1. Conteúdo Deste Documento

Este documento descreve as diretrizes e procedimentos da gestão de segurança e da tecnologia da informação, afim de garantir princípios que deverão ser aplicados na proteção das informações e propriedade intelectual da organização da Nova Futura CTVM Ltda, assim como de clientes e público em geral.

2. Características Gerais

O setor de tecnologia da informação fornece o suporte necessário a todas as demais áreas da organização, de forma a permitir que as mesmas desenvolvam suas atividades com segurança, rapidez, confiabilidade e eficiência.

As ações relativas às atividades de TI são desenvolvidas por técnicos habilitados, conhecedores dos processos de negócios internos e capazes de identificar a necessidade de novos aplicativos, prospectar, avaliar e implantar softwares adquiridos de terceiros, bem como orientar os usuários na utilização dos sistemas utilizados pela corretora.

2.1. Responsabilidade Sobre Segurança Da Informação

A Nova Futura reconhece que a segurança sobre os bens da informação é uma responsabilidade de todos os seus funcionários e colaboradores. As políticas de segurança da informação são disponibilizadas em local de acesso a todos os colaboradores com proteção contra alterações.

Na medida em que as informações são essenciais ao desempenho das atividades da corretora, as rotinas de segurança garantem que as informações sejam continuamente protegidas na sua integridade, disponibilidade e confidencialidade.

O setor de tecnologia da informação responde pela gestão dos meios de armazenamento e processamento de dados, mas a responsabilidade pela autorização de acesso às informações cabe aos gestores das áreas nas quais esta informação é registrada e disponível seguindo os princípios de:

Confidencialidade: Garantindo que informações seja disponibilizada somente para pessoas autorizadas.

Disponibilidade: Garantindo que a informação sempre esteja disponível.

Integridade: Garante a completa descrição de métodos e processamentos da informação.

2.2 Conceito De Bem Da Informação

Entendemos como bem de informação todos os dados, equipamentos e softwares, diretamente relacionados com os sistemas de informação da Nova Futura e que são pré-requisitos para o seu funcionamento.

2.3 Segurança Da Informação

Esta norma de segurança da informação tem por finalidade garantir que toda informação tenha a proteção necessária no seu manuseio, tratamento e divulgação, determinando limites de comportamento e medidas a serem tomadas no caso de sua violação em consonância com o presente documento. A Gestão de Segurança da Informação envolve os seguintes aspectos:

- Definir diretrizes e responsabilidades que devem subsidiar a elaboração de normas, procedimentos e padrões de proteção da informação, abrangendo sua geração, utilização, armazenamento e distribuição;
- Evitar que usuários possam fazer o uso da informação de forma mal-intencionada, para obtenção de benefícios próprios;
- Estabelecer padrões para auxiliar a elaboração do Termo de Responsabilidade e Compromisso a ser assinado por cada funcionário e colaborador.
- Estabelecer subsídios para as implementações de cláusulas específicas nos contratos que visam garantir que a informação tenha a devida proteção;
- Atender aos objetivos dos negócios e ao Sistema de Controles Internos da corretora.

2.3.1 Diretrizes De Segurança Da Informação

A Nova Futura manterá sistemas confiáveis mediante utilização de elevados padrões tecnológicos de segurança de rede, para evitar fraudes internas e invasões e garantir o sigilo de toda informação e comunicação interna e externa, especialmente via internet.

Toda informação relevante deverá ser protegida, de acordo com seu grau de sigilo, integridade e disponibilidade, de forma a atender aos objetivos de segurança da informação.

São realizadas periodicamente manutenções e atualizações técnicas e de segurança, de forma a manter em plenas condições de funcionamento, os equipamentos de informática e de telecomunicações.

As ações que afetam a segurança da informação são registradas com número do incidente e descrição e ficam disponíveis para avaliação de risco pelo compliance ou diretoria.

Somente a diretoria da Nova Futura pode autorizar a divulgação pública de informações dos diversos setores, independentemente do canal de comunicação: mídia impressa, eletrônica ou qualquer outro meio.

Quando as informações se tornarem sem utilidade aos negócios da Nova Futura serão destruídas, independentemente do conteúdo e a forma de armazenamento, sempre respeitando a as regras de reaproveitamento ou descarte de informação.

