2023

Política da Segurança da **Informação**

Avenida Tamboré 350, Barueri, São Paulo, 06460-000
+55 (11) 4688-4001 | info@abaigroup.com.br

1. POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

CONTROLE DE REVISÃO

Revisão	Data	Histórico de Alterações	Resp. pela Elaboração	Resp. pela Aprovação
00	07/11/2023	Edição para divulgação PÚBLICA no site ABAI de acordo com layout definido por Marketing Espanha	INFOSEC	CISO

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Abai para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Sua aplicação é obrigatória em todas as áreas da empresa.

A PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

A Política de segurança da informação, na Abai, aplica-se a todos os colaboradores e prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da empresa, ou acesso a informações pertencentes a Abai.

Todo e qualquer usuário de recursos computadorizados da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de tecnologia da informação.

Fica definido como violação desta política qualquer ato que:

- Exponha a companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança de dados ou informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

2. OBJETIVOS

Estabelecer diretrizes que deverão ser seguidas pelos colaboradores, clientes residentes e prestadores de serviços da Abai, contemplando padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Abai quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

  É dever de todos dentro da Abai:

- Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a Abai e deve sempre ser tratada profissionalmente.

3. APLICAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, clientes residentes e prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.
Esta política dá ciência de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.
É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou com a área de Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores e prestadores de serviços como resultado da atividade profissional contratada pela Abai pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.
Os equipamentos de tecnologia da informação, comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.
A Abai, por meio das áreas de Segurança da Informação e Tecnologia da Informação, poderá monitorar e manter registros de todo uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5. RESPONSABILIDADES

As responsabilidades dos Colaboradores , clientes residentes e Prestadores de Serviços são:

- Respeitar a Política de Segurança da Informação da Abai sob pena de incorrer nas penalidades cabíveis;
- Preservar a integridade e confidencialidade dos Ativos de Informação da organização ou sob sua custódia;
- Não compartilhar, sob quaisquer meios, informações confidenciais com quem não possua a devida autorização de acesso, toda informação gerada na Abai é de propriedade da organização, não podendo ser externada para outros ambientes através de qualquer mídia sem prévia e formal autorização;
- Comunicar qualquer ocorrência ou indício de incidente de segurança da informação.

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da empresa, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos.

A área de TI e SI poderá realizar auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Qual informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

6. DIRETRIZES

Uso de Dispositivos Móveis

Os usuários que tiverem direito ao uso de dispositivos móveis corporativos (laptop, notebook, celular etc.), ou qualquer outro equipamento computacional, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

Abaixo estão as regras básicas para manter os dispositivos móveis protegidos.
Tais regras são válidas para todos os dispositivos eletrônicos móveis (por exemplo: laptops, notebooks, IPADs, Tablets, Celulares, Pen Drives, HDs Externos etc.).

- Usuários de notebook quando estiverem em outras localidades fora da Abai ou em trabalho remoto, após encerrar o expediente convém que os mesmos sejam guardados em local protegido.
- Não deixe dispositivos eletrônicos móveis sem supervisão em salas de reuniões ou áreas públicas.
- Não deixe dispositivos eletrônicos móveis sem supervisão em áreas públicas ou em qualquer lugar fora do escritório.
- Fique atento em aeroportos, hotéis e ao usar transporte público uma vez que esses ambientes proporcionam amplas oportunidades de roubo de dispositivos eletrônicos móveis.
- Mantenha dispositivos eletrônicos móveis fora de vista para evitar roubo se for permanecer em seu veículo sem supervisão. Recomendamos a guarda do dispositivo móvel no porta-malas do seu veículo até a chegada ao seu destino.
- É obrigatório armazenar todas as informações de negócios em servidores ao invés de armazenar localmente no seu dispositivo móvel. Se essas informações forem

armazenadas localmente em seu dispositivo móvel, recursos de segurança deverão ser usados para proteger as informações contra perda ou roubo.

