POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA (PSI) DO BENÍCIO ADVOGADOS ASSOCIADOS

1. INTRODUÇÃO

A Política de Segurança da Informação e Segurança Cibernética ("PSI" ou "Política") é o documento que orienta e estabelece as diretrizes do Benício Advogados Associados ("BA" ou "Escritório") para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

Os princípios de Segurança da Informação e Segurança Cibernética aqui estabelecidos possuem aval e total aderência da alta administração do Escritório, devendo ser observados por todos os colaboradores, clientes e parceiros, ao executarem suas funções e ao se relacionarem com o BA.

2. NORMAS

A PSI do BA está fundamentada nas recomendações da família de normas técnicas ABNT NBR ISO/IEC 27000 em suas versões mais recentes.

3. ESCOPO

A PSI tem por escopo a proteção da informação contra vários tipos de ameaças, no intuito de garantir a continuidade do negócio, minimizar seus riscos, maximizar as oportunidades de negócio, abrangendo três propriedades básicas:
(i) Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
(ii) Integridade: Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;
(iii) Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

4. OBJETIVO GERAL

A PSI tem como objetivo dar as diretrizes gerais para o estabelecimento de políticas e procedimentos que assegurem a segurança das informações, sem impedir ou dificultar os processos internos do Escritório, mas garantindo:
(i) A preservação da confidencialidade, da integridade e da disponibilidade dos dados de propriedade ou sob a guarda do Escritório;
(ii) O compromisso do BA com a proteção das informações de sua propriedade e/ou sob sua guarda;
(iii) A participação e o cumprimento por todos os colaboradores em todo o processo.

5. OBJETIVOS ESPECÍFICOS

A PSI visa orientar a alta administração e todos os colaboradores do BA em ações aptas para dar concretude à Segurança da Informação dentro do Escritório. Para o pleno alcance deste intento, estabelecem-se os seguintes objetivos específicos da PSI:
(i) Constituição de Comitê de Gestão da Informação do BA, em até 03 (três) dias úteis após a aprovação da PSI pela alta administração;
(ii) Aprovação de "Política de Gestão de Documentos", em até 30 (trinta) dias úteis após a constituição do Comitê previsto no item (i);
(iii) Aprovação de "Política de Privacidade de Dados Pessoais", em até 30 (trinta) dias úteis após a constituição do Comitê previsto no item (i);
(iv) Aprovação de "Procedimento(s) Operacional(ais) Padrão" que seja(m) capaz(es) de criar rotinas específicas de Segurança da Informação, para divulgação e treinamento junto a todos os nossos colaboradores;
(v) Ajuste e reajuste de todo o ferramental institucional – plataformas virtuais, documentos, formulários, contratos e outros documentos – a esta PSI e às Políticas dos itens (ii) e (iii), em até 90 (noventa) dias úteis após a aprovação das Políticas previstas em (ii) e (iii);
(vi) Treinamento de todos os colaboradores do BA, em até 60 (sessenta) dias úteis após a aprovação do(s) Procedimento(s) previsto(s) no item (iv);
(vii) Revisão anual, por parte do Comitê previsto no item (i), desta Política, das Políticas dos itens (ii) e (iii) e do(s) Procedimento(s) do item (iv), com necessidade de divulgação irrestrita das alterações perpetradas e treinamento compulsório dos colaboradores, caso as alterações comportem alterações no(s) Procedimento(s) previsto(s) no item (iv).

6. PRINCÍPIOS GERAIS DE SEGURANÇA DA INFORMAÇÃO ADOTADOS PELO BA

São princípios norteadores da PSI do Escritório:
(i) toda informação de propriedade ou sob a guarda do BA deve ser protegida de forma a não comprometer sua confidencialidade, integridade e disponibilidade, independentemente da forma ou meio pelo qual é coletada, armazenada ou compartilhada;
(ii) os acessos às informações são realizados somente mediante autorização do responsável pela informação e são restritos a pessoas autorizadas;
(iii) todo colaborador do BA possui um *login* pessoal e intransferível, capaz de identificar de maneira inequívoca seu detentor, para que tenha acesso às informações de propriedade ou sob a guarda do BA;
(iv) o Escritório tem controles para prevenir que vírus e outros tipos de *softwares* maliciosos entrem e se espalhem nos sistemas de informação por meio de arquivos e *softwares* não homologados e cuja instalação e uso são proibidos;
(v) o Escritório conta com procedimentos específicos para garantir a recuperação de dados e informações quando necessário;
(vi) o Escritório adota práticas orientadas aos colaboradores, a fim de que não deixem informações à mostra e as descartem sempre que necessário;
(vii) todos os contratos firmados com o BA possuem cláusula de confidencialidade;

(viii) o Escritório utiliza somente *softwares* validados e equipamentos configurados de acordo com o padrão do BA;
(ix) o Escritório tem controles que previnem o vazamento de informações e boas práticas para uso de correio eletrônico, acesso à internet, acesso remoto, uso de telefones, inclusive móveis, e impressoras, comportamento dos colaboradores e na troca de informações com clientes e parceiros.

