Política de Segurança da Informação

SUMÁRIO

CONTROLE DE VERSÕES

Data	Evento	Modificações	Autor
Jan/2019	Criação		André

Política de Segurança da Informação

1. INTRODUÇÃO

A presente política foi criada com o intuito de orientar o acesso dos diretores, funcionários, estagiários e prestadores de serviços (“Agente” ou, em conjunto, “Agentes”) da Consultora, no sentido de limitá-los quanto às informações confidenciais.

As informações, atualmente, tratam-se do maior e mais importante ativo a ser protegido pelas empresas em qualquer ramo de atuação, principalmente no mercado financeiro e de capitais.

A Consultora depende de seus ativos de informação para realizar negócios e atender suas obrigações operacionais, comerciais e estratégicas.

Entendemos que sistemas de informação, bases de dados, equipamentos de tecnologia e documentos impressos são ativos de informação, sejam eles internos ou externos, e todos devem ser protegidos e preservados durante o período em que estiverem sendo utilizados ou manuseados na execução de nossos negócios.

Para efeito desta política, são considerados como “*ativos de informação*”, todas as informações em quaisquer meios (inclusive físicos) ou sistemas de informação utilizados pela Consultora, bem como todos os equipamentos e instalações onde estas informações são manuseadas, acessadas ou armazenadas.

2. OBJETIVO

O presente documento dispõe acerca da Política de Segurança da Informação (“PSI”) da GRAFOINVEST S/A (“Consultora”) tendo como objetivo estabelecer regras que orientem o controle de acesso a informações confidenciais pelos diretores, funcionários, estagiários e prestadores de serviços (“Agente” ou, em conjunto, “Agentes”) da Consultora, inclusive no seu estabelecimento de regras para a utilização de equipamentos e emails, para gravação de cópias de arquivos, para *download* e instalação de programas nos computadores da empresa, dentre outras.

3. ABRANGÊNCIA

O presente instrumento abrange todos os Agentes visando atender as necessidades dos clientes da Consultora, assegurando confidencialidade nas informações.

3. GESTÃO DE ACESSOS LÓGICOS E FÍSICOS

3.1 - ACESSO LÓGICO

- O acesso lógico aos sistemas internos e externos deve ser solicitado ao gestor da área do Agente solicitante;
- Após aprovação pelo gestor da área, cabe ao Gestor de Compliance avaliar a solicitação e conceder o acesso solicitado;
- Anualmente, ou sempre que solicitado, o Gestor de Compliance deve revisar os usuários cadastrados para deliberar sobre a manutenção, revisão ou revogação dos perfis de acesso existentes;
- Na eventualidade de transferências ou alterações de cargo, função ou área, os perfis de acesso lógico são revisados;
- Ao responsável pela gestão dos Recursos Humanos cabe a responsabilidade de informar tempestivamente, para a área de COMPLIANCE, os períodos de ausências programadas de Agentes (tais como, férias e licenças em geral, dentre outras);

3.2 - POLÍTICA DE SENHAS (REDE INTERNA CONSULTORA E SISTEMAS)

- A senha é de uso pessoal e intransferível;
- O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todos os cuidados necessários para salvaguardá-la;
- O compartilhamento de senhas somente será permitido em casos de indisponibilidade para uso individual e se aprovado prévia e formalmente pela Diretoria;
- Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em casos de desligamento, suspensão, demissão, férias ou licenças de Agentes;
- Quanto às características e complexidade, a senha:

  Deve possuir, no mínimo, 8 (oito) caracteres incluindo números, caracteres especiais e letras maiúsculas e minúsculas;

  Deverá ser alterada, compulsoriamente, a cada ano;

  Sendo nova, o usuário deverá, obrigatoriamente, alterá-la no primeiro acesso seguindo os critérios acima citados.

3.3 - ACESSO FÍSICO

- É proibida a entrada de ex-Agentes sem expressa autorização da Diretoria;
- Quaisquer terceirizados ou fornecedores somente poderão prestar os serviços solicitados com o devido acompanhamento de algum Agente da Consultora;
- Outras pessoas, além das acima mencionadas, somente podem ter acesso às dependências da Consultora com a ciência do responsável da área ou a quem este previamente autorizar;
- Agentes ou visitantes que necessitarem sair das dependências físicas portando quaisquer documentos, recursos ou materiais de propriedade da Consultora devem ser expressamente autorizados; e
- Os arquivos físicos, principalmente os que contemplam documentos e informações de clientes da Consultora, são de acesso controlado e restrito somente aos Agentes autorizados.

4. ARMAZENAMENTO E TRATAMENTO DE DADOS E INFORMAÇÕES

Cada Agente da Consultora é responsável direto pela guarda e verificação da integridade dos arquivos, documentos, planilhas, relatórios e todas as demais formas de armazenamento de dados e informações.