2.3.2 Diretrizes Operacionais

Todos os programas que tratam dados da Nova Futura devem ser homologados e conter trilhas de rastreamento de forma que uma auditoria possa identificar o responsável da ação e que atendam às especificações técnicas estabelecidas quando requerido.

São utilizados equipamentos de rede que possibilitam a segmentação e/ou integração com outras redes, facilitando essas interligações, preservando segregados os interesses de tráfego de cada rede e evitando o congestionamento e outros efeitos que possam prejudicar seu desempenho

3. Critérios Básicos E Controles

3.1 Gestão De Ativos

Ativos são todo e qualquer equipamento ou software que possa criar, processar ou armazenar informação. Todos os ativos devem ser identificados e inventariados de acordo com suas características e protegidos de acesso indevido disponibilizados em documento e atualizados anualmente.

3.2 Controle De Acesso Lógico

Aos colaboradores, inclusive aos estagiários e prestadores de serviço deverá ser fornecida uma identificação pessoal para acesso aos recursos tecnológicos.

Esta concessão de acesso será feita com base nas necessidades funcionais de cada colaborador e terá como suporte a autorização do gestor do negócio ou do processo de suporte, devidamente documentada. Esta autorização poderá ser feita por sistema, e-mail ou documento físico e aprovada pela diretoria responsável por cada área/processo.

Essa identificação, representada por meio de login e senha, deverá ser pessoal, intransferível e tratada confidencialmente.

A correta utilização da identificação é de responsabilidade de cada usuário.

As informações e os recursos tecnológicos (sistemas informatizados e equipamentos) serão disponibilizados apenas aos colaboradores quando necessitarem utilizá-los no exercício de suas atividades profissionais.

Os equipamentos de informática deverão ser dotados de dispositivos de segurança contra acessos e instalação de programas não autorizados.

3.2.1 Regras De Acesso De Segurança/Usos De Senha

- Política de senha para estações e aplicativos de negociação.
- Tamanho mínimo de senha: Seis caracteres;
- Senha inicial auto expirada (troca compulsória): sim
- Prazo de necessidade de troca obrigatória: 30 dias
- Senhas recentes não aceitas em troca: Seis últimas
- Tentativas de acesso inválidas para bloqueio: Três
- Necessidade de pedido de inativação por férias: Sim (o RH deve informar a equipe de tecnologia quais funcionários estão de férias)
- Duração do bloqueio: até o administrador liberar
- Requisito de complexidade de senha: ativado
- Criptografia: ativado.

- Orientação geral para acessos a todos os sistemas:
- Evitar o uso de senhas óbvias e que usem dados reais do usuário (nome de esposa (o), filhos, e outros, datas, números de documento);
- Não anotar a senha em local visível e que facilite sua identificação para uso indevido;
- Somente serão permitidas identificações de acesso não nominais para necessidades técnicas de sistemas ou infraestrutura devidamente gerenciada pela TI.
- A disponibilização do acesso concedido nominalmente a um colaborador para outro será considerada falta grave suscetível de punição prevista na legislação trabalhista e cível.

3.2.2 Concessão E Revogação De Acessos

Na admissão ou desligamento de colaboradores deve seguir os processos internos de concessão e aprovação de acessos da corretora assim como a revogação, conforme os parâmetros da matriz de segregação de acessos vigente.

Os procedimentos devem seguir os seguintes passos:

Solicitação de Acesso

Quando do ingresso de um novo colaborador, o RH ou o *Compliance* encaminham o *Check* list para conhecimento da Diretoria.

Aprovação dos Acessos

Os acessos são aprovados pela Diretoria

Concessão de Acessos

Após a aprovação, a T.I. concede os acessos

Reavaliação

Caso detectado algum conflito a T.I. encaminha para a Diretoria, copiando o Compliance

Revogação

A área de T.I. após comunicação deve revogar todos os acessos.

3.3 Desenvolvimento, Aquisição E Instalação De Softwares

Todas as ferramentas desenvolvidas ou adquiridas devem ser de uso exclusivo para o tratamento das informações da Nova Futura, deve se prever também que todos os softwares devem ser homologados, testados e protegidos conforme os procedimentos de gestão de mudança da Nova Futura.

