POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Data: Dezembro de 2017

SUMÁRIO

1. Introdução

Esta política ("Política") tem como objetivo detalhar os instrumentos e processos que visam manter a segurança das informações e das atividades desempenhadas no que se refere à segurança dos sistemas de informações confidenciais, bem como detalhar a periodicidade de verificação da integridade dos sistemas adotados.

2. Aplicabilidade

Esta Política é aplicável a todos os Colaboradores da Infinity, independentemente do nível hierárquico, os quais deverão ter ciência de seu conteúdo e eventuais atualizações, e busca refletir:

- ✓ A estrutura adotada pela Infinity para assegurar a proteção a informações confidenciais mantidas nos sistemas;
- ✓ Os critérios e os procedimentos básicos a serem adotados pelos Colaboradores da Infinity a fim de minimizar o risco de exposição da informação confidencial;

- ✓ A periodicidade e o tipo de teste empregado a fim de verificar a integridade dos sistemas adotados.

A ciência pelos Colaboradores das práticas, rotinas e procedimentos previstos nesta Política não os desobriga de ter conhecimento e de observar os conteúdos previstos nas demais políticas e manuais adotados pela Infinity, incluindo, sem limitação, o Código de Ética e Conduta e o Manual de Compliance.

Os Colaboradores que desejarem maiores informações sobre as demais políticas e manuais adotados, ou que tenham qualquer dúvida a respeito do conteúdo da presente Política e/ou dos procedimentos a serem adotados, deverão contatar a equipe de compliance, presencialmente ou por meio dos seguintes canais de comunicação:

Telefone: (11) 3049-0732
E-mail: infinity@infinityasset.com.br

3. Política de Segurança da Informação

Esta Política tem por objetivo detalhar os instrumentos e processos que visam manter a segurança das informações e das atividades desempenhadas, inclusive no que se refere à segurança dos sistemas de informações confidenciais.

Para tanto, a estrutura adotada pela Infinity está dimensionada e preparada para eventuais paralisações decorrentes de queda de energia e casos de contingência de equipamentos, passando por testes periódicos que visam verificar sua integridade, nos termos abaixo:

(i) Sistema STI - É realizado teste de restauração de toda base de dados em servidor de contingencia, sendo assim dando continuidade na utilização do sistema STI. Sistema o qual é utilização pela mesa de negociações;

(ii) Sistema de Arquivos - Testes de restauração de arquivos e diretórios em outro servidor, que assumirá função de servidor de arquivos. Arquivos utilizados por toda empresa, como planilhas ou documentos.

3.1. Infraestrutura de Comunicação

A rede de dados e voz é toda estruturada e certificada, a Infinity conta, ainda, com servidores adequados e eficientes à aplicação, todos com discos espelhados, equipamentos redundantes e de contingência. Backups diários permitem rápida restauração das informações, se necessário.

A infraestrutura de comunicação da Infinity utiliza links dedicados e redundantes para Internet, linhas diretas para contingência do E1 além de LPs (Linhas Privadas), que permitem a comunicação independente e direta com as corretoras e bancos. Esta estrutura se completa de forma eficiente e segura através de duas centrais telefônicas de específicos – Sistema IPC Alliance Voip IQMAX e Tadiran Coral IPx500, com sistema de gravação Vox Perfect IP.

A Infinity adota sistema de gravação de voz dedicado para todos os seus departamentos. Solicitações de gravações podem ser realizadas para a equipe de tecnologia de informação, as quais dependerão de autorização prévia do Diretor de Compliance e Riscos para envio ao solicitante. Todo o processo é feito e arquivado através de e-mail.

3.2. Infraestrutura Física

O acesso de qualquer pessoa às instalações da Infinity só é feito mediante autorização por Colaboradores responsáveis por esse controle e mediante identificação do visitante, com os registros através de foto e identificação de documentos.

O acesso às instalações é controlado por meio com sistema de controle de acesso interno, que segrega o acesso a cada departamento e nas áreas técnicas, sempre identificando e registrando todos os acessos, com informações sobre o Colaborador, local, data e horário de acesso. O sistema também permite que cada Colaborador tenha acesso somente às áreas que lhe competem, assim, por exemplo, apenas a equipe de tecnologia da informação possui acesso ao data center. A Infinity também conta com sistema de gravação de imagem em suas instalações.

