POLÍTICA INTERNA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

LION CONSULTORIA DE INVESTIMENTOS LTDA

SUMÁRIO

1. **INTRODUÇÃO**
2. **OBJETIVO**
3. **DEFINIÇÕES**
4. **RESPONSABILIDADE**
5. **INFORMAÇÕES**
6. **GESTÃO DA INFORMAÇÃO**
7. **ATAQUES A SEGURANÇA DA INFORMAÇÃO E PREVENÇÕES**
8. **MEDIDAS DE SEGURANÇA DA INFORMAÇÃO**
9. **NORMATIVAS E TERMOS**
10. **PENALIDADES**
11. **DISPOSIÇÕES FINAIS**

1. INTRODUÇÃO

Considerando a Lei n° 12.965/2014 que estabelece o Marco Civil da Internet;

Considerando a Lei n° 13.709/18 (Lei Geral de Proteção de Dados) que dispõe sobre a Proteção de Dados Pessoais;

Considerando o tratamento de Dados Pessoais e Informações que a empresa LION CONSULTORIA, **("Consultoria")**, inscrita no CNPJ sob o n° 67.745.884/0001-84, realiza e podem ser suscetíveis a incidentes de diversas naturezas;

Considerando que as Informações são a base do desenvolvimento do mercado financeiro e entendendo a importância do efetivo tratamento seguro dos dados, a Consultoria vem através desta Política, definir as diretrizes a serem cumpridas por todos os membros da empresa.

Serão definidas as normas e padrões responsáveis por assegurar de forma legítima e eficaz os quatro princípios que norteiam a Segurança da Informação (Disponibilidade, Integridade, Confidencialidade e Autenticidade), com o objetivo de prover a proteção necessária para a realização das operações nas dependências físicas e digitais da Consultoria.

Praticar as medidas essenciais para manter a Segurança da Informação objetiva evitar que os membros da Consultoria distribuam de forma indevida elementos sigilosos os quais gerenciam, sejam derivadas de documentos físicos, de um software utilizado pela empresa ou de uma rede de sistemas.

Esta política se aplica a todas as informações que estejam sob a responsabilidade da Consultoria, em quaisquer formas e que eventualmente sejam apresentadas ou compartilhadas. De acordo com o nosso compromisso com a proteção e segurança da informação, essas devem estar sempre protegidas adequadamente, de acordo com os controles estabelecidos neste documento.

2. OBJETIVO

A presente Política objetiva promover orientações que visam a assegurar os quatro princípios da Segurança da Informação, sendo eles a Disponibilidade, Integridade, Confidencialidade e Autenticidade.

Com a finalidade de manter a plena e efetiva proteção dos dados e informações tratados pela empresa, a Política em questão dispõe sobre as medidas

que devem ser praticadas por todos os membros da Consultoria, de acordo com as regulamentações e legislações aplicáveis.

3. DEFINIÇÕES

Informação: define-se como os dados organizados e devidamente analisados, que produzem um conhecimento relevante e transmitem um significado gerador de compreensão dentro de um contexto.

Segurança da Informação: essa prática visa a assegurar a proteção de um conjunto de informações que uma pessoa ou empresa possuem, por conta disso, existem princípios dentro da S.I. que devem ser respeitados, sendo eles o da Disponibilidade, Integridade, Confidencialidade e Autenticidade.

Disponibilidade: esse princípio da Segurança da Informação disserta sobre a acessibilidade das informações e dos sistemas da empresa, estando estes disponíveis a qualquer momento pelos colaboradores de uma instituição. Cumprindo com esse princípio, é facilitado o acesso dos setores que necessitam operar integralmente. Para garantir que o princípio da disponibilidade seja efetivamente respeitado, utiliza-se ferramentas como firewall e backup.

Integridade: para manter uma informação de forma íntegra, nenhum dado pode ser alterado indevidamente, devendo ser definido que somente poderão ser alterados por pessoas autorizadas.

Confidencialidade: este pilar da segurança da informação prevê que devem ser definidos membros específicos da equipe para obter acesso ao conjunto de dados sigilosos. Isso chama-se possuir uma devida gestão de acesso dentro da empresa, nas quais somente os responsáveis por elas poderão acessá-las. A criptografia é uma das melhores técnicas utilizadas para manter a rigorosa segurança da confidencialidade.

