SEQUOIA PROPERTIES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I. – OBJETIVO

Artigo 1º – O objetivo desta Política de Segurança da Informação ("**Política de TI**") é estabelecer o conjunto procedimentos que devem ser observados pela SEQUÓIA para preservar a segurança, integridade e confidencialidade das informações detidas pela SEQUÓIA.

CAPÍTULO II. – ACESSO ÀS DEPENDÊNCIAS DA SEQUÓIA

Artigo 2º – O livre acesso às dependências da SEQUÓIA é restrito aos Colaboradores e compreende o ingresso dos Colaboradores no edifício no qual a SEQUÓIA se encontra localizada e o ingresso dos Colaboradores nas instalações próprias da SEQUÓIA, sendo que, nos termos do Código, a área de administração de recursos de terceiros da SEQUÓIA é segregada fisicamente das demais áreas da SEQUÓIA, sendo de acesso restrito aos respectivos colaboradores.

Parágrafo Primeiro – O ingresso dos Colaboradores no edifício é realizado por meio de cartões eletrônicos de uso pessoal e intransferível. Ademais, o edifício conta com câmeras de vigilância e seguranças familiarizados com os funcionários do edifício.

Parágrafo Segundo – O ingresso dos Colaboradores nas instalações próprias da SEQUÓIA é realizado em dois atos mediante a utilização de senha de abertura de portas de conhecimento apenas dos Colaboradores, e é acompanhado por câmeras de vigilância.

CAPÍTULO III. – ACESSO ÀS INFORMAÇÕES DETIDAS PELA SEQUÓIA

Artigo 3º – As informações digitais detidas pela SEQUÓIA são mantidas em uma rede de uso exclusivo da SEQUÓIA, cujo acesso é restrito aos Colaboradores, e é realizado por meio da utilização de ***login*** e **senha** de uso pessoal e intransferível, sendo que, nos termos do Código, a informação alcançada em função da atividade profissional desempenhada por cada Colaborador não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

Parágrafo Primeiro – As informações detidas pela SEQUÓIA por meio documentos físicos em geral são mantidas em arquivos localizados em sala própria localizada nas instalações da SEQUÓIA.

Parágrafo Segundo – Os Colaboradores são integralmente responsáveis por todas as ações e atividades realizadas por intermédio de seu *login* e senha de acesso.

Parágrafo Terceiro – É exigida a alteração da senha de acesso dos Colaboradores a cada 6 (seis) meses.

Parágrafo Quarto – Sem prejuízo dos Parágrafos acima, as ações e atividades dos Colaboradores na rede da SEQUÓIA devem observar as seguintes orientações e diretrizes:

(a) **Acesso às pastas.** Todo arquivo de trabalho deve estar em uma das pastas do servidor central. Arquivos de trabalho no drive local (C:) não são permitidos, com exceção do arquivo ".pst" do Microsoft Outlook, por razões técnicas;

(b) **Programas**: Todo programa só pode ser instalado pela área de Tecnologia;

(c) **Correio eletrônico:** Deve ser utilizado apenas para atividades profissionais. Pastas de correio eletrônico diferentes da Inbox ("pastas pessoais" no jargão Microsoft) devem ser armazenadas na rede, no diretório U: ("usuários"), sob a pasta pessoal;

(d) **Acesso à internet:** O acesso à internet é monitorado por *login* e sujeito a filtros de conteúdo. Deve ser utilizado apenas para atividades profissionais, sendo proibido:

(i) o acesso a conteúdo pornográfico, de jogos, relacionamentos, conteúdo de *hackers*, *proxys*, conteúdo racista ou discriminatório de qualquer natureza;

(ii) a utilização de *softwares* P2P e *torrent* como Emule, Kazaa, Vuze e outros; e

(iii) *download* de filmes, músicas, seriados, jogos e *softwares*;

(e) **Messenger:** Apenas as contas de "**Usuários Designados**", assim definidos os usuários constantes da lista arquivada com o Assistente Administrativo, têm acesso autorizado ao Messenger, mediante gravação de toda a conversação, sendo proibido:

(i) postar mensagens de cunho discriminatório, difamatório, ou de qualquer maneira ilegal; e

(ii) representar a SEQUÓIA fora da função específica a que se destina;

(f) ***Pen Drive*:** Apenas Usuários Designados podem utilizar *pen drive* sem restrições;

(g) **CD-ROM:** Apenas Usuários Designados têm dispositivo de gravação habilitado;

(h) **Dispositivos de impressão:** Há um dispositivo de impressão por área. Cada estação de trabalho deve mapear exclusivamente o dispositivo de impressão da sua área, exceto as estações de trabalho dos Usuários Designados, as quais poderão ter acesso a todos os dispositivos de impressão, inclusive para ter acesso aos dispositivos de impressão de alta qualidade;

(i) **Acesso remoto à rede da SEQUÓIA (VPN):** Apenas Usuários Designados podem ter acesso à VPN, sendo que, considerando a potencial vulnerabilidade da estação remota (VPN), o seu uso pelos Usuários Designados deve ser parcimonioso.

Parágrafo Quinto – Eventual infração às orientações e diretrizes estabelecidas no Parágrafo anterior será devidamente investigada e esclarecida pelo Representante Compliance, e todos os envolvidos serão advertidos e passíveis de punições a serem definidas pelo Representante Compliance.

CAPÍTULO IV. – PROCEDIMENTOS DE *BACKUP* DE INFORMAÇÕES

Artigo 4º – Todas as informações do servidor da SEQUÓIA, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com *backup*.