- Use somente dispositivos de armazenamento móveis pertencentes e aprovados pela TI da Abai (por exemplo, pen drives, unidades USB, unidades flash). Os dispositivos de armazenamento móveis não aprovados, podem não conter recursos de segurança suficientes para proteger as informações armazenadas neles em caso de perda ou roubo.
- Certifique-se de que pessoas desconhecidas ao redor não possam ver as informações exibidas na tela do seu computador ("sobre os ombros"). Um filtro de privacidade para tela é recomendado, especialmente para viajantes frequentes. O filtro de privacidade para tela pode ser acoplado à parte da frente da tela do computador para ajudar a impedir que outras pessoas vejam o conteúdo da tela.
- Não faça alterações não autorizadas na configuração de segurança dos dispositivos eletrônicos da Abai .
- Os dispositivos que não forem gerenciados pela Abai (por exemplo, unidades USB, iPods, MP3 players, celulares) não devem ser conectados a um computador da empresa mesmo para fins de recarga de bateria.
- A Abai não permite a utilização de notebooks particulares, mesmo que temporariamente.
- A Abai disponibiliza celular corporativo e/ou chip corporativo para colaboradores conforme autorização da Diretoria. Para tanto as seguintes diretrizes de segurança deverão ser seguidas:

➢ Os celulares devem conter senha de acesso.
➢ O acesso ao e-mail se dá através de utilização de partição segura.
➢ O uso do celular particular é permitido somente com autorização da diretoria e SI, no entanto devem seguir todas as regras e diretrizes de segurança aqui estabelecidas.(Vide Termo de Consentimento para Comunicações via WhatsApp.docx)

Em caso de furto ou perda o usuário deverá proceder conforme segue:

Registre a ocorrência em uma delegacia de polícia;
Comunique imediatamente ao seu superior e as áreas de TI e SI, preferencialmente no mesmo dia da ocorrência;
Envie uma cópia da ocorrência para as áreas de TI e SI.

O não cumprimento destas orientações no caso de roubo ou furto estão sujeitas às penalidades, conforme determinado no item 7.18 desta política.

Classificação da Informação

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (documentos, relatórios e/ou mídias) gerada por sua área de acordo com as regras a seguir.

- **Regras para classificação das informações**

Toda informação produzida na organização deverá ser classificada considerando os seguintes aspectos:

- **Confidencialidade**: a informação deve ser protegida contra acesso não autorizado.
- **Integridade**: a informação deve ser protegida contra alterações não autorizadas, intencionais ou não.
- **Disponibilidade**: a informação deve estar disponível, sempre que necessária, de acordo com o perfil de acesso do funcionário.

As informações deverão ser classificadas como públicas, internas, restritas e confidenciais.

- **Públicas**: informações de domínio público, sem necessidade de restrições ou controle a seus acessos. Incluem-se, por exemplo, informações de caráter informativo ou promocional, ou informações de divulgação obrigatória em função de legislação vigente, como balanços e prestação de contas aos acionistas.
- **Internas:** informação de uso dos colaboradores ou prestadores de serviços autorizados, que não possuem segredo de negócio ou que não comprometam a imagem da organização. Incluem-se, por exemplo, informações impressas ou digitais que contenham o logo da organização, políticas, normas, procedimentos, circulares ou qualquer outro tipo de informação de uso em serviço.
- **Restritas**: informações de uso destinadas a um grupo de colaboradores ou área específica de trabalho. Incluem-se, por exemplo, informações sobre política ou estratégia de uma determinada área/ equipe, detalhes técnicos sobre determinados produtos, serviços ou tecnologia, dados de clientes, como número de cartões ou faturas.
- **Confidenciais**: informações estratégicas e sigilosas, que podem causar um impacto sensível na organização (financeiro, de imagem ou operacional) se acessadas por pessoas não autorizadas. São informações restritas a um número de pessoas que, pela natureza do cargo ou função que exercem, são obrigadas a conhecê-las. Incluem-se, por exemplo, informações estratégicas e principais direcionamentos da organização no mercado, informações salariais, prêmios, bonificações, novos produtos em desenvolvimento ou novas tecnologias.

