comunicar imediatamente seu superior ou Diretor de Compliance. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

A Drýs deverá manter o programa de segurança cibernética continuamente atualizado, com o objetivo de identificar tanto novos riscos como reavaliando riscos residuais. Também realizará, periodicamente, campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as informações necessárias para atuar no tema.

4. Identificação/Avaliação de riscos (*risk assessment*)

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, devem ser previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e documentados e testados durante a fase de execução.

Periodicamente, a Drýs deverá revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas conforme estabelecido nessa Política.

5. Ações de Prevenção e Proteção

A Drýs estabeleceu medidas para mitigar os riscos identificados e prevenir ataques cibernéticos, incluindo a programação e implementação de controles. Cada Colaborador é responsável por manter a segurança e controle das informações armazenadas ou disponibilizadas em seus equipamentos.

5.1 Internet, e-mail e computadores

A Drýs oferece a seus Colaboradores uma estrutura tecnológica completa para o exercício de suas atividades. É responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Além disso, cada Colaborador é responsável pela proteção de seu banco de dados, que pode ser composto por planilhas, e-mails e/ou conversas telefônicas contendo dados confidenciais de clientes e/ou da Drýs, dentre outros.

Algumas diretrizes devem ser seguidas:

- Os equipamentos e computadores da Drýs devem ser usados para atender aos interesses comerciais legítimos da Drýs e sob nenhuma hipótese servirão de instrumento à qualquer forma não autorizada por lei
- O uso de equipamentos da Drýs para fins particulares é permitido de forma moderada;
- Os downloads de qualquer natureza devem ser feitos de forma ponderada e com a devida diligência por parte do usuário, respeitando o espaço individual de cada usuário. Periodicamente e sem aviso prévio serão realizadas inspeções nos computadores para averiguação de downloads impróprios não autorizados ou gravados em local indevido;
- O correio eletrônico disponibilizado pela Drýs caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas. É permitida a utilização pessoal de forma moderada;
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (os “Emails Corporativos”), seus respectivos anexos, e a navegação através da rede mundial de computadores (a “Internet”) através de equipamentos da Drýs serão monitoradas;
- Os E-mails Corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem;
- Nos equipamentos e computadores disponibilizados pela Drýs não deverão ser utilizados: e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico para comunicação externa que não o correio corporativo da Drýs. Fica também proibido a utilização de programas de conversas eletrônicas (CHATS) externos, gratuitos ou não, salvo para fins comerciais e quando autorizados pelo Responsável pela Segurança Cibernética.

5.2 Senhas

As senhas fornecidas aos Colaboradores para acesso à rede corporativa e sistemas internos, são de caráter sigiloso, pessoal e intransferível, sendo os Colaboradores os responsáveis pela manutenção de cada senha e suas características.

5.3 Monitoramento Telefônico

As conversas telefônicas originadas ou recebidas pelo sistema de telefonia da Drýs serão monitoradas e gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial.

5.4 Monitoramento por Câmeras

A Drýs utiliza um serviço de monitoramento por câmeras e são gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política.

6. Procedimentos na Contratação de Terceiros

Os Colaboradores externos da Drýs, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. Esses riscos devem ser levados em conta pela Drýs.

A contratação de terceiros se pautará, no que tange à segurança cibernética e conforme se verificará em diligência específica, pelos seguintes critérios:

- Possuir políticas, programa e procedimentos formais relativos à segurança da informação que sejam auditados e atualizados periodicamente.
- Política formalizada de segurança cibernética, e atualização de suas certificações necessárias à prestação dos serviços contratados.
- Disponibilização de plano de resposta a incidentes de segurança cibernética.
- Realização de ações de conscientização, educação e formação de segurança de seus funcionários.
- Possuir, comprovadamente, mecanismos satisfatórios para proteção dos dados transacionados com a Drýs.
- Canal de Compliance adequado para o reporte completo e tempestivo de incidentes de segurança cibernética.

Nesse sentido, a área de Compliance deverá realizar diligência para o tema de segurança cibernética de terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (*links*)

com a Drýs ou (iv) qualquer outros que a área de Compliance julgue que por qualquer motivo possa gerar risco de cibersegurança à Drýs, previamente à sua contratação.

O resultado da diligência será avaliado pelo Compliance, formalizado e periodicamente reavaliado.

A Drýs deverá incluir os requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pelo terceiro contratado para atender aos requisitos durante a vigência do contrato, na forma mencionada acima.

CONTROLE DE VERSÕES

Revisão: Out/2024

Próxima Revisão: Out/2026

Revisado por: Giovanna Duarte | Compliance

 João Victor Fregnan | Tecnologia

Aprovado por: Maria Senger | Diretora de Riscos e Compliance

Histórico de Versões:

202009 | Revisão e Alterações estruturais.

202111 | Incluída redação no âmbito do Projeto da LGPD da Equitas, Alterações estruturais e Controles.

202202 | Revisão de versão. Sem alteração de conteúdo.

202304 | Revisão de texto

202410 | Alteração denominação social, revisão de seções e atualização de itens pontuais. Mudança no prazo de revisão para 2 anos.

REFERÊNCIAS

<https://dryscapital.com.br/documentos>

\\Compartilhado - Documentos\Compilado Documentos\ PolíticasManuais_Publicados \
Políticas e Manuais\