7. SEGURANÇA CIBERNÉTICA

A Segurança Cibernética do Escritório é responsável por identificar, proteger, detectar, responder e recuperar-se rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.
Incidentes de Segurança Cibernética, caso ocorram, serão analisados e classificados de acordo com o grau de impacto do incidente.

8. CLASSIFICAÇÃO DAS INFORMAÇÕES

Para fins da Segurança da Informação e das Políticas afetas ao tema, inclusive a presente, as informações de propriedade e/ou guarda do BA devem ser classificadas em:
(i) Públicas: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não é a ninguém comprometedora e que, por isso, não necessitam de proteção efetiva ou tratamento específico;
(ii) Internas: são informações disponíveis aos colaboradores do Escritório para a execução de tarefas rotineiras, não se destinando ao público externo;
(iii) Confidenciais: são informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação poderá violar a privacidade de indivíduos ou violar cláusula de confidencialidade;
(vi) Restritas: são informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente constam como destinatários exclusivos das informações.

9. DAS RESPONSABILIDADES DOS COLABORADORES

Sem prejuízo de responsabilidades oriundas de outras diretrizes, inclusive legais, a presente PSI erige como responsabilidades mínimas de seus colaboradores e da alta administração do Escritório:
(i) Cumprir fielmente todas as diretrizes, normas, Políticas, cláusulas e procedimentos relacionados à Segurança da Informação;
(ii) Buscar membros do Comitê de Gestão da Informação para esclarecimentos de dúvidas referentes à PSI;
(iii) Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizadas;
(iv) Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Escritório;

(v) Descarte adequado de documentos de acordo com seu grau de classificação;
(vi) Comunicar prontamente à chefia imediata ou a qualquer membro do Comitê de Gestão da Informação violações a esta Política;
(vii) à alta administração, diretores, gestores e chefias, compete especialmente: ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão; dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento desta PSI; exigir de parceiros, prestadores de serviços, clientes e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso; elaborar e aprovar, se necessário, os Procedimentos Operacionais Padrão que tratem de Segurança da Informação das suas áreas, fornecendo as informações necessárias e mantendo-as atualizadas; informar, sempre que necessário, de forma imediata, alterações ou atualizações referentes a processos e/ou cadastros de colaboradores concedidas ou revogadas;
(viii) aos membros do Comitê de Gestão da Informação, compete especialmente: elaborar, aprovar e propor alterações, atualizações ajustes à PSI; propor e aprovar investimentos relacionados à Segurança da Informação no intuito de minimizar cada vez mais os riscos; propor classificação e reclassificação de informações, sempre que necessário; avaliar incidentes de segurança, tomar e propor ações corretivas;
(ix) aos membros da equipe de Tecnologia da Informação ("TI"), compete especialmente: definir as regras para instalação de *hardware* e *software* no âmbito do Escritório; homologar equipamentos do Escritório e equipamentos pessoais para uso na rede do BA; monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a presente PSI e todas as diretrizes aplicáveis, inclusive legais; manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações; propor metodologias e processos referentes à Segurança Cibernética, especialmente a respeito da avaliação de riscos e vulnerabilidades; ocuparem, como membros naturais, posições dentro do Comitê de Gestão da Informação.

10. UTILIZAÇÃO DA REDE DO BA

O ingresso à rede interna do BA deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidades das informações sejam minimizadas.
(i) A *Internet* cabeada estará disponível apenas para máquinas e equipamentos de propriedade do BA, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores;
(ii) A *Internet* sem fio deverá ser segregada, garantindo o isolamento da rede interna, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas;
(iii) O BA reserva-se o direito de monitorar e registrar o acesso à *Internet* como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