Parágrafo Primeiro – Os serviços de *backup* de informações utilizados pela SEQUÓIA no desempenho de suas atividades são:

(a) ***Backup InSite*.** Incremental mensal por mínimo de 6 (seis) meses, com finalidade de recuperar arquivos acidentalmente perdidos;

(b) ***Backup OffSite*.** *Backup* para disco rígido removível (criptografado, protegido por senha), armazenado em local diferente do *site* principal e do *site* de contingência ou em servidor externo (criptografado, protegido por senha) acessível remotamente (“Nuvem”); e

(c) ***Backup* de correio eletrônico no servidor.** No servidor externo, e juntamente com os *backups* de rede sendo obrigatória a cópia pelos usuários dos arquivos “.pst” para a rede.

Parágrafo Segundo – Em nenhuma circunstância os equipamentos de *Backup OffSite* e *site* de contingência poderão estar ao mesmo tempo no *site* principal.

CAPÍTULO V. – CONTINUIDADE DE NEGÓCIOS

Artigo 5º – A continuidade dos negócios da SEQUÓIA deverá ser preservada de acordo com os seguintes planos de contingência:

(a) ***Link* de contingência.** *Link* de internet redundante a ser acionado em caso de queda do *link* principal;

(b) **Contingência de correio eletrônico.** Conta de correio eletrônico de provedor com reputação internacional e, eventualmente, serviço FTP em caso de interrupção do serviço de correio eletrônico; e

(c) **Queda de energia.** *No-breaks* para servidor de arquivo para, no mínimo, 15 (quinze) minutos.

CAPÍTULO VI. – ROTINA DE TESTES

Artigo 6º – A SEQUÓIA adota a seguinte rotina de testes, sob a supervisão do Representante Compliance:

(a) **Teste do *site* de Contingência**:

(i) realizadas aleatoriamente, com frequência esperada trimestral, as rotinas essenciais (liberação de quota, SMA) deverão ser feitas do *Site* Nível I, do qual será desconectada a energia elétrica.

(ii) realizadas aleatoriamente, com frequência esperada trimestral, as rotinas essenciais (liberação de quota, SMA) deverão ser feitas do *Site* Nível II.

(b) **Teste de gravação de telefonia**: A SEQUÓIA se reserva no direito de gravar qualquer ligação telefônica dos Colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela SEQUÓIA para a atividade profissional de cada Colaborador.

CAPÍTULO VII. – GRAVAÇÃO DE COMUNICAÇÕES

Artigo 7º – A SEQUÓIA, por meio do Representante Compliance, monitorará o trafego de informações através de suas redes de comunicação, ou seja, *internet* e correio eletrônico, observado o quanto segue:

(a) comunicações via Messenger são gravadas por rotina específica; e

(b) os acessos feitos pela internet são gravados pelo servidor, com identificação do Colaborador que realizou o acesso e o destino.

CAPÍTULO VIII. – SEGURANÇA CIBERNÉTICA

Artigo 9º – A SEQUÓIA deverá indetificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Código Anbima de Segurança Cibernética definiu que os ataques mais comuns de criminosos cibernéticos (cybercriminals) são os seguintes:

i. Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
ii. Engenharia Social;
iii. pharming;
iv. Phishing scam;
v. ishing;
vi. Smishing;
vii. Acesso pessoal;
viii. Ataques de DDoS e botnets; e
ix. Invasões (advanced persistent threats).

Parágrafo Primeiro – A SEQUÓIA adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A SEQUÓIA trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário. Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Parágrafo Segundo – Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a SEQUÓIA deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

Parágrafo Terceiro – A SEQUÓIA conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas. A SEQUÓIA realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

Parágrafo Quarto – Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na SEQUÓIA ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o

expediente da SEQUÓIA, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Área de Gestão de Riscos e de Compliance e/ou por prestador de serviços externo.

Artigo 10º – *Monitoramento e Testes.* Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da SEQUÓIA, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

Parágrafo Primeiro – A SEQUÓIA possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.

Parágrafo Segundo – Periodicamente, a SEQUÓIA realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, em linha, inclusive, com o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da SEQUÓIA. Dentre as medidas, incluem-se, mas sem se limitar:

i. Verificação dos logs dos Colaboradores;
ii. Alteração periódica de senha de acesso dos Colaboradores;
iii. Segregação de acessos;
iv. anutenção trimestral de todo os hardwares; e
v. Backup diário, realizado na nuvem.

Parágrafo Terceiro – Sem prejuízo dos testes realizados na forma do Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da SEQUÓIA, a SEQUÓIA realizará simulações de ataques e respostas da SEQUÓIA que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da SEQUÓIA, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

Parágrafo Quarto – O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da SEQUÓIA, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência. As rotinas de backup são periodicamente monitoradas.

Artigo 10º – *Plano de resposta*. Havendo indícios ou de suspeita fundamentada, O Representante Compliance e a empresa responsável pela segurança digital deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Parágrafo Primeiro – Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Parágrafo Segundo – Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado. Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de Compliance e Código de Ética e Conduta.

Parágrafo Terceiro – Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos e de Compliance. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que sumariamente, constar no Relatório de Controles Internos.

CAPÍTULO IX. – TREINAMENTO

Artigo 11º – Em decorrência desta Política de TI, os Colaboradores receberão treinamento interno apropriado relativo às disposições desta Política de TI, o qual compreenderá, inclusive, mas não se limitando, conceitos relativos à segurança da informação, negociação por detentores de informação privilegiada e segregação de informação.

Parágrafo Primeiro – O treinamento será realizado pelo menos uma vez por ano, em data a ser determinada pela SEQUÓIA, sendo que a presença de todos os Colaboradores obrigatória.

Parágrafo Segundo – Cada Colaborador assinará uma declaração de que participou do treinamento.