1) Objetivos

A Política tem como objetivo estabelecer princípios e diretrizes pertinentes à Segurança Cibernética e instituí-las junto aos processos que possuem acesso as informações sensíveis de clientes e parceiros, conforme determinado pela Diretoria e instituições vigentes dos Órgãos reguladores Banco Central e Comissão de Valores Mobiliários.

A SENSO entende que a segurança cibernética se refere ao conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação e transmitida por meio das redes de comunicação, incluindo a internet e telefones celulares.

As demais diretrizes gerais relacionadas ao controle de acesso, segregação de funções, classificação dos tipos de informações utilizadas pela SENSO, propriedade intelectual, segurança física, uso de recursos de TI e demais diretrizes estão publicadas na Política de Segurança da Informação.

2) Procedimentos e controles

2.1 - Autenticação: as regras relacionadas à configurações de senhas são determinadas pela área de Tecnologia da Informação, que adota os requisitos mínimos em conformidade com a norma vigente. Os colaboradores, prestadores de serviços e/ou terceiros contratados são responsáveis pela confidencialidade de suas respectivas senhas, lembrando que as mesmas são individuais e intransferíveis.

2.2 - Criptografia: a SENSO utiliza mecanismos de segurança e privacidade que tornam uma determinadas comunicações ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem. As chaves criptográficas adotadas internamente, propõem a proteção de todos os conteúdos transmitidos, evitando a intercepção por parte de cibercriminosos, hackers e espiões, bem como garantem a confidencialidade das mesmas contra ataques ativos e passivos e, também, a autenticação de origem e destino, características obrigatórias de um protocolo confiável para distribuição de chave.

2.3 - Prevenção e detecção de intrusão: o monitoramento do tráfego de rede, identificação de atividades maliciosas e a geração de informações de log sobre estas atividades, o sistema Sophos faz todo este gerenciamento visando a segurança ativa na Instituição. As regras relacionadas ao Firewall, estão descritas e publicadas internamente na Política de Segurança da Informação – TI.

2.4 - Mecanismos de rastreabilidade: Tendo como processo extremamente importante para o bom funcionamento das operações e negócios, os sistemas utilizados pela Instituição possuem dados e fatos organizados, ou seja, possuem o registro das ações realizadas, bem como dispõem a capacidade de identificar de onde vem cada um dos registros, alertas e problemas de uma determinada área. Dentre os sistemas críticos da Instituição relacionados às operações que possuem o mecanismo de rastreabilidade e que garantem a segurança das informações sensíveis, está o sistema homologado pela B3 "Sistema Integrado de Administração de Corretoras (SINACOR) ", que controla toda a movimentação do cliente na corretora, as operações de bolsa, conta corrente e custódia de ativos

2.5 - Manutenção de cópias de segurança dos dados e das informações: A Instituição possui regras definidas para a realização da manutenção de cópias de segurança dos dados e das informações. São realizados backup diários que ficam armazenados em outro local físico. A cópia diária (backup) compõe todos os arquivos de dados do servidor (base de dados, planilhas, textos, entre outros) e as últimas atualizações efetuadas (inclusões, alterações e exclusões de registros). A regras sobre o tema estão descritas e na Política de Segurança da Informação.

2.6 - Controle de acesso e segmentação da rede de computadores: Visando assegurar a integridade do processo de Controle de Acesso - Segregação de Funções, o processo consiste na separação de atribuições ou responsabilidades especialmente aquelas descritas como críticas pela norma vigente.As regras e diretrizes estão descritas na Política de Segurança da Informação.

2.7 - Formalização e controles - Gestão de incidentes: Para a SENSO um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade e os demais incidentes (não relacionados à segurança) são eventos que impactam as operações e geram uma interrupção ou diminuição na qualidade do serviço. Todos os incidentes são registrados e administrados pelo departamento de Tecnologia da informação.

2.8 - Comunicação de Dados e Voz: todos os ramais da SENSO são gravados por ferramenta própria administrado pelo TI chamado "Elastix" e as mesmas são armazenadas pelo período mínimo de 5 (cinco) anos.