Autenticidade: de acordo com esse princípio, a informação deve possuir veracidade quanto a sua autoria, desse modo, operações realizadas nas condições iniciais devem ocorrer de forma autêntica, não devendo alterar a sua origem. A Biometria, Assinatura e Certificados Digitais possuem um nível elevado de autenticidade.

Criptografia: é um método de codificação das informações, garantidor da confidencialidade, que tem como finalidade evitar que essa seja compreendida por pessoas que não possuem o devido acesso.

Controle de Acesso: é um conjunto de procedimentos e meios utilizados com o objetivo de bloquear ou conceder o acesso às informações a um grupo específico.

Lei Geral de Proteção de Dados Pessoais: a lei 13.709/18 dispõe sobre como deverá ocorrer o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou jurídica, de direito público ou privado.

Dados Pessoais: todo e qualquer dado relacionado a pessoa natural identificada ou identificável, como disposto no art. 5°, I, da Lei Geral de Proteção de Dados.

Dados pessoais identificados: São aqueles em que a informação é ligada diretamente à pessoa que os possui, permitindo sua identificação. Como exemplo: o nome completo, o CPF, o RG, a CNH e muitos outros.

Dados pessoais identificáveis: Estes dados não permitem chegar diretamente ao reconhecimento da pessoa que os possui, porém dentro de um contexto de informações é possível chegar em sua identificação. Por exemplo: o IP do computador, a profissão, o estado civil, o endereço residencial e muitos outros.

Dados pessoais sensíveis: São os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural;

Tratamento de Dados: de acordo com a LGPD, é toda operação realizada como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Terceiros: parceiros comerciais da Consultoria, como por exemplo, prestadores de serviços.

4. RESPONSABILIDADE

Prezar pela Segurança da Informação dentro da Consultoria é dever de todos os consultores, colaboradores, funcionários, prestadores de serviços e demais membros da equipe, assim como agir em consonância com as medidas de segurança e prevenções necessárias no dia a dia.

A atividade de prezar pela Segurança da Informação se trata de uma prática imprescindível para manter a privacidade e proteção de todo conjunto de elementos contidos no banco de dados da empresa, bem como a leitura e reprodução das regras e obrigações dispostas nesta Política.

5. INFORMAÇÕES

Informações são os dados que devidamente organizados e analisados, produzem um conhecimento relevante o qual transmite um significado que gera compreensão dentro de um contexto específico.

A Consultoria, para cumprir com seu objetivo como empresa que presta serviços de consultoria em investimentos, necessita tratar Informações e também Dados Pessoais com diferentes e específicas finalidades.

Além disso, Dados Físicos podem ser utilizados e armazenados no banco de dados da empresa para fins de cadastro e inserção de novos membros na Consultoria.

Considerando que prezamos pela efetividade do compromisso de assegurar a proteção e privacidade de toda e qualquer informação tratada pela empresa;

Considerando os princípios já estabelecidos nesta Política e na Lei Geral de Proteção de Dados, define-se abaixo, de modo exemplificativo e não taxativo, os objetivos acerca do tratamento de Informações e Dados pela empresa, sendo eles:

- Entrar em contato com seus clientes ou possíveis clientes com o intuito de dar sequência nas atividades e relacionamento comercial;
- Realizar o atendimento no site oficial, seja referente a dúvidas quanto aos serviços fornecidos pela empresa, como para atender às diferentes solicitações dos Titulares dos Dados;
- Divulgar os conteúdos e serviços disponibilizados pela Consultoria, podendo ser distribuídos por meio de campanhas e eventos;
- Selecionar novos colaboradores a compor a empresa, por intermédio de um processo seletivo no qual é enviado o currículo do candidato, contendo suas informações pessoais.

6. GESTÃO DA INFORMAÇÃO

Todas as informações que circulam pela Consultoria são confidenciais por definição, salvo disposição ou regulação interna que obrigue sua divulgação. Todos os consultores e colaboradores da equipe devem obter treinamento frente à Proteção

de Dados, bem como zelar pela manutenção de níveis de confidencialidade adequados. Quaisquer informações obtidas ou geradas pela Consultoria e terceiros são classificadas nos seguintes níveis:

Confidencial: É o nível mais alto de segurança dentro deste padrão. São aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Consultoria. São protegidas por rigorosos controles de acesso e criptografia.