No momento em que uma informação for gerada, adquirida ou herdada, deverá ser designado um responsável que irá classificá-la quanto a sua necessidade de sigilo, considerando as exigências do negócio.

A classificação da informação deve ser bem criteriosa e, no caso de um conjunto de informações de diferentes níveis de classificação, por princípio, deve-se adotar a classificação de maior nível de segurança possível.

Caso uma informação não possua uma classificação explícita quanto ao sigilo, esta deverá ser considerada uma informação interna.

Caso haja necessidade, a informação poderá ser reclassificada, de acordo com os critérios definidos pelo responsável.

O descarte de uma informação, após o fim de sua vida útil, deverá seguir os critérios de classificação, de forma que não haja acesso não autorizado, mesmo em sua obsolescência.

- **Rotulagem**
  Toda informação classificada deverá ser rotulada quanto ao seu grau de sigilo (interna, restrita ou confidencial), exceto as informações públicas, que não necessitam de rotulagem.

- **Proteção de Dados Pessoais**
  A Abai tem o compromisso de realizar o tratamento de dados pessoais de acordo com as disposições legais vigentes na Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

DADOS DOS COLABORADORES

A Abai se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores, além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de colaboradores que porventura sejam armazenados serão considerados dados confidenciais. Dados pessoais de colaboradores sob a responsabilidade da Abai não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados pessoais de colaboradores não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso, a lista de endereços eletrônicos (e-mails) usados pelos colaboradores da Abai. Por outro lado, os colaboradores se comprometem a não armazenar dados pessoais nas instalações da Empresa, sem prévia e expressa autorização por parte da diretoria.

Mesmo que seja autorizado o armazenamento destes dados, a Abai não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos servidores da empresa, e jamais poderão fazer parte da rotina de backup da empresa.

ADMISSÃO E DEMISSÃO DE COLABORADORES / TEMPORÁRIOS / ESTAGIÁRIOS

A área de Departamento Pessoal da empresa deverá informar por e-mail ao Setor de TI, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de colaboradores, para que os mesmos possam ser cadastrados ou excluídos no sistema da Empresa. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo Setor de TI.

Cabe ao setor solicitante da contratação a comunicação ao Setor de TI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à Empresa, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso

ao sistema. No caso de demissão, o setor de Departamento Pessoal deverá comunicar o fato o mais rapidamente possível ao Setor de TI, para que o funcionário demitido tenha seus acessos bloqueados.

Cabe a área de Departamento Pessoal dar conhecimento e obter as devidas assinaturas de concordância de todos os contratados em relação à Política de Segurança da Informação da Abai e demais documentos aplicáveis. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

DADOS DE CLIENTES, FORNECEDORES E PARCEIROS DE NEGÓCIO

Os dados pessoais de clientes, fornecedores e parceiros de negócios serão tratados de forma a dar efetiva proteção aos mesmos, utilizando-os tão somente para os fins necessários à consecução de atividades previstas em contrato, ou nos limites do consentimento expressamente manifestado por escrito por seus respectivos titulares.

O compromisso da Abai com a proteção de dados pessoais está formalizado na Política de Privacidade, disponível no site e nas cláusulas contratuais com clientes e fornecedores.

Uso da Internet

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na Abai. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pela área de TI, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que utilizou a Internet e quais páginas foram acessadas.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da Abai sem expressa anuência da área de TI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

A transmissão de informações confidenciais, proprietárias ou de segredo comercial são estritamente proibidos, a menos que o uso, o armazenamento ou a transmissão de tais materiais sejam necessários para cumprir os objetivos de negócios da Abai devidamente previstos em contratos e com as devidas aprovações.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- Que defendam atividades ilegais;
- Sites com conteúdo pornográficos;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da empresa;
- Que promovam discussão pública sobre os negócios da Abai, a menos que autorizado pela Diretoria;

- Que possibilitem a distribuição de informações de nível “Confidencial”;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Mesa Limpa e Tela Limpa e Uso de Impressor

Mesa Limpa e Tela Limpa são práticas de segurança da informação recomendadas para o local de trabalho (in company ou remoto), a fim de se evitar a exposição desnecessária de informações consideradas sensíveis, com o objetivo de se evitar o comprometimento da informação reduzindo riscos de acesso não autorizado, perda ou danos às informações durante e fora do horário do expediente.