O arquivamento externo, quando houver, seja de mídias ou documentos físicos, deve ser objeto de formalização contratual e ser periodicamente submetido à avaliação e visita presencial;

Locais destinados ao armazenamento de informações de clientes, confidenciais ou relevantes, devem permanecer em locais (físicos ou lógicos) de acesso restrito, em segurança e devidamente organizados;

Não é permitido o uso do e-mail para o armazenamento de informações relevantes. Estas deverão ser arquivadas na rede corporativa para assegurar o efetivo procedimento de backup dos dados em caso de contingência ou incidente;

Os arquivos lógicos ou físicos com informações de clientes, confidenciais ou relevantes, devem ser descartados de forma fragmentada que não permita sua reutilização;

O envio de informações e documentos em meio físico para locais externos deve ser necessariamente protocolado (entrada e saída) e arquivado para fins comprobatórios e de rastreamento, quando necessário; e

Relatórios de auditorias, órgãos reguladores ou fiscalizadores são de propriedade da Consultora e, consequentemente, estritamente confidenciais.

4.1 – *BACKUP* DE DADOS E INFORMAÇÕES DA CONSULTORA

A prática e as rotinas diárias de *backup* visam assegurar a disponibilidade das informações geradas ou utilizadas pela empresa, devendo ser mantida cópia de segurança (i) fora do escritório principal; (ii) desconectada da rede e dentro do escritório; (iii) cópia dos 3 últimos dias uteis; e (iv) do fechamento do mês anterior.

O período de armazenamento de informações, antes do descarte definitivo, deve respeitar os prazos exigidos por leis, normas e regulamentos aplicáveis aos negócios da Consultora.

É vedada, aos usuários, a prática de armazenamento de dados e informações em disco local, cabendo aos mesmos a responsabilidade de manipular e salvar arquivos lógicos somente na rede corporativa da Consultora.

4.2 - USO DE RECURSOS DE TECNOLOGIA

A Consultora é proprietária do direito de uso de todos os recursos de tecnologia colocados à disposição dos Agentes, bem como de toda a informação criada e gerada durante as atividades profissionais ou nas dependências da empresa.

Os recursos de tecnologia da Consultora abrangem computadores, notebooks, impressoras, *scanner*, aparelhos de fax, softwares, periféricos, equipamentos de telefonia e mídias em geral.

É permitida a utilização de recursos de tecnologia que não sejam de propriedade da Consultora, desde que autorizados previamente pela Diretoria.

Os usuários de recursos portáteis deverão atestar, através de assinatura de termo de responsabilidade específico, que tomarão todos os cuidados necessários no transporte e utilização destes equipamentos e, ainda, se comprometem a cumprir a função obrigatória de armazenar, na rede corporativa, cópia de todas as informações disponíveis nestes recursos.

O bom e correto uso dos recursos de tecnologia é de responsabilidade de todos os Agentes da Consultora.

4.3 - UTILIZAÇÃO DO E-MAIL, TELEFONE E INTERNET

- O Agente deve prezar pela boa e responsável utilização de sua conta de e-mail corporativo;
- Não é permitida a utilização do e-mail, telefone e Internet para fins particulares, exceto quando previamente autorizado pela Diretoria;
- Não é permitida a utilização do e-mail para envio de mensagens em massa, correntes, convites, cartões virtuais, promoções pessoais e outros assuntos não relacionados às atividades profissionais e aos negócios da Consultora;
- Em nenhuma hipótese devem ser acessados e-mails de remetentes ou assuntos desconhecidos;
- O correio eletrônico não pode ser utilizado, sem autorização prévia e controle específico, para envio ou recepção de mensagens que contenham arquivos executáveis, macros ou sequências de comandos, explícitas ou implícitas, ou ainda outros mecanismos que possam conter vírus e, portanto, causar algum dano aos equipamentos da Consultora ou dos destinatários;
- É expressamente proibido o uso do e-mail corporativo para participação em blogs, redes sociais, serviços de webmail ou para cadastramento em sites para fins pessoais;
- É expressamente proibido o envio, recepção ou encaminhamento de mensagens com teor ofensivo, ideologias políticas, religiosas ou raciais, pornografia, apologia às drogas, terrorismo, dentre outros conteúdos impróprios;
- Somente é permitido o uso de assinaturas de e-mail conforme modelo padrão interno, previamente definido;

5. COMUNICAÇÃO DE FRAUDES E INCIDENTES

Todos os Agentes da Consultora são diretamente responsáveis pela imediata comunicação, ao responsável pelo Compliance, dos casos de eventual suspeição de fraude ou incidente que comprometa a segurança das informações da Consultora ou no caso de ocorrência de vazamento de informações ou incidente de segurança.

6. ADESÃO E TREINAMENTO

Todos os Agentes deverão, além de aderir a esta PSI, receber treinamentos anuais e materiais educativos que visem, principalmente, a plena conscientização sobre o tema.
Os novos Agentes devem ser submetidos a um treinamento inicial acerca das funções e responsabilidades profissionais, sob a coordenação do superior hierárquico.
O treinamento deve ser ministrado por profissional interno (ou terceirizado) com experiência comprovada quanto à gestão de segurança da informação.