Restrita: É o nível intermediário de confidencialidade. São informações estratégicas que devem possuir gestão de acesso. Esses dados são protegidos por controle de acesso a sistemas em nuvem.

Uso interno: Representa baixo nível de confidencialidade. São aquelas que não podem ser divulgadas para pessoas que sejam de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente ao princípio da Integridade.

Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

7. ATAQUES A SEGURANÇA DA INFORMAÇÃO E PREVENÇÕES

São inúmeros os exemplos de ataques existentes que afetam a segurança da informação de uma instituição. De acordo com isso, surge a necessidade da adoção de medidas técnicas e administrativas que previnam essas invasões a redes, sistemas e até mesmo a documentos físicos. Alguns ataques são mais recorrentes e notórios do que outros, sendo eles:

Phishing: Na tradução, "Pescaria" é um tipo de ataque cujo objetivo é pescar informações, como o próprio termo dispõe. O intuito do ataque é captar rapidamente, sendo a partir de um link ou corrente falsa enviados à vítima, bem como mensagens falsas do Banco ou instituição parceira que a pessoa/empresa utilize.

Para realizar a prevenção deste ataque, é necessário levar em consideração alguns métodos e análises como:

- Suspeitar de links e ofertas muito alarmantes, contendo promoções fora do normal;
- Saber que instituições confiáveis normalmente não solicitam dados pessoais por mensagem ou e-mail;

- Ligar para o número da empresa o qual seja publicamente disponibilizado, a fim de confirmar a solicitação enviada;
- Utilizar antivírus e firewall.

Baiting: Neste ataque, o hacker distribui dispositivos infectados por um malware, como, por exemplo, um pendrive. Seu objetivo é que um membro da equipe curioso acabe introduzindo o dispositivo no computador da empresa e a rede de sistemas seja infectada, comprometendo a integridade e confidencialidade de todas as informações que constam nessa. Para facilitar que isso aconteça, normalmente o arquivo que contém dentro do dispositivo traz uma denominação que chama atenção e desperta curiosidade, como "Relatório estratégico do ano" ou "Planilha de bonificação futura".

Primeiramente, o modo mais adequado de não ser vítima de ataques à segurança de informação, é obtendo conhecimento dos diversos modelos e como eles ocorrem. A partir disso, existem táticas para se prevenir do Baiting, expostas na sequência:

- Cuidado com a curiosidade. Se a existência de um pendrive deixado em qualquer lugar for uma prática anormal da sua empresa, desconfie.
- Se o pendrive não for seu, não o introduza em seu computador.
- Pergunte aos demais membros de quem é o dispositivo em questão.

Visual Hacking: Essa prática se trata da coleta de informações pela visualização mal intencionada. O hacker fica atento a todo e qualquer indício de dados ou documentos que possam ser vistos e capturados, como senhas, dados pessoais ou registros financeiros.

O Visual Hacking é um dos ataques mais comuns a serem realizados, no entanto, normalmente não é posto em destaque com a mesma intensidade. O cuidado deve ocorrer e ser realmente efetivo, podendo ser realizado das seguintes maneiras:

- Não deixar o computador à vista com abas que contenham informações sigilosas abertas;
- Recolher todos os documentos gerados pela impressora;
- Manter mesas e ambientes livres de documentos com dados pessoais que sejam facilmente visíveis, incluindo em reuniões por videoconferência.
- Atuar em local reservado caso você lide com alto sigilo e confidencialidade.

Ransomware: Neste ataque em questão, quando o computador/sistema é infectado, as informações contidas são criptografadas, impedindo que qualquer pessoa acesse ou tenha conhecimento desses dados. Normalmente os hackers pedem um resgate pelos dados capturados.

Este ataque se trata de uma violação aos sistemas muito perigosa, de modo que suas informações pessoais ou de sua empresa estarão sendo vítimas de um vazamento irreversível, o qual torna toda e qualquer base de dados indistinguível a partir da criptografia. Para realizar a prevenção de que esse ataque comprometa a integridade e confidencialidade, é necessário que algumas práticas sejam executadas:

- Realizar backup regularmente;
- Manter todos os softwares da empresa atualizados;
- Utilize um antivírus renomado, o investimento em prevenção é muito necessário.