3.3. Infraestrutura Eletrônica

A segurança das informações conta, ainda, com bloqueio de portas USB e dos gravadores de mídia em todos os computadores, segregando as informações através de estrutura apartada de diretórios, por meio do qual cada Colaborador tem acesso somente às informações das respectivas equipes a que pertencem. Esse acesso se dá via login e senha individual de cada Colaborador que autorizam o acesso a um diretório exclusivo, cujas informações e conteúdo disponível levam em consideração sua atividade, nível hierárquico e departamento. Desta forma cada Colaborador só tem acesso aos sistemas e informações previamente autorizados pelos diretores da Infinity.

Adicionalmente, a segurança das informações provedor de e-mail da Infinity, hoje terceirizado com a empresa Telium, é garantida por meio de certificado SSL para suas portas de acesso. Desta forma, todos os e-mails enviados pelo domínio da Infinity seguem criptografados até o seu destinatário, evitando possíveis perdas ou furto de informações.

A senha de acesso é uma das ferramentas disponíveis para garantir a integridade e a confidencialidade dos dados da Infinity, evitando eventual uso indevido. Para outros aplicativos adotados pela Infinity, tais como os Sistemas DMA e Market Datas, dentre outros, a senha individual serve para garantir a disponibilidade do sistema a seu usuário legítimo e seu uso por um único Colaborador, evitando que a conexão em uso seja desconectada.

Para as medidas acima descritas sejam efetivas, é fundamental que a senha associada ao login individual seja criada pelo próprio Colaborador, com caracteres alfanuméricos e com no mínimo seis dígitos. Tal login e senha são de uso pessoal e intransferível, dando acesso exclusivo ao Colaborador aos sistemas da Infinity. Este vínculo garante que o respectivo login seja utilizado somente por um único colaborador, não sendo possível a criação do mesmo login para Colaboradores distintos.

Todos os Colaboradores são orientados, inclusive através de normas internas, a desligarem seus equipamentos no final do dia, para isso fazendo logoff de todos os sistemas, bem como a manter documentos físicos trancados. Qualquer documento mantido sobre a mesa dos Colaboradores ao final do dia é recolhido para guarda e devolução no dia útil seguinte.

Como forma de minimizar o risco de roubo de informações ou contaminações dos sistemas, não é permitida ou utilizada qualquer forma de acesso externo ou conexão com os servidores internos da Infinity. A Infinity adota, ainda, antivírus Kaspersky e monitoramento da rede e do tráfego de dados, além de controlar eventuais instalações de sistemas ou softwares não autorizados.

3.4. Testes Periódicos de Segurança

A fim de verificar a integridade dos sistemas adotados, inclusive com relação aos sistemas de informações confidenciais mantidas em meio eletrônico, a equipe de tecnologia da informação realiza

testes semestrais, que são formalizados por meio de relatório enviado ao Diretor de Compliance e Riscos.

Semestralmente a equipe de tecnologia da informação enviará e-mails separados para os respectivos coordenadores de cada Colaborador, contendo a lista de todos os sistemas e quais Colaboradores possuem acesso a cada um. Os coordenadores deverão confirmar as prerrogativas dos Colaboradores e se deverá ser mantido o acesso a cada um desses sistemas.

Em linha com o exposto acima, o relatório semestral a ser enviado ao Diretor de Compliance e Riscos deverá conter:

- ✓ a lista de todos os sistemas e quais Colaboradores possuem acesso a cada um, preparada em linha com as confirmações dos respectivos coordenadores; e

- ✓ eventuais inconsistências detectadas em cada um dos sistemas.

O Diretor de Compliance e Riscos deverá revisar a lista de atribuições, confirmando a adequação dos acessos de cada Colaborador ao seus respectivos cargos e prerrogativas, além de adotar eventuais medidas cabíveis para correção das inconsistências detectadas no relatório descrito acima.

4. Atualizações desta Política e demais manuais e políticas da Infinity

Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da Infinity.

As atualizações das demais políticas da Infinity devem ser realizadas pelos gestores responsáveis pelas atividades endereçadas por cada política.

Todas as políticas e manuais da Infinity passarão pelo seguinte procedimento de elaboração e revisão:

- ✓ Gestor responsável pela alteração solicitada e/ou inclusão de novo procedimento na política;
- ✓ Revisão pelo gerente de riscos, caso pertinente;
- ✓ Revisão pela Gerente de Compliance; e
- ✓ Revisão pelo Diretor de Compliance e Riscos.

As versões atualizadas da presente Política serão enviadas a todos os Colaboradores por e-mail pela equipe de tecnologia da informação com aviso de recebimento.

4.1. Controle de revisões

Revisão da Política	Data	Motivo
Área da Segurança da Informação	Outubro, 2014	Elaboração
Área da Segurança da Informação	Dezembro, 2017	Revisão geral