Abaixo estão as regras básicas das práticas de Mesa Limpa e Tela Limpa.

- Todas as áreas devem possuir local para armazenamento de documentos e mídias, como gaveteiros e armários com chaves, para a utilização pelos colaboradores;
- Deve-se manter a área de trabalho limpa e organizada, evitando o excesso de papéis, pastas, mídias de computador e objetos de uso pessoal;
- Deve-se manter sobre a mesa de trabalho apenas o material necessário ao desempenho de suas atividades;
- Informações sensíveis ou críticas do negócio, quando não requeridas, devem ser guardadas de forma segura e fechada nos locais de armazenamento disponibilizados para as áreas, especialmente quando o escritório estiver vazio;
- O uso de impressoras e de outra tecnologia de reprodução (por exemplo, scanners, máquinas fotográficas digitais), deve ter seu acesso restrito e controlado;
- Retirar papéis, anotações e lembretes das mesas de trabalho, quando não estiver no local e ao final do expediente;
- O descarte das mídias contendo informações de clientes ou sigilosas deve ser realizado de acordo com o estabelecido no item 7.15 desta política.
- Todos os documentos obtidos de outros departamentos devem ser devolvidos prontamente quando não forem mais necessários;
- A quantidade de papel utilizado deve ser reduzida e as impressões só deverão ser feitas quando forem realmente necessárias. Evite imprimir documentos apenas para lê-los, ou seja, leia-os na tela, se possível;
- Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora;
- Os monitores devem ter suas áreas de trabalho organizadas, com o mínimo de informações disponíveis, evitando que informações importantes sejam acessadas por pessoas não autorizadas;
- As estações de trabalho (computadores desktops, notebooks) devem ser bloqueadas sempre que o colaborador se ausentar da mesa (Ctrl+Alt+Del Enter ou tecla Windows+L), a fim de impedir que outros usuários possam acessar indevidamente seus acessos corporativos.
- Se uma sessão estiver ociosa por mais de 05 minutos, é necessário que o usuário redigite a senha para reativar a estação de trabalho.

Trabalho Remoto

É considerado trabalho remoto toda forma de trabalho fora do local físico da organização, incluindo ambientes de trabalho não tradicionais, local de trabalho flexível, trabalho virtual ou trabalho home office.

De forma a evitar o vazamento e a perda de informações críticas, por conduta inadequada de trabalho fora da organização, todos os colaboradores deverão seguir as seguintes diretrizes:

- Todo e qualquer trabalho remoto deve ter autorização formal concedida pelo gestor responsável da área.
- O colaborador que faz a utilização externa de equipamentos disponibilizados pela organização deve seguir as diretrizes de uso de dispositivos móveis contidas nesta política e seguir as orientações de contrato de comodato de equipamento, quando aplicável.
- Em caso de acesso remoto ao ambiente da Abai, o gestor responsável deve fazer a solicitação através do sistema de abertura de chamados para a liberação do acesso. Após isso, a área de TI fará uma análise para aprovação do acesso.
- O acesso remoto ao ambiente da Abai tem seus logs constantemente gravados para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada.
- O colaborador que estiver realizando trabalho remoto, deve-se atentar ao ambiente físico a ser utilizado, com o objetivo de evitar o vazamento de informações por meio de mídias, conversas ou telefonemas.
- Ao realizar qualquer tipo de acesso ao ambiente de armazenamento da Abai (rede, nuvem ou sistemas SAAS), o profissional deve evitar que pessoas não autorizadas tenham acesso visual aos sistemas e informações da organização, vejam ou ouçam dados e / ou informações relevantes.
- O colaborador que estiver realizando trabalho remoto deve se atentar a possíveis acontecimentos que possam causar danos físicos às informações e equipamentos de trabalho (ex. molhar, derrubar, queimar).