8. MEDIDAS DE SEGURANÇA

A equipe da Consultoria, bem como seus respectivos parceiros comerciais, devem ter conhecimento sobre a presente Política e seguir as diretrizes dispostas em relação à segurança da informação; necessitam também obter toda a documentação dos sistemas e serviços relacionados às suas atividades.

8.1. DOS TREINAMENTOS

Todos da Consultoria devem realizar os cursos, palestras e treinamentos referentes aos temas Segurança da Informação e Proteção de Dados disponibilizados pela empresa, de modo a cumprir com as diretrizes dispostas nesta Política Interna de Privacidade e Segurança da Informação e nas demais regulamentações internas da Consultoria.

8.2. GESTÃO DE ACESSOS

Deverão praticar rigorosamente o controle e a gestão de acesso indicados para cada setor, com o objetivo de preservar a confidencialidade das informações, podendo ser acessadas somente por membros da empresa autorizados;

8.3. AMBIENTE FÍSICO

Manter mesas e locais de desempenho das atividades limpos e livres de documentos que contenham informações expostas, visando exatamente a proteção do ataque Visual Hacking já mencionado nesta Política;

Manter computadores protegidos por senha integralmente, bem como prezar pelo cuidado das informações que você é o responsável por gerenciar.

Ao utilizar a impressora coletiva, o documento impresso deve ser imediatamente recolhido. Caso não seja mais útil, este não deve ser utilizado como folha de rascunho, devendo ser descartado.

Descarte de dados: Para manter a devida segurança em relação aos dados físicos existentes na empresa, é indicada preferencialmente a utilização de máquina fragmentadora ou de papel, quando não houver mais necessidade ou finalidade do tratamento desses pela instituição. Na falta da primeira medida, o descarte deve ocorrer de forma manual, fracionando os documentos até que não seja possível compreender o conteúdo.

8.4. CUIDADO COM SENHAS

É proibido compartilhar as senhas de acesso à rede e aos sistemas internos com os colegas e/ou terceiros, uma vez que a senha é pessoal e intransferível. Por isso, o zelo pela senha pessoal deve ser extremo, devendo ser guardada com sigilo absoluto.

Deve-se praticar as medidas de proteção e segurança das informações, respeitando as normas internas cabíveis de acesso interno e observando as seguintes disposições frente à criação de senhas:

a) Utilização de números, letras e símbolos para a emissão da senha;

b) Não abordar datas ou acontecimentos significativos; e

c) Não anotar em papéis ou documentos (físicos ou eletrônicos) que tenham acesso ao público.

Todas as atividades efetuadas são associadas ao usuário, de modo a responsabilizá-lo no caso de irregularidades ocasionadas por meio deste.

Caso a pessoa vinculada à Consultoria perca sua senha pessoal ou desconfie que alguém possa ter tido acesso a ela, deverá, imediatamente, realizar a alteração de suas credenciais e informar a Administração da empresa sobre a ocorrência de tal fato ou suspeita.

8.5. MEIOS DE CONTATO

Todos da Consultoria possuem a verificação de dois fatores ativada no aplicativo Whatsapp, no pessoal e corporativo.

Com o objetivo de proteger nossos clientes contra ataques de phishing e spoofing, a Consultoria realizou implementações de mecanismos de segurança que garantem que os e-mails enviados em nome da empresa sejam autênticos e confiáveis:

Foram adotados os mecanismos SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting, and Conformance). Com esta implementação busca-se reduzir significativamente o número de e-mails fraudulentos e melhorar a segurança das comunicações realizadas pelos sistemas da empresa.

O SPF é um mecanismo de autenticação de e-mail que permite aos servidores de e-mail verificar se uma determinada mensagem foi realmente enviada pelo domínio de origem, auxiliando a prevenir e-mails falsificados e a proteger a reputação do domínio.

O DKIM é um método de autenticação de e-mails que permite verificar se a mensagem foi realmente enviada pelo domínio indicado no cabeçalho. É utilizada criptografia assimétrica para adicionar uma assinatura digital à mensagem, que pode ser verificada pelo servidor de destino.