(iv) Os equipamentos, tecnologias e serviços fornecidos para o acesso à *Internet* são de propriedade do BA, que pode analisar e, se necessário, bloquear arquivos, *sites*, correios eletrônicos, domínios ou aplicações, visando assegurar o cumprimento desta PSI;
(v) A *Internet* disponibilizada pelo BA aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada pela chefia e que não prejudique o andamento dos trabalhos rotineiros;
(vi) Apenas colaboradores devidamente autorizados a falar em nome do BA para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por *e-mail*, entrevista *on-line*, documento físico, ligação telefônica, etc.;
(vii) É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a Internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
(viii) Os colaboradores com acesso à *Internet* só poderão fazer o *download* de programas necessários às suas atividades no BA e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pelo Comitê Gestor da Informação;
(ix) O uso, a cópia ou a distribuição não autorizada de *softwares* que tenham direitos autorais, marca registrada ou patente são expressamente proibidos;
(x) Os colaboradores não poderão em hipótese alguma utilizar os recursos do Escritório para fazer o *download* ou distribuição de *software* ou dados pirateados ou para suporte à prática de qualquer atividade considerada delituosa de acordo com a legislação nacional;
(xi) Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de *bypass* de *firewall*;
(xii) Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando o Comitê Gestor da Informação deverá estar devidamente ciente e concedido autorização específica;
(xiii) Não é permitida a alteração das configurações de rede e inicialização das máquinas, bem como modificações que possam trazer algum problema futuro;
(xiv) Haverá geração de relatórios de sites, downloads, telefonemas e impressões por usuário;
(xv) A utilização remota da rede interna poderá ser autorizada pelos membros do Comitê Gestor da Informação que também sejam membros do setor de TI, desde que autorizado pelo gestor/chefia imediata do colaborador solicitante e que o TI configure o dispositivo pessoal do colaborador para o acesso remoto seguro; é vedado ao colaborador armazenar arquivos em pastas não compartilhadas, sendo preferencial o armazenamento nas pastas compartilhadas da própria rede do Escritório; o armazenamento em nuvens deverá se dar somente em caso de impossibilidade técnica de armazenamento na rede interna e sempre na forma compartilhada e mediante controle de acesso através de senhas.

11. POLÍTICA DE LOGINS, SENHAS e E-MAILS CORPORATIVOS

Em relação aos *logins*, senhas e *e-mails* corporativos, ficam estabelecidas as seguintes regras:
(i) A senha é pessoal e intransferível, de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
(ii) A senha inicial só será fornecida ao próprio colaborador, preferencialmente de forma presencial; caso seja necessário transmiti-la por outros meios, deve-se garantir sua inequívoca indevassabilidade;
(iii) É proibido o compartilhamento de *login* para funções de administração de sistemas;
(iv) As senhas não devem ser anotadas;
(v) As senhas deverão seguir seguintes pré-requisitos de segurança definidos pela equipe de TI;
(vi) O acesso do usuário deverá ser imediatamente cancelado pela equipe de TI e sob requisição da chefia/gestor ou do RH nas seguintes situações: (a) desligamento do colaborador; (b) mudança de função do colaborador que reflita diferentes graus de acessibilidade às informações detidas ou sob a guarda do Escritório; (c) quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação;
(vii) O *e-mail* corporativo é destinado a fins profissionais e relacionados às atividades dos colaboradores;
(viii) Os *e-mails* enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear *spams*, *malwares* ou outros conteúdos maliciosos que violem esta PSI;
(ix) É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo "corrente", campanhas ou promoções;
(x) É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
(xi) É proibido enviar qualquer mensagem por meios eletrônicos que torne o Escritório vulnerável a ações civis ou criminais;
(xii) É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
(xiii) É proibido produzir, transmitir ou divulgar mensagem que: (a) contenha ameaças eletrônicas, como: *spam, phishing, mail bombing, malwares*; (b) contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, a menos que expressamente autorizado pela chefia/gestor ou membro da equipe de TI; (c) vise obter acesso não autorizado a outro computador, servidor ou rede; (d) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; (e) vise burlar qualquer sistema de segurança; (f) vise vigiar secretamente ou assediar outro usuário; (g) vise acessar informações confidenciais sem autorização expressa de seu titular ou da chefia/gestor; (h) venha conteúdo considerado impróprio, obsceno ou ilegal; (i) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros; (j) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;
(xiv) O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando: (a) não contrariar as normas estabelecidas nesta PSI; (b) não interferir negativamente nas atividades profissionais individuais ou nas de outros colaboradores; (c) não interferir negativamente no BA e em sua imagem.