3.4 Segurança Física

Os funcionários e colaboradores da Nova Futura utilizam TAG RFID de acesso aos ambientes internos visando evitar acessos indevidos por pessoas não autorizadas nas áreas de acesso restrito.

Os funcionários e prestadores de serviços de manutenção ou suporte de terceiros são autorizados a acessar o ambiente de DATA CENTER somente mediante acompanhamento de funcionário de TI.

As mídias que contenham informações da Nova Futura são mantidas permanentemente em áreas de controle restrito em cofre seguro no departamento de TI e sua movimentação para fora da empresa, somente ocorre sob rígido controle de pessoa designada.

3.5 Segurança Na Comunicação De Dados E Voz

As instalações e equipamentos de comunicação de dados e voz são gerenciados de modo a que seja mantida a segurança e inviolabilidade das informações que trafegam por elas. A Nova Futura em conformidade com legislação vigente mantém sistema de gravações das comunicações feitas pelos seus funcionários e colaboradores que utilizam os equipamentos e instalações, visando preservar a corretora no caso de eventuais ações dolosas ou contrárias a seus interesses comerciais.

Da mesma forma o monitoramento de acessos à internet e utilização de e-mails deverá ser feito somente para uso exclusivo no exercício das atividades profissionais que estão sujeitas a monitoramento eletrônico.

As gravações e rotinas de monitoramento serão feitas com base em concordância expressa dos funcionários e colaboradores mediante adesão e assinatura de Termo de Responsabilidade e Compromisso com as Normas de Segurança da Informação da Nova Futura.

3.6 Segurança De Hardware E Software

As estações de trabalho utilizadas pelos funcionários e colaboradores dispõem de políticas ou ferramentas que protege o equipamento e a rede de dados e impossibilita, que os usuários extraiam informação através de mídias removíveis ou instalem programas não autorizados pela área de Tecnologia da Informação. Dispositivos removiveis podem ser abertos somente em modo leitura.

3.6.1 Proteção De Cyber Segurança

A Nova Futura detém ferramentas de controle contra intrusão em camada de borda e softwares com inteligência artificial que detectam anormalidades no ambiente abrangendo todos os servidores e estações de trabalho, as ferramentas estão sempre atualizadas conforme recomendação do fabricante.

Os servidores com acesso à internet e e-mail dispõem de firewalls e ferramentas de segurança de rede com proteções contra tentativas de acessos não autorizados.

Os controles de cyber segurança são constantemente verificados e passiveis de evolução de acordo com o gestor de tecnologia. Podendo ser classificado da seguinte forma:

Crítico: Correções de emergência, a fim de mitigar erros ou tentativas de intrusão.

Sustentabilidade: Planos de ações de curto ou médio prazo para mitigar erros mantendo o ambiente seguro.

Estruturantes: Planos de ações de médio ou longo prazo que tratam de mudanças mais profundas ao ambiente afim de torná-lo seguro ou preparar para tecnologias futuras.

3.7 Trilhas De Auditoria

Os softwares referentes aos processos de negócios e de controle dispõem de trilhas de auditoria para assegurar o rastreamento de eventos. Essas trilhas incluem:

- Identificação do usuário;
- Data e horário de ocorrência do evento;
- Identificação do evento (inclusão, alteração ou exclusão).

3.8 Normas De Backup

Foram estabelecidas as seguintes regras quanto à realização de backups:

- Geração diária de cópias de segurança;
- Inclusão de todas as informações armazenadas nos servidores;
- Guarda dos arquivos em duas cópias mantidas em locais distintos.
- Garantia de sua integridade, quando de uma eventual necessidade de restauração.

A restauração das informações armazenadas e sua integridade são testadas por amostragem, de acordo com rotina estabelecida pela área de TI.

No caso de identificação de erros, esses serão devidamente registrados inclusive a solução adotada, que poderá ser tratada como uma ação corretiva formalizada com registro e número de incidente contento análise de risco e aprovação do compliance.