E o DMARC se trata de uma política de autenticação de e-mails que permite ao remetente especificar como os servidores de destino devem tratar os e-mails que não passem na verificação do DKIM ou SPF (mecanismos apresentados acima). Através do DMARC é possível definir se esses e-mails devem ser rejeitados, marcados como spam ou aceitos com um aviso.

A Consultoria está comprometida em manter a segurança e a confidencialidade das informações de seus clientes.

Nesse sentido, a Administração da Consultoria juntamente ao Encarregado pela Proteção de Dados devem agir com o objetivo de evitar incidentes de segurança no ambiente da empresa, reforçando e fomentando as práticas necessárias para a garantia da efetiva Segurança, a partir da:

I - Apuração de ações que violem quaisquer diretrizes dispostas na presente PSI;

II - Aplicação de sanções dispostas em legislação aplicável aos responsáveis pela infração acima disposta;

III - Coordenação das atividades de tratamento e resposta a eventuais incidentes de segurança ocorridos na Consultoria;

IV - Realização ações reativas que incluem recebimento de notificações de incidentes.

A Consultoria reserva-se o direito de auditar todo e qualquer tipo de sistema e/ou ativo de informação para garantir a conformidade com esta Política.

Em caso de dúvidas, sugestões, denúncias e/ou qualquer outra demanda relacionada a esta Política, entre em contato com o Encarregado pela Proteção de Dados.

9. NORMATIVAS E TERMOS

A empresa poderá implementar além da Política de Segurança da Informação, diversas normativas específicas para cada medida a ser realizada, de acordo com a necessidade. Podem ser implementadas normativas específicas sobre:

I. Acesso remoto da informação;
II. Uso de equipamentos computacionais pessoais;
III. Norma de classificação, rotulagem e manuseio da informação;
IV. Proteção contra códigos maliciosos;
V. Uso de serviços de e-mail e comunicações instantâneas;
VI. Gestão de identidade e controle de acesso;
VII. Acesso à internet e comportamento em mídias sociais;
VIII. Monitoramento de ativos e serviços da informação;
IX. Resposta a incidentes de segurança da informação;
X. Termo de uso dos sistemas internos;
XI. Norma de uso aceitável de ativos de informação;

A empresa também disponibiliza o Termo de Responsabilidade aos membros da equipe, como forma de declaração de cumprimento das obrigações impostas pelas Legislações e regulamentos internos.

10. PENALIDADES

O descumprimento de qualquer preceito deste documento ou das demais normativas e termos, inclusive a Política de Segurança Cibernética de eventual parceiro que a Consultoria se vincule, pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar a exclusão, demissão ou outras sanções, inclusive decorrentes de legislações aplicáveis.

Poderão ser aplicadas demais sanções previstas nos regimentos internos da Consultoria e de eventual corretora que a Consultoria se vincule, como suspensão do membro da equipe ou até mesmo o seu desligamento da empresa.

11. DISPOSIÇÕES FINAIS

Este documento é de uso interno da Consultoria e foi formalmente aprovado pela diretoria da empresa.

Declara-se que qualquer violação às diretrizes desta Política será visualizada de acordo com seu Capítulo 10, estando todos da Consultoria passíveis de qualquer uma das sanções previstas.

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica infrações, uma vez que a Política é disponibilizada a todos os membros da equipe da empresa. Portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a diretoria da empresa.

Deverá ser notificada imediatamente à diretoria da Consultoria qualquer suspeita de irregularidade no cumprimento das disposições desta Política, de modo que será iniciada uma investigação interna.

Reforçamos o contato do Encarregado pela Proteção de Dados, o qual pode ser acionado a qualquer momento.

É obrigatório o cumprimento de todas as diretrizes estabelecidas pelo presente documento, em concordância com a imprescindibilidade de sempre garantir a Proteção da Informação.

Ante o exposto, fica instituída a Política Interna de Privacidade e Segurança da Informação da Consultoria, tendo validade a partir de Setembro de 2026, devidamente avaliada e aprovada pela Administração e Diretoria de Compliance.

LION CONSULTORIA DE INVESTIMENTOS LTDA