TERMO DE POLÍTICA DE SEGURANÇA E PRIVACIDADE

A empresa Fiducial Consultoria e Serviços Financeiros Ltda com sede na rua Espírito Santo nº 616- 8º andar inscrita no CNPJ 22.440.788/0001-90 e suas filiais através do presente termo vem através do presente dar conhecimento e plena aplicação a **POLÍTICA DE PRIVACIDADE E SEGURANÇA** de todos os dados armazenados na empresa próprios ou de terceiros.

1- Conforme definição da norma ABNT NBR ISO/IEC 27002:2005**,** "A **informação** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente."

De acordo com a mesma norma, "**Segurança da informação** é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

a)Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;

b)Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;

c)Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."

Mediante tal embasamento e considerando o disposto em seu Planejamento Estratégico, a FIDUCIAL resolve implantar **TERMO DE POLITICA SEGURANÇA E PRIVACIDADE DE INFORMAÇÃO** conforme abaixo e passa a ter aplicação imediata:

2- TERMOS E DEFINIÇÕES

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Áreas críticas: dependências da FIDUCIAL ou de seus clientes onde esteja situado um ativo de informação relacionado a informações críticas para os negócios da empresa ou de seus clientes.

Ativo: qualquer coisa que tenha valor para a organização.

Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Informação: agrupamento de dados que contenham algum significado.

Informações críticas para os negócios da FIDUCIAL: toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais ou financeiras à FIDUCIAL ou seus clientes. Cita-se, como exemplo, uma informação que exponha ou indique dados ou informações de terceiros, sigilo bancário, diretrizes estratégicas, e contribua potencialmente ao sucesso técnico e/ou financeiro de um produto ou serviço, refira-se a dados pessoais de clientes, fornecedores, empregados ou terceirizados ou que ofereça uma vantagem competitiva em relação à concorrência.

Risco: combinação da probabilidade de um evento e de suas conseqüências.

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3.OBJETIVO

O presente documento constitui uma declaração formal da FIDUCIAL acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observado e aderidos por todos os seus empregados, estagiários, aprendizes e prestadores de serviços.

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação na Organização, estabelecendo as diretrizes a serem seguidas para implantação e manutenção e segurança de informação e dados.

4.ESTRUTURA NORMATIVA

a) **Política** : constituída do presente documento, define as regras de alto nível que representam os princípios básicos que a FIDUCIAL decidiu incorporar à sua gestão e serve como base para que as normas e os procedimentos sejam criados e detalhados;

b) **Normas** : especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política;

c) **Procedimentos** : instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da FIDUCIAL.

4.1DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Os documentos integrantes da estrutura devem ser divulgados a todos os empregados, estagiários, aprendizes e prestadores de serviços da FIDUCIAL quando de sua admissão, bem como, através dos meios oficiais de divulgação interna da empresa de maneira que seu conteúdo possa ser consultado a qualquer momento.

5.PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da empresa ou sob sua custódia como fator primordial nas atividades profissionais de cada empregado, estagiário, aprendiz ou prestador de serviços da FIDUCIAL, sendo que:

a)Os empregados devem assumir uma postura pró-ativa no que diz respeito à proteção das informações da FIDUCIAL e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade da FIDUCIAL;

b)As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

c)Assuntos confidenciais não devem ser expostos publicamente;

d)Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

e)Somente softwares homologados podem ser utilizados no ambiente computacional da FIDUCIAL;

f)Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

g)Todo usuário, para poder acessar dados das redes de computadores utilizadas pela FIDUCIAL, deverá possuir um código de acesso atrelado à uma senha previamente cadastrados, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;

h)Não é permitido o compartilhamento de pastas nos computadores de empregados da empresa. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

i)Todos os dados considerados como imprescindíveis aos objetivos da FIDUCIAL devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

j)O acesso à dependências da FIDUCIAL ou à ambientes sob controle da FIDUCIAL dispostos em dependências de seus clientes deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação ali

armazenada ou manipulada, garantindo a rastreabilidade e a efetividade do acesso autorizado;

k)O acesso lógico à sistemas computacionais disponibilizados pela FIDUCIAL deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;

l)São de propriedade da FIDUCIAL todas as criações, códigos ou procedimentos desenvolvidos por qualquer empregado, estagiário, aprendiz ou prestador de serviço durante o curso de seu vínculo com a empresa.

6.PRIVACIDADE DA INFORMAÇÃO SOB CUSTÓDIA DA FIDUCIAL

Todas as informações que estão sob custódia da FIDUCIAL, caracterizada por informações próprias ou aquelas que pertencem aos seus clientes e que são manipuladas ou armazenadas nos meios às quais a FIDUCIAL detém total controle administrativo, físico, lógico e legal são de total privacidade e segurança e não podem ser objeto de qualquer meio de divulgação.