3.9 Segurança No Ambiente De DATA CENTER

A área de tecnologia mantém no ambiente do DATA CENTER controlado com sensores de temperatura e umidade relativa do ar do data center que está conectado com a rede para enviar alertas sobre as condições do ambiente.

Os equipamentos estão ligados à rede de energia elétrica, devidamente aterrada com estabilizador de voltagem e filtro de linha conforme a necessidade que garantem:

- A uniformidade da tensão da rede, em casos de picos de energia;
- A entrada em operação das baterias, na falta de energia elétrica, a autonomia é verificada periodicamente.

Também com outros métodos de sensores de sistemas de combate a incêndio e com permissão de acesso apenas às pessoas autorizadas.

Periodicamente são verificadas as instalações da corretora em relação a riscos potenciais de incêndio, e realizadas manutenções periódicas dos extintores e sistema de prevenção de incêndio, de acordo com as recomendações dos fabricantes.

3.10 Monitoramento Da Rede

A área de tecnologia dispõe de monitoramento da rede e recursos críticos para gestão de falhas e acompanhamento da capacidade dos recursos tais como: trafego da internet, links, monitoramento do trafego da rede interna e externa (LAN/WAN).

Adicionalmente é monitorado o desempenho dos servidores quanto a utilização de espaço/CPU, capacidade de processamento e memória.

Um sistema de alarmes está configurado para indicar qualquer equipamento desligado ou quando qualquer servidor ou outro equipamento da rede atingir aos 80 % da sua capacidade, estes valores também podem ser ajustados de acordo com a necessidade.

A partir dessa indicação a equipe de T.I avalia o grau de comprometimento do servidor ou outro equipamento da rede, quanto a (à) necessidade de sua substituição.

3.11 Aquisição De Hardware/Softwares

Pesquisar no mercado, dentre os fornecedores / prestadores de serviços homologados, aqueles que apresentam condições de atender às necessidades dos usuários, elaborando cotação de preço junto a fornecedores, respeitando o seguinte fluxo:

Avaliar, com a participação dos diretores e usuários, os softwares selecionados, quanto aos seguintes quesitos:

- Arquitetura;
- Adequação de seus requisitos e especificações às necessidades da área/processo.
- Necessidade de customização:
- Viabilidade técnica e aderência à plataforma tecnológica;
- Facilidade de operação e de manutenção;
- Documentação e procedência;
- Licença de uso;
- Relação custo-benefício.

Propor a aquisição, preferencialmente, dos chamados softwares de prateleira (sistemas operacionais, editores de texto, planilhas e outros) junto com os equipamentos ou sob a forma de licença de uso, dando cobertura a cada cópia requerida conforme sua necessidade.

Apresentar à diretoria o resultado da avaliação e da cotação de preços, obtendo a aprovação para a aquisição do hardware / software.

Efetuar os testes para homologação do sistema a ser adquirido, em ambiente de teste, selecionando a melhor solução a ser indicada para aquisição.

Obter a aprovação da contratação do sistema pelos respectivos usuários e Diretoria, após concluir por sua adequação técnica, orçamentária e negocial.

Todas as aquisições devem ser acompanhadas de seus respectivos documentos, contratos, notas de acordo com os métodos de contração, perpetuo, mensal ou anual.

A cotação para aquisição de novos equipamentos/softwares ou contratação de empresas prestadoras de serviços é realizada pela área de TI, porém, as aquisições e contratações são analisadas e aprovadas pela diretoria da Nova Futura.

3.12 Contratação De Serviços

Observar os procedimentos quanto ao recebimento da solicitação do usuário.

Selecionar dentre os prestadores de serviços homologados, no mínimo 3 (três) empresas, obtendo as respectivas propostas.

Analisar as propostas em conjunto com os usuários / diretoria e adotar os procedimentos previstos para contratação do serviço, pagamento e arquivamento da documentação.

Após a aquisição e implantação do novo hardware e software, atualizar o bem no Inventário de TI, e atualizar seus controles de licenças de software.

3.13 Instalação De Hardware E Serviços

O equipamento deve ser configurado para instalação na rede da corretora e outros links externos, mediante a instalação dos softwares necessários.

Habilitar os usuários para uso dos softwares de rede, mediante senha de acesso.