Uso de Serviços de Comunicação Corporativa (Email e Teams)

O e-mail e teams fornecidos pela Abai é um instrumento de comunicação interna e externa para a realização do negócio da empresa. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da Abai, não podem ser contrárias à legislação vigente e nem aos princípios éticos da Abai.

O uso do e-mail e teams é exclusivo para fins profissionais e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;

- Possam prejudicar a imagem de outras empresas;
- Sejam prejudiciais à capacidade técnica da rede;
- Sejam incoerentes com as políticas da Abai.

Ambos devem ser utilizados de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.

Por se tratar de um recurso da empresa, não deve haver expectativa de privacidade nas mensagens enviadas e recebidas por e-mail ou teams. A empresa poderá realizar auditoria e monitoramento, caso haja alguma suspeita de fraude ou mal uso de ambos.

Nossos servidores de e-mail e teams encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isto algumas regras devem ser obedecidas:

- ➢ É proibido o envio de grande quantidade de mensagens de e-mail (spam). Evitem arquivos anexos muito grandes, maiores que 5 MB. Inclui-se qualquer tipo de mala direta ou e-mail em lote, como por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.
- ➢ É proibido o envio de e-mail ou mensagens mal-intencionadas, tais como email bomb ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou função.
- ➢ Evitar o uso de Linguagem Coloquial em respostas aos e-mails comerciais, como abreviações de palavras e uso de gírias.
- ➢ É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.
- ➢ Não execute ou abra arquivos anexados enviados por remetentes desconhecidos ou suspeitos.
- ➢ Desconfie de qualquer e-mail com assuntos estranhos ou desconhecidos e de instituições bancárias ou órgãos públicos que solicitem atualização cadastral ou troca de senha e no caso de recebimento consultem o Suporte TI antes de abrir ou clicar em algum item do e-mail.
- ➢ Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta de que solicitou este e-mail.
- ➢ É obrigatória a utilização de assinatura nos e-mails, seguindo padrão estabelecido pela Abai.

Para incluir um novo usuário no e-mail, a respectiva gerência deverá abrir um chamado através da ferramenta (xxx) que a área de TI providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

Caso necessite efetuar comunicações através de sistemas de mensagens instantâneas como o WhatsApp e Telegram, não sendo possível usar os meios oficiais da empresa, o Termo de

Aceitação de Riscos (Consentimento para Comunicações via WhatsApp). Este documento deverá ser preenchido pelo colaborador , e assinado pelo diretor da área a qual atua.

Instalação de Software

A Abai respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da empresa.
É terminantemente proibido o uso de programas ilegais (sem licenciamento) na Abai.
Os usuários não podem, em hipótese alguma, instalar qualquer tipo de "software" (programa) nos equipamentos da Empresa, somente a equipe da área de TI tem autorização para instalação de programas previamente autorizados de acordo com o documento Procedimento de Gestão de Softwares. Periodicamente, a equipe de TI realiza verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes serão removidos dos computadores.
Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados se responsabilizam perante a Empresa por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos às sanções previstas neste documento.

Uso de Antivírus

Todo arquivo em mídia proveniente de entidade externa a Abai deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho (desktop ou notebook) devem ter um antivírus instalado. A atualização do antivírus será automática e controlada pela área de TI.
A configuração padrão do software de prevenção contra vírus não deve ser alterada ou desativada — isso pode tornar o software ineficaz.
Não devem ser abertos e-mails que pareçam suspeitos, mesmo se forem supostamente de um remetente conhecido. O malware normalmente personifica ("falsifica") o remetente, dando a aparência de que o e-mail foi enviado por um contato legítimo. E-mails suspeitos devem ser excluídos.
Não devem ser abertos anexos ou hyperlinks que venham em e-mails suspeitos. Eles podem conter vírus.
Em caso de suspeita de que o computador esteja infectado, o usuário deve desligá-lo e a área de TI deve ser imediatamente contatada para uma análise. Não se deve tentar remover o malware sozinho.