7. PENALIDADES

A não observância do disposto nesta política interna será considerada como falta grave.

8. RESPONSABILIDADES

8.1 COMITÊ EXECUTIVO

Disseminar a importância e estar engajado quanto ao cumprimento do conteúdo desta PSI, bem como gerenciar a observância de conformidade através da revisão contínua de relatórios periódicos, participação em reuniões internas, treinamentos, dentre outras atividades.

8.2 COMPLIANCE

As principais atribuições deste segmento na Consultora, no tocante à segurança das informações, são:

- Gerenciar as ações em segurança da informação física e lógica;
- Mapear processos e descrever procedimentos e rotinas operacionais;
- Analisar potenciais ameaças e estabelecer mecanismos de controle que minimizem eventuais vulnerabilidades de segurança;
- Elaborar e atualizar regras e procedimentos referentes à segurança da informação, bem como promover a sua aplicabilidade.
- Administrar a segurança física e a prestação de serviços de manutenção e limpeza terceirizados (quando aplicável);
- Gerenciar os serviços de expedição de documentos e correspondências;
- Gerenciar os procedimentos inerentes à identificação de Agentes, terceiros e visitantes da Consultora;
- Assegurar a segurança e bom uso dos locais destinados para armazenamento de documentos, mídias, dentre outros, em especial nos ambientes onde há compartilhamento de informações para que tenham acesso restrito;

- Comunicar e atualizar, tempestivamente, todas as informações referentes à movimentação de pessoal, em especial no caso de saída de colaboradores;
- Efetuar o registro e o controle formal dos treinamentos anuais.
- Providenciar a adesão a termos de confidencialidade e normas internas da Consultora de todos os novos Agentes e/ou demais profissionais terceirizados, quando for o caso.

8.3 TECNOLOGIA

O Gestor de Tecnologia, mesmo quando terceirizado, se reporta diretamente a Diretoria de Riscos e suas principais funções são:

- Desenvolver programas regulares de avaliação de riscos de tecnologia com acompanhamento direto da Diretoria de Riscos;
- Seguir procedimentos rígidos que garantam a base tecnológica para recuperação de desastres e continuidade dos negócios da Consultora;
- Homologar novos recursos de tecnologia, para a segurança das informações, conforme definido pela empresa;
- Realizar gravação telefônica dos ramais necessários e o *backup* diário de informações, mantendo em arquivo seguro e organizado durante os prazos legais e as normas internas;
- Criar processos que garantam a verificação dos registros de atividades ("*logs*") em todos os sistemas e recursos de tecnologia e dados; e
- Informar, registrar e tratar incidentes de tecnologia relacionados à segurança das informações ou continuidade dos negócios.

8.4 JURÍDICO

As principais atribuições deste segmento na Consultora, no tocante à segurança das informações, são:

- Revisar contratos garantindo a existência de cláusulas referentes à confidencialidade e segurança das informações; e
- Elaborar termos de confidencialidade e responsabilidade.

8.5 RELAÇÃO COM INVESTIDORES

A principal atribuição deste segmento na Consultora, no tocante à segurança das informações, consiste em assegurar a confidencialidade das informações e documentos pessoais de clientes sob sua responsabilidade.

9. CONSIDERAÇÕES FINAIS

Estamos comprometidos e cientes de que a implementação de uma estrutura de controles formal para gerir a segurança de nossas informações (e dos nossos clientes) é um passo essencial para estabelecer os níveis de controle e responsabilização necessários para preservar os ativos de informação e constituir um diferencial aos nossos negócios.

Seguindo os conceitos das boas práticas de controles e de segurança da informação, esta política interna da Consultora foi elaborada com o intuito de prezar pela segurança, bom uso e acesso controlado a determinadas informações, recursos e pessoas.

Nesse sentido, todos os Agentes da Consultora firmarão o Termo de Adesão anexo ao presente documento (Anexo I), tomando conhecimento e expressamente anuindo com o conteúdo do mesmo.

ANEXO I

TERMO DE ADESÃO - POLITICA DE SEGURANÇA DA INFORMAÇÃO

Eu, _____, portador(a) da Cédula de Identidade nº _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que:

Em _____ de _____ de _____ participei do treinamento específico realizado em consonância com o Manual de Política de Segurança da Informação da GRAFOINVEST S/A, sendo que compreendi perfeitamente as regras estabelecidas no referido Manual e aderi aos mesmos, comprometendo-me a observar integralmente todos os termos e condições da Política de Segurança da Informação.

2. Tenho pleno conhecimento de que a não observância dos termos ou das condições elencados no Manual de Política de Segurança da Informação poderá resultar na caracterização de falta grave, o que implicará na aplicação das penalidades cabíveis, inclusive demissão por justa causa.

Rio de Janeiro (RJ), _____ de _____ de _____.

Nome Completo:

CPF:

Assinatura: _____