2.9 - Proteção e revisão de registros de eventos (Logs): Os sistemas utilitários como gerenciador de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em Produção, geram o Registro de Operações, é fundamental que os logs gerados sejam protegidos de alteração e deleção. Deve ser realizada a revisão periódica dos mesmos, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados. Para manuseio, troca e armazenamento de dados não deve ser permitido ao colaborador a extração direta de informações, sem que seja formalizado um pedido, e aprovado pela Diretoria. As exceções devem ser deliberadas pela Diretoria.

2.10 - Utilização de equipamentos periféricos: Todos os equipamentos periféricos (que recebem ou enviam informações para o computador, podendo ser, impressoras, mouses, teclados, entre outros) devem ser homologados pela Área de Tecnologia da Informação, sendo necessária a priorização do uso seguro de impressoras e material impresso. No uso cotidiano todos os colaboradores devem adotar a opção de timeout nas estações de trabalho, ou seja, ativar a Proteção de Tela do Windows protegida por senha, de modo que em ausência maior que 10 minutos, seja ativada esta proteção.

2.11 - Descarte de mídias: As mídias de armazenamento permanente ou temporário de informações devem ter tratamento seguro para as situações de descarte, visando proteger a Instituição de exposição não autorizada de informações. As diretrizes estão descritas na Política de Segurança da Informação.

2.12 - Rede Wireless: A Instituição possui rede sem fio configurada para comodidade e flexibilidade em acessos de natureza específica ou extraordinária. O acesso a rede sem fio somente deve ser permitido mediante aprovação da Diretoria. A rede sem fio da Instituição não permite acesso aos recursos de rede local, sua utilização visa exclusivamente o acesso à internet, de forma irrestrita. O controle de acesso deve ser efetuado garantindo de forma confiável a restrição de acessos indevidos e/ou maliciosos. O detalhamento deste processo está descrito na Política de Segurança da Informação.

3) Registro de incidentes

A área de Tecnologia da Informação deve anualmente produzir o Relatório sobre a implementação do plano de ação e de respostas a incidentes, com data base de 31 de dezembro de cada ano que deverá ser apresentado à Diretoria até 31 de março do ano seguinte a data base, o mesmo deverá ficar a disposição do legislador para posterior consulta.

4) Responsabilidades

- Diretoria de Tecnologia da Informação**:** assegurar que esta Política de Segurança Cibernética esteja em conformidade com a regulamentação vigente, aprovar a Política de Segurança Cibernética, emitir parecer acerca das ações a serem implementadas para correção das deficiências apontadas, orientar as áreas e gestores a respeito das regras a serem cumpridas, responder aos requerimentos dos Órgãos Reguladores, manter esta Política atualizada, juntamente com as áreas de Compliance e Controles Internos e Tecnologia da Informação, devendo o conteúdo ser revisado, no mínimo, anualmente. Analisar e deliberar o relatório, anual sobre a implementação do plano de ação e de resposta a incidentes, disponibilizado pela Área de Tecnologia da Informação.

- Compliance e Controles Internos: Assegurar que as regras estabelecidas nesta Política estejam de acordo com o determinado pela Diretoria e regulamentações vigentes. Desenvolver o modelo do relatório anual sobre a implementação do plano de ação e de resposta a incidentes, bem como acompanhar o preenchimento do mesmo pela Área de Tecnologia da Informação. Fazer com que todos os colaboradores, prestadores de serviços de TI e terceiros contratados de TI tenham conhecimento deste documento.

- Tecnologia da Informação: Executar e manter os procedimentos necessários, garantindo que regras informadas neste documento sejam realizadas, em atendimento às determinações da Diretoria e Órgãos Reguladores. Preencher e disponibilizar para aprovação o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

- Colaboradores, Prestadores de serviços de TI ou terceiros contratados de TI: Cumprir integralmente as regras determinadas nesta Política. Formalizar, junto à Área de Tecnologia da Informação, qualquer ação que não condiz com o determinado nesta Política