12. ESTAÇÕES DE TRABALHO E IMPRESSORAS

São medidas de segurança que devem ser tomadas para o uso das estações de trabalho e impressoras do BA:
(i) É de responsabilidade do colaborador do equipamento zelar pelas estações, mantendo-as em boas condições;
(ii) Não é permitido personalizar os equipamentos;
(iii) É vedada a abertura de equipamentos, para qualquer tipo de reparo, que deverão ser feitos exclusivamente por membros da equipe de TI ou terceirizados contratados especificamente para este fim;
(iv) As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas;
(v) É proibida a instalação de *softwares* ou sistemas nas estações de trabalho pelos usuários finais, sem que haja autorização expressa de membro da equipe de TI, com anuência da chefia/gestor imediato;
(vi) É proibida a instalação de *softwares* que não possuam licença e/ou não sejam homologados pela equipe de TI;
(vii) As estações de trabalho devem permanecer bloqueadas (*logoff*) nos períodos de ausência do colaborador;
(viii) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
(ix) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
(x) É proibido o uso de estações de trabalho para: (a) tentar ou obter acesso não autorizado a outro computador, servidor ou rede; (b) burlar quaisquer sistemas de segurança; (c) interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; (d) cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular; (e) hospedar pornografia, material racista, homofóbico, misógino ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
(xi) A equipe de TI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição, a menos que seja nas condições taxativamente previstas nesta PSI;
(xii) As estações de trabalho possuem códigos internos que permitem sua identificação na rede; assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário da estação de trabalho no momento da execução sob referência;
(xiii) É proibida a impressão e xerox de documentos de cunho pessoal e/ou ilegal;
(xiv) A configuração e manutenção das impressoras só podem ser realizadas por membros da equipe de TI;
(xv) A instalação das impressoras deverá ser realizada necessariamente através de servidor próprio, sendo proibida a instalação por vias diretas através da rede;

(xvi) Um membro da equipe de TI de cada setor/unidade será o responsável pelas impressoras localizadas naquele setor, inclusive para responder a questionamentos como impressões/xerox excessivas ou não autorizadas, sem prejuízo da responsabilização do colaborador que efetivamente tiver executado as rotinas de impressão.

13. BACKUPS

Todo sistema ou informação relevante para o funcionamento do Escritório deverá possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição.

Membros do Comitê de Gestão da Informação, da alta administração e as chefias/gestores das áreas são igualmente responsáveis por deflagrarem a instauração de procedimentos de *backup* dos dados, sugerindo o tempo de retenção das cópias.

Todos os *backups* devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, em períodos de pouco ou nenhum acesso de usuários.

As mídias de *backup*, se existentes, devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo) e, preferencialmente, distantes o máximo possível do datacenter, se houver.

Toda infraestrutura de suporte aos processos de *backup* e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento.

O Comitê de Gestão da Informação deve preparar um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as chefias/gestores das áreas.

Na situação de erro de *backup* e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse *backup*, eles deverão ser executados apenas mediante justificativa de necessidade.

14. DATACENTER

As máquinas (servidores) que armazenam sistemas do Escritório devem ser instaladas em áreas protegidas e seguras, bem como todos os sistemas ou equipamentos classificados como críticos.

A entrada ao Datacenter somente se dará a pessoas autorizadas e/ou com acesso devidamente controlado e monitorado.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a mesma deve ser autorizada pelo por pelo menos três membros do Comitê Gestor da Informação.

Nesta PSI fica definido que somente os analistas de TI, mediante ciência dos membros do Comitê Gestor da Informação, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no *Datacenter* é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados; assim, somente colaboradores credenciados e autorizados pelo Comitê Gestor da Informação podem ter acesso aos dados armazenados.

Os logs dos ativos de rede devem ser monitorados constantemente afim de evitar acessos indevidos.

15. INFRINGÊNCIAS À PRESENTE POLÍTICA

No caso de descumprimento das normas estabelecidas nesta PSI, o colaborador poderá sofrer as seguintes penalidades:

(i) advertência formal: o colaborador será advertido da infração cometida e ao mesmo será recomendada a leitura da presente Política e de diretrizes correlatas, inclusive legais, aplicáveis ao caso;

(ii) advertência formal com notificação da chefia/gestor imediato: em caso de reincidência ou de infração de natureza grave, o colaborador será advertido da infração através de comunicado que será enviado, em cópia, para a chefia/gestor responsável, a fim de que sejam adotadas medidas cabíveis no caso, como, por exemplo, desligamento, rescisão, demissão, comunicação a autoridades públicas, etc.

(iii) no caso de clientes e parceiros: envio de comunicação para adequação às regras contidas nesta e nas diretrizes correlatas; havendo resistência à adequação/readequação, caberá à chefia/gestor da área, ouvidos os membros do Comitê de Gestão da Informação e da alta administração, tomar providências que podem importar, inclusive, a rescisão, por justa causa, dos contratos com eles mantidos.

16. DISPOSIÇÕES FINAIS

Esta é uma Política pública que pode ser alterada a qualquer momento, sendo de responsabilidade do Escritório dela dar ciência plena e inequívoca a todos os seus colaboradores, inclusive em caso de alterações.

Em caso de controvérsias, fica eleito para dirimi-las, com prejuízo de qualquer outro, por mais privilegiado que seja, o Foro Central da Comarca de São Paulo.

Esta Política entra em vigor da data de sua publicação.