Acesso Lógico

A regulamentação do controle de acesso lógico constitui-se fator de grande importância para a Política de Segurança da Informação, visando à manutenção da integridade e confidencialidade dos ativos de informação em uso ou de propriedade da Abai.
O controle de acesso lógico tem como objetivo proteger equipamentos, sistemas, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.
Os eventos que envolvem o controle de acesso incluem, sem se limitar, às seguintes situações:

- Contratação de um novo funcionário, estagiário, terceirizado ou prestador de serviço da Abai;
- Necessidade de acesso ao sistema ou recurso específico no desempenho de função;
- Afastamento temporário por férias ou licença médico;
- Alteração da função desempenhada;
- Transferência para outra área;
- Desligamento do funcionário, estagiário, terceirizado ou prestador de serviço por rescisão do contrato.

O acesso aos recursos de sistemas e rede deve ser concedido único e exclusivamente para as finalidades e funções que exijam este acesso, devendo ser observados os processos formais de solicitação, alteração e exclusão de acessos, bem como as restrições
O parâmetro de configuração de senhas de acesso adotado pela Abai segue as seguintes diretrizes:

- A senha deve ser formada por, no mínimo, 8 (oito) caracteres alfanuméricos, não sendo permitidos caracteres sequenciais;
- A senha deve ser alterada obrigatoriamente a cada 30 dias, a contar da data da criação ou última alteração;
- O login de acesso deve ser bloqueado automaticamente, por 05 minutos, após 03 tentativas sucessivas de acesso sem sucesso;
- Obrigar a troca de senha no primeiro acesso do usuário, após seu cadastramento ou alteração da senha pelo administrador.

As chaves de acesso e suas respectivas senhas são de propriedade do usuário, não devendo este, em hipótese alguma, fornecer, compartilhar, divulgar a qualquer pessoa de qualquer forma que seja.
Cada usuário deve zelar pela guarda de suas chaves de acesso e senhas de forma segura, não a deixando de forma visível ou de fácil conhecimento.
A concessão das chaves de acesso e senhas deve ser feita de maneira formal, considerando que o usuário está ciente de suas responsabilidades para a manutenção efetiva dos controles de acesso a partir da assinatura do Acordo de Confidencialidade incluído nos termos e condições do seu Contrato de Trabalho ou de Prestação de Serviço.

Acesso e Uso da Rede

Na utilização da rede todos os usuários devem respeitar as seguintes diretrizes:

- Não alterar as configurações da rede;
- Não instalar softwares, exceto quando autorizado;
- Nunca remover ou desativar softwares antivírus;
- Nunca expor, armazenar ou distribuir materiais de natureza pornográfica (músicas e vídeos) e/ou racista por meio de recursos da empresa;
- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como “cracking”). Isso inclui acesso aos dados não disponíveis

para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas;
- Será feito sempre que necessária limpeza nos arquivos armazenados na pasta temporário para que não haja acúmulo desnecessário de arquivos.

Backup e Restore

Todos os dados da Abai deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança de sistemas e servidores de rede são de responsabilidade da área de TI e deverão ser feitas de acordo com os padrões estabelecidos pela empresa.

Não é política da Abai o armazenamento de dados em desktops individuais, entretanto, na necessidade de armazenamento em fora destes padrões, a área TI deverá ser avisada para que o usuário faça o backup dos dados de sua máquina periodicamente mantendo cópia de backup no servidor.
É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos colaboradores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da Empresa.
No caso das informações consideradas de fundamental importância para a continuidade dos negócios da Abai a área de TI disponibilizará área de armazenamento na rede onde cada usuário deverá manter estas informações. Estas informações que serão mantidas na rede serão incluídas na rotina diária de backup da área de TI.

