1) OBJETIVO

Definir diretrizes para a implantação de práticas voltados a segurança cibernética/ e da informação com foco em riscos, controles, classificação e gestão da informação preservando a confidencialidade, integridade, disponibilidade e autenticidade da informação nos ambientes da Senso Corretora de Valores

2) APLICAÇÃO

Aplica-se à todas as áreas e localidades que contém informações da Senso Corretora de Valores e prestadoras de serviço.

3) REFERÊNCIAS

Normas ISO 27000, 27001 e 27002 (Segurança da Informação) e 27701 (Privacidade)
Frameworks NIST, COBIT e ITIL
LGPD - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018: Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4) DEFINIÇÕES

SEGURANÇA DA INFORMAÇÃO: Conjunto de medidas que visam a preservação da confidencialidade, integridade, autenticidade e disponibilidade das informações;
PILARES DA SEG. DA INFORMAÇÃO: Disponibilidade, confidencialidade e integridade;
SEGURANÇA FÍSICA E PATRIMONIAL - Conjunto de medidas que têm por objetivo a proteção contra ocorrências, visando evitar, conter e/ou minimizar atos deliberados que possam ou não causar danos ao pessoal, ao patrimônio, às informações, à execução dos serviços e à imagem da Senso;
FRAUDE: Subterfúgio para alcançar um fim ilícito e/ou engano dolosamente provocado, induzimento em erro ou aproveitamento de preexistente erro alheio;
PREVENÇÃO CONTRA A FRAUDE: Conjunto de medidas que têm por objetivo a prevenção e análise de todo caso de fraude na Senso;
USERNAME: Chave única de identificação do usuário para acesso a Rede, Correio Eletrônico e Sistemas de TI;

PERFIL DE ACESSO: Conjunto de permissões definidas para um posto de trabalho, conforme as necessidades do negócio.
ARQUIVAMENTO: cópia de dados de um dispositivo de armazenamento a outro para que possa ser recuperado em caso de auditoria ou consulta de dados históricos, onde a mídia de destino é armazenada em cofre;
BACKUP OU SALVAGUARDA: Guarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada;
CRIPTOGRAFIA: Mecanismo de segurança que visa proteger as informações permitindo que somente o receptor da informação circulada possa acessa-la;
DADOS PESSOAIS, PRIVADOS OU SENSÍVEIS: Dados que caracterizem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
DISPONIBILIDADE: Garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;
INCIDENTE DE SEGURANÇA: Qualquer evento que afeta ou possa afetar, de forma prejudicial e/ou maliciosa, os negócios e a integridade física e/ou lógica dos ambientes da Senso;
TESTES DE RESTORE: Processo de recuperação dos dados salvaguardados e sua colocação em produção.

5) DIRETRIZES GERAIS

As diretrizes estabelecidas nesta política visam permear os tópicos que apresentem relacionamento direto ou indireto com aspectos de segurança, classificação, controle e gestão das informações utilizadas e/ou geradas pela Senso em seu desempenho corporativo. Os princípios definidos nesta política devem ser, onde aplicável, desdobrados em normas e procedimentos adequados a sua correta execução e controle, reduzindo riscos de erros de aplicação e monitoramento. Situações específicas que não estejam contempladas ou sejam conflitantes com esta política devem ser tratadas pelo proprietário da informação em conjunto com o Comitê de Segurança Organizacional, sendo as decisões justificadas, documentadas e aprovadas pelas partes envolvidas. Periodicamente processos de revisão e atualização desta política e dos instrumentos normativos derivados desta devem ser aplicados.

6) RESPONSABILIDADES

- Diretoria**:** assegurar que esta Política de Segurança Cibernética e da Informação esteja em conformidade com a regulamentação vigente, solicitar a aprovação da mesma, emitir parecer acerca das ações a serem implementadas para correção das deficiências apontadas, garantir a orientação das áreas e gestores a respeito das regras a serem cumpridas, responder aos requerimentos dos Órgãos Reguladores, garantir que a Política esteja atualizada, devendo o conteúdo ser revisado, no mínimo, anualmente.

- Compliance: 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.
- Colaboradores, Prestadores de serviços de TI ou terceiros contratados: 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.

7) PROCEDIMENTOS, GESTÃO DE RISCOS E CONTROLES

Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, indicando o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade, nos seguintes níveis sugeridos: **Confidencia**l: Informação exclusiva a quem se destina. Requer tratamento especial e contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da instituição ou causar impactos graves, sob o aspecto financeiro, legal e normativo. **Restrita**: Informação com impacto menor do que as informações confidenciais, porém consequências relevantes. Interna: Informação que pode ser divulgada para os colaboradores da empresa, enquanto estiverem desempenhando suas atividades

profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos à empresa. **Pública**: Informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à empresa.