A divulgação de qualquer informação Confidencial, pública ou interna da empresa FIDUCIAL ou de seus clientes, relacionada aos seus negócios ou contratos firmados pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à FIDUCIAL ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

7. RESPONSABILIDADES

EMPREGADOS, ESTAGIÁRIOS, APRENDIZES E PRESTADORES DE SERVIÇOS

Cabe aos empregados, estagiários, aprendizes e prestadores de serviços da FIDUCIAL cumprir com as seguintes obrigações:

a)Zelar continuamente pela proteção das informações da Organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;

b)Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da empresa e seus negócios;

c)Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

d)Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

e)Selecionar de maneira coerente os mecanismos de segurança da informação;

f)Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

g) Não efetuar qualquer copia de arquivos tendo em vista a segurança e sigilo das informações e dados;

h) Não utilizar aparelho como celular, tabletes ou outros dentro do local da operação e execução dos serviços;

i) Não utilizar bolsas, pochetes ou outro qualquer recipiente do local da execução dos serviços, tendo em vista que todos os pertences devem ser armazenados em armário antes de se adentrar no local da operação onde serão executados os serviços;

j) Não utilização de papel, caneta, lápis ou qualquer outro instrumento que possibilite a anotação de dados sigilosos no local da operação, tendo em vista que já tem disponibilizado onde devem ser armazenados qualquer informação ou anotação a ser feita;

8- DO CUMPRIMENTO

Para fins de fazer valer a politica de privacidade e segurança da empresa caberá aos gestores, gerentes, e supervisores as seguintes obrigações:

a)Requisitar informações das demais áreas da FIDUCIAL, através das diretorias, gerências e supervisões, RH, TI, Departamento Juridico com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;

b)Receber, documentar e analisar casos de violação da política e das normas normas e procedimentos de segurança da informação;

c)Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;

d) Notificar as gerências e diretorias quanto a casos de violação da política e das normas e procedimentos de segurança da informação;

e) Receber sugestões dos gestores da informação para implantação de normas e procedimentos de segurança da informação;

f) Propôr projetos e iniciativas relacionadas à melhoria da segurança da informação;

g)Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;

h)Realizar, sistematicamente, em conjunto com outros setores da empresa gestão de riscos relacionados a segurança da informação.

9- GERÊNCIAS

Cabe às Gerências:

a)Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;

b)Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

c)Sugerir procedimentos de segurança da informação relacionados às suas áreas;

d)Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas;

e)Comunicar imediatamente à Diretoria e RH eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

9.1GERÊNCIA JURÍDICA

Cabe, adicionalmente, à Gerência Jurídica:

a)Manter as áreas da FIDUCIAL informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

b)Incluir na análise e elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da FIDUCIAL;

c)Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

9.2GERÊNCIA DE RECURSOS HUMANOS

Cabe, adicionalmente, à Gerência de Recursos Humanos:

a)Assegurar-se de que os empregados, estagiários, aprendizes e prestadores de serviços comprovem, por escrito, estar cientes da estrutura normativa da FIDUCIAL e dos documentos que a compõem;

b)Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional da FIDUCAL.

9.3 GERENCIA DE TI

Cabe à área de Segurança da Informação:

a)Consolidar e coordenar a elaboração, acompanhamento e avaliação da FIDUCIAL;

b) Adotar medidas de segurança nos equipamentos e computadores da FIDUCIAL de forma a coibir que os equipamentos produzam cópias, retenção ou reprodução de informações;

c)Prover as informações de gestão de segurança da informação solicitadas pela FIDUCIAL;

d)Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;

e)Executar projetos e iniciativas visando otimizar a segurança da informação na FIDUCIAL.

9.4 DIRETORIA EXECUTIVA

Cabe à Diretoria Executiva:

a)Aprovar a política e as normas de segurança da informação e suas revisões;

d)Receber, relatórios de violações da política e das normas de segurança da informação, quando aplicável;

e)Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação.

10.AUDITORIA

Todo ativo de informação sob responsabilidade da FIDUCIAL é passível de auditoria em data e horários determinados, podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser, obrigatoriamente, aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade da FIDUCIAL ou de seus clientes de forma que se misture ou impeça o acesso à informações de propriedade ou sob responsabilidade da FIDUCIAL.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de Segurança da Informação poderá realizar monitoramento e controle pró-ativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

11. VIOLAÇÕES E SANÇÕES

11.1 VIOLAÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a)Quaisquer ações ou situações que possam expôr a FIDUCIAL ou seus clientes à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b)Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Gestor da Informação;

c)Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da FIDUCIAL ou de seus clientes;

d)A não comunicação imediata à área de Segurança da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um empregado, estagiário, aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

11.2 SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação da FIDUCIAL são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

12.LEGISLAÇÃO APLICÁVEL

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

a)Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

b)Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

c)Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

d)Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

e)Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);

f)Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

g)Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias).

O presente **TERMO DE POLITICA E SEGURANÇA DE PRIVACIDADE** passa a ter aplicação imediata a partir da presente data e deve ser objeto de conhecimento e aceite por todos os empregados, estagiários, aprendizes ou prestadores de serviços, através de Termo de conhecimento e aceite a ser firmado individualmente e passa a compor a pasta de ficha de registro dos funcionários para surta todos os efeitos práticos e jurídicos, devendo uma copia do mesmo ser anexada nos locais de operação de execução de serviços para fins de consulta.

Belo Horizonte, 14 de setembro de 2016.

FIDUCIAL CONSULTORIA E SERVIÇOS FINANCEIROS LTDA