Necessidade Novos Aplicativos e Equipamentos

A área de TI é responsável pela aplicação da Política da Abai em relação à definição de compra e substituição de “softwares” e “hardwares”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardwares) deverá ser solicitada formalmente para a área

de TI que irá realizar análise de viabilidade da solicitação. Esta solicitação sendo aprovada a equipe de TI irá executar a aquisição. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

Segurança Física e dos Ambientes

O controle de acesso físico às dependências internas da Abai são garantidas, por meio do crachá de acesso e identificação que é fornecido para todos os colaboradores, clientes , visitantes e

prestadores de serviço envolvidos em nossas atividades. Estes serão registrados para o monitoramento periódico de conformidade das regras.
Para o uso correto do crachá deverão ser adotadas as seguintes regras:

- O crachá é único, pessoal e intransferível, logo todo acesso será atribuído ao seu usuário;
- Utilizar o crachá de maneira visível enquanto estiver dentro das dependências físicas da Abai;
- Não é permitido emprestar o crachá de acesso;
- Não permitir a entrada ou entrar em áreas controladas de "carona", tais como, ambiente operacional, ambiente de desenvolvimento de sistemas, data center e entre outras.

Todas as instalações da Abai são equipadas com sistema monitoramento CFTV e o acesso as imagens são devidamente controladas e restritas, protegido por normas e leis vigentes

No caso de infração das regras supra citadas, temos:
- colaborador : DP emite em 2 vias Aviso de Advertência ,descrevendo o motivo , e coleta assinatura do colaborador e do Gestor da área.
Uma cópia deve ser armazenada no dossiê do colaborador e a outra deverá ser entregue ao mesmo.

- cliente residente , terceiros/prestadores de serviços ou visitantes : Infosec preenche Aviso de Advertência , coleta assinatura da Hierarquia , comunica Gestor da área a qual prestador /cliente residente atua.
Este documento deverá ser armazenado na pasta /diretório de Infosec

Descarte de Documentos Físicos, Equipamentos ou Mídia

O descarte de documentos físicos, equipamentos e mídias deve ser realizado garantindo o zelo pela segurança das informações contidas nos mesmos.
Informações confidenciais e sensíveis podem estar armazenadas em arquivos digitais, sistemas da informação, diretórios da rede, banco de dados, códigos de sistemas, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, documentos físicos originais ou cópias, entre outros.
A destruição segura tem como finalidade garantir o atendimento às exigências legais e de mercado quanto à confidencialidade das informações presentes nos documentos (dados de clientes, contratos, informações internas, etc.), além de preservar a marca evitando a exposição indevida (situação comum em situações de extravio no sistema de coleta de lixo tradicional).
A destruição segura possibilita a destruição total, impossibilitando a recuperação da informação após o processo.
Documentos confidenciais impressos, relatórios e todos os demais documentos em papel devem ser triturados antes do descarte.
Abaixo alguns exemplos de itens que devem ter o descarte seguro:

- Documentos confidenciais impressos (com dados de colaboradores, clientes, etc);
- Gravação de voz ou de outros tipos;
- Relatórios impressos;

- Equipamentos (estações de trabalho ou notebooks);
- Fitas magnéticas;
- Discos removíveis e cartuchos;
- Meio de armazenamento ótico (todas as formas)
- Documentação de sistemas.

Equipamentos, fitas magnéticas, HDs e outras mídias devem ser encaminhados para a área de TI que realizará o descarte seguro obedecendo às normas e leis vigentes.
Este determinará se uma empresa especializada irá efetuar a desmagnetização e trituração dos ativos, garantindo que as informações se tornem absolutamente inacessíveis. Estes métodos devem ser ecologicamente corretos de acordo com Laudos emitidos pela CETESB relativos à proteção ambiental.