A área de TI é responsável por homologar os mecanismos de criptografia ou codificação para o armazenamento e a transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade entre as localidades da Senso. Os resultados da classificação estão atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

Segurança Física e do Ambiente: Todo processamento e guarda de Informações Corporativas classificadas como confidenciais devem ser mantidas em áreas com segurança apropriadas, disposta de recursos para controle de acesso. Medidas específicas para evitar o vazamento de informações impressas ou armazenadas em mídias magnéticas, classificadas como confidenciais, devem ser adotadas visando sua segurança e manutenção.

Controle de acesso e segregação de funções

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. As regras e diretrizes estão descritas na Política de Segurança Cibernética e da Informação.

Senhas

As regras relacionadas à configurações de senhas são determinadas pel 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.

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.

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.

Mecanismos de rastreabilidade

Tendo como processo extremamente importante para o bom funcionamento das operações e negócios, os sistemas 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, conta corrente e custódia de ativos.

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.

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.

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.

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.

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.

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.

Tratamento 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 através da ferramenta de registro dos incidentes, “diário de bordo”, onde são documentados o tempo de atendimento, o tipo de incidente, a criticidade e a solução.

Após algum incidente registrado no “diário de bordo” considerado com “Grau de Criticidade = Alto” a comunicação com os clientes envolvidos e com os órgãos de administração/CVM,

são realizadas com a aprovação da Diretoria.

Os monitoramentos realizados através da ferramenta ZABBIX no ambiente de controles da Senso são diversos, visando a mitigação dos riscos e dos fator de de riscos, tais como:

Links de internet
Conexão VPN
Problemas de falta ou falha de memória dos servidores
Serviços críticos
Monitoramento de espaço em disco dos servidores
Etc...
O tratamento de incidentes na Senso possui as seguintes subdivisões alinhada com as melhores práticas, como mostramos abaixo:

- Gerenciamento da disponibilidade
- Estratégia de Serviços
- Operação dos Serviços
- Melhoria Contínua

Utilização de e-mail, Internet e Telefonia
Os serviços de acesso à internet, e-mails e telefonia disponibilizados aos usuários para a realização de suas atividades durante a jornada de trabalho, devem atentar quanto à sua utilização para fins não condizentes com suas funções e responsabilidades profissionais. Os funcionários da Senso são instruidos a não utilizar internet, e-mails e telefonia de maneira que viole os acordos de privacidade de outros usuários ou infrinja legislações vigentes (leis de direitos autorais, calúnia e difamação etc.)

O acesso internet, e-mails e telefonia não deverá ser feito para fins não profissionais que não estejam previstos pela Senso, bem como para utilização de jogos e outros passatempos recreativos, correntes, redes sociais, atividades de cunho político ou quaisquer outras que possam ser entendidas como ilegais ou não autênticas.

Utilização de Software
Somente devem ser utilizados softwares que já estejam previamente homologados pela área de TI, não sendo tolerado a utilização de software sem licença ou cópia não autorizada, sem permissão formal da área de TI. Toda mudança de utilização de software deve ser previamente avaliada e aprovada pelas áreas envolvidas em conjunto com T.I., considerando os impactos no ambiente computacional da Senso.

Uma estrutura específica de controles internos de TI deve ser estabelecida, de forma que garanta a segurança dos sistemas que suportam o atendimento aos aspectos legais.

Periodicamente devem ser realizadas avaliações dos controles internos de TI e todas as não conformidades identificadas devem ser endereçadas aos responsáveis pelo processo para o estabelecimento de planos de ação

Programa de Conscientização de segurança cibernética
A SENSO disponibilizara anualmente para seus membros do quadro societario, funcionarios, colaboradores e estagiarios o programa de conscientização sobre a utilização adequada de ativos de informac;ao e prevencção a incidentes de Segurança da lnformação. Cabe ressaltar que o referido Programa de Conscientização sobre Segurança da lnformação possui as seguintes características:

- Frequencia mínima anual;
- Qustionário individual enviado para cada colaborador; e
- E-mails de conscientização enviados pela TI para todos os colaboradores.

Histórico de versões

Versão 1 – 03/06/2019
Versão 2 – 06/05/2022
Versão 3 – 19/08/2022