3.14 Comunicação De Dados E Voz

A manutenção da infraestrutura de comunicações da Nova Futura envolve:

- Links de dados de alta velocidade conectando a corretora com a rede de negociação.
- Conexão dedicada aos serviços de Home Broker;
- Links de contingência;
- Ambiente de rede de dados;
- Linhas telefônicas;
- Sites ativo/ativo;
- Canais de voz;

- Sistemas de gravação de voz e mensagens instantâneas.

O Setor de tecnologia da informação dispõe de meios para garantir a não interrupção das comunicações, efetuar o monitoramento do desempenho dos links de dados, adotar providências internas junto às concessionárias para melhoria do desempenho e corrigir eventuais problemas.

O monitoramento das gravações de ligações telefônicas e mensageria, é feita diariamente pela área de compliance.

3.15 Abertura E Fechamento De Chamados (Help Desk)

Os chamados são operacionalizados e monitorados pela área de TI mantendo registro e número de chamados para o acompanhamento e resolução de problemas.

O profissional técnico designado para atender ao chamado após diagnosticar e resolver o incidente atualizará o sistema com o status do chamado até seu encerramento.

O registro e controle das demandas permite ao gestor de TI monitorar o status do chamado e as estatísticas das demandas de serviços, contendo informações e indicadores sobre as áreas solicitantes, técnicos designados e categorização de incidentes.

3.16 Inventário

Relacionar em meio eletrônico (planilha) todos os bens de informação existentes na Nova Futura discriminando, entre outras, as seguintes informações:

- Departamento e usuário responsável;
- Quantidade, marca, modelo e características;
- Sistema operacional e aplicativos instalados ou acessados através do equipamento;
- Dados relativos à rede de transmissão de dados acessada pelo equipamento.

Registrar também, em planilha eletrônica, os servidores utilizados pela Nova Futura, suas características, utilização e abrangência.

Atualizar o inventário, constantemente sempre que ocorrer uma inclusão ou exclusão de item ou na alteração de qualquer um dos dados contidos em seus registros.

Confrontar, periodicamente, sendo pelo menos uma vez ao ano as informações do inventário dos bens próprios com a posição do registro contábil de controle patrimonial e daqueles em comodato com a respectiva documentação.

3.17 Plano De Continuidade

A Nova Futura mantém um plano de continuidade de negócios que define as ações de contingência para eventos graves, com os respectivos sistemas, links e estações de trabalho prevendo operação alternativa para os casos de indisponibilidade de rede, sistema, dados ou comunicações nas mesas de forma a mitigar os riscos de interrupção das atividades essenciais da corretora, foram previstos procedimentos a serem adotados em qualquer situação contingencial, inclusive para os sistemas de negociação na internet, preservando, assim, o atendimento aos investidores e a preservação das atividades internas.

As pessoas envolvidas nos planos de contingência são adequadamente treinadas para execução das ações de sua responsabilidade, os testes são executados conforme cronograma estabelecido, os planos são atualizados sempre que necessário, e os recursos alternativos (sistemas e sites de contingência) quando requeridos são disponibilizados para uso, dentro dos prazos mínimos requeridos.

O Plano de Continuidade de Negócios deverá ser objeto de testes, no mínimo anualmente, devidamente formalizado em relatório específico, cujos resultados são apresentados à diretoria para validação e comprometimento com a solução de eventuais problemas que possam resultar em riscos para a corretora.

No caso de interrupção das atividades da corretora, o plano de recuperação e continuidade será acionado conforme definido no Plano de Continuidade de Negócios - PCN da Nova Futura.

Estas definições foram estabelecidas com base nas avaliações de risco contidas no PCN.

4.Segregação De Funções

Durante a admissão de um novo colaborador é necessário o envio dos seus respectivos acessos a área de tecnologia após a aprovação de compliance e diretoria, que concede os acessos conforme a sua função, caso seja identificado um conflito o acesso é descrito em planilha com a data e identificação de aprovação da diretoria.

O controle e registro dos acessos aos sistemas internos da Nova Futura são concedidos conforme a área de atuação de cada colaborador da Nova Futura e revisados pelo menos a cada 6 meses.