Notificação de Incidentes de Segurança da Informação ou Violação de Privacidade de Dados

É responsabilidade de todos os colaboradores, que na identificação de um incidente, uma violação de privacidade dados ou mesmo suspeitas de fragilidades de segurança da informação ou privacidade, notificar imediatamente a área de SI por meio da abertura de chamado registrado no sistema GLPI ou contato formal com o Gerente de SI ou por celular através do número (11) 949754164 em casos confidenciais dar preferência pelo acionamento por celular ou pessoalmente.

Segue abaixo alguns tipos de incidentes ou fragilidades de segurança que devem ser notificados:

- Vazamento de informações;
- Uso indevido de ativos da empresa;
- Uso de celular em ambientes não autorizados;
- Uso indevido de dados pessoais ou sensíveis;
- Uso de e-mail corporativo para spam ou promoção de negócios pessoais;
- Ferramenta não autorizada instalada;
- Uso de pendrive de forma não autorizada;
- Impressão de documentos de forma não autorizada;
- Tentativas não autorizadas de acesso;
- Má utilização de um sistema;
- Falhas no sistema que impede um acesso autorizado;
- Ataques de negação de serviço;
- Vírus e outros códigos maliciosos;
- Sequestro de dados (ransomware);
- Desfiguração de sites;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do proprietário;
- Desrespeito à política de segurança ou à política de uso aceitável dos sistemas de informação empresa;
- Perda ou furto de ativos da empresa (exemplo: celular, notebook, HD, etc);
- Perda ou destruição indevida de documentos em meio físico;

- Acesso por meio de carona aos ambientes seguros;
- Acesso físico indevido aos ambientes seguros;
- Circulação sem uso crachá de identificação pessoal nas instalações da empresa;
- Uso indevido do crachá de identificação pessoal;
- Deleção/apagamento de arquivo ou informações de forma indevida.

Monitoramento de Atividades

Esta política dá ciência a todos os colaboradores de que os ambientes, sistemas, computadores e redes da empresa estão sendo monitorados e gravados, conforme previsto nas leis brasileiras.
O uso de ferramentas de monitoramento tem como intuito:

- Garantir o uso adequado dos ativos da empresa;
- Monitorar ações que tenham sido motivo de preocupação por parte da direção da empresa;
- Detectar fraudes de usuários ou detectar aqueles que representam uma ameaça, para reagir rapidamente prevenindo ataques internos e protegendo os dados da empresa e dos clientes;
- Levantamento de logs para eventual auditoria;
- Investigação de incidentes de segurança da informação ou violação da privacidade de dados.

O monitoramento físico e lógico é realizado por meio de ferramentas específicas acessadas pela área de TI e SI.

Conscientização e Treinamento

Como forma de garantir que os colaboradores, terceiros e prestadores de serviço tenham recebido informações necessárias para cumprir de maneira correta com as diretrizes da Política de Segurança da Informação são realizados treinamentos e reciclagens anuais.
Além disto, todos os colaboradores que atuam na Abai assinam o termo de sigilo e confidencialidade na efetivação dos seus contratos, bem como participam do processo de Integração que aborda o tema Segurança da Informação.
Como forma de se manter um processo contínuo de conscientização dos colaboradores, são utilizados diversos meios para a divulgação das regras de segurança da informação da Abai, além da divulgação na intranet.
Os treinamentos de reciclagem, poderão ser realizados em intervalos menores com o objetivo de disseminar novas diretrizes e práticas de segurança da informação ligadas ao negócio da Abai, tais como requisitos contratuais de clientes.
As ações de planejamento de conscientização e treinamento dos nossos colaboradores (funcionários, prestadores de serviços e terceiros) nas diretrizes de Segurança da Informação é coordenado pela área Treinamento e mantidos registros e evidências.

Violações da Política e Penalidade

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar em medidas disciplinares cabíveis, tais como, advertência, suspensão ou desligamento, a qualquer colaborador que violar esta política.

7. REFERÊNCIAS

- NBR ISO/IEC 27001, na versão vigente.
- NIST