POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Data: fevereiro de 2019

SUMÁRIO

1. Introdução

Esta política ("Política") visa relatar os instrumentos e procedimentos para manter a segurança das informações das atividades desempenhadas na Infinity no que se refere à segurança dos sistemas de informações, além de contemplar os procedimentos estabelecidos pela Resolução BACEN nº 4.658/2018, que dispõe sobre a segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

2. Objetivo

O principal objetivo da Política de Segurança da Informação e Cibernética é esclarecer os procedimentos operacionais e técnicos que visam garantir, de forma solidária, a segurança das informações dos clientes ou de qualquer pessoa, seja física ou jurídica que possuírem seus dados cadastrais registrados nos sistemas utilizados na Infinity.

Os controles adotados para reduzir a vulnerabilidade da Infinity a incidentes e atender os objetivos de segurança cibernética estão descritos no decorrer da referida política, a saber:

3. 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: compliance@infinityasset.com.br

4. Estrutura

A Infinity conta com um Diretor e dois profissionais de tecnologia, estando de acordo com seu porte, perfil e modelo de negócio. Sua estrutura sistêmica está dimensionada e preparada para eventuais paralisações decorrentes de queda de energia e casos de contingência de equipamentos que passam por testes periódicos que visam verificar sua integridade, nos termos abaixo:

- ✓ 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;

- ✓ 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.

5. Controles específicos

Para a rastreabilidade da informação no sentido de buscar garantir a segurança das informações sensíveis a Infinity;

- ✓ Adota monitoramento e análise de logs de acesso quanto a utilização rotineira dos recursos no intuito de identificar anomalias atípicas ao perfil ou ao acesso realizado pelo usuário;

- ✓ Realiza acompanhamento periódico quanto aos acessos restritos das atividades realizadas por cada colaborador que atua com dados sensíveis, seja de pessoa física ou jurídica;

6. Ocorrências de Curso Anormal

Diante de incidentes, a Infinity atua no mapeamento das atividades consideradas críticas e essenciais para a continuidade dos negócios.

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes, caso ocorram, deverão ser registrados e controlados por formulário específico contendo as informações abaixo:

- ✓ Data de Ocorrência;
- ✓ Breve Relato;
- ✓ Consequências;

- ✓ Providências para regularização;
- ✓ Ciência e despacho da Diretoria;
- ✓ Evidências.

Por meio das ocorrências registradas no referido formulário, os profissionais da área de tecnologia da informação atuam no sentido de mitigar e evitar reincidência e/ou novos incidentes.

Para a prevenção e tratamento dos incidentes a serem adotados por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou relevantes a Infinity adota o envio de um termo de confidencialidade das informações que deverá ser lido, compreendido e assinado por todos os prestadores de serviços;

Ainda, a Infinity atua na atua na revisão periódica das cláusulas contratuais estabelecidas em contrato visando identificar, entre outras, a existência de cláusula específica de segurança cibernética;

Para a classificar os dados e as informações quanto sua relevância são considerados:

- ✓ Nível de importância das informações;
- ✓ Grau de confidencialidade;
- ✓ Conteúdo, quando confidencial, estratégico ou que envolve dados cadastrais;
- ✓ Classificação do profissional responsável pela atividade;
- ✓ Classificação da área/departamento;
- ✓ Atividades que exigirá o uso da informação.

Os parâmetros abaixo são os utilizados na avaliação da relevância dos incidentes:

- ✓ A classificação da criticidade do recurso afetado;
- ✓ A classificação da criticidade da informação;
- ✓ O tempo de resposta, restauração e regularização do incidente;
- ✓ Os tipos de contornos, ou seja, qual o procedimento a ser realizado interinamente até a regularização do incidente.

Os procedimentos e os controles descritos no decorrer desta Política abrangem, inclusive:

- ✓ A autenticação por login e senha com grau de complexidade e criptografia;
- ✓ A prevenção e a detecção de intrusão através de utilização de firewall (IDS);
- ✓ A prevenção de vazamento de informações através de bloqueio de acesso a gravadores com monitoramentos realizados pela área de tecnologia;
- ✓ A proteção contra softwares maliciosos realizando testes periódicos e varreduras para a detecção de vulnerabilidades por meio dos sistemas de antivírus e firewall;
- ✓ Os mecanismos de rastreabilidade por meio das trilhas de auditorias e logs de eventos;

- ✓ Os controles de acesso e de segmentação da rede de computadores em ambientes, diretórios e arquivos específicos e segregados;
- ✓ A manutenção de cópias de segurança dos dados e das informações por backups com testes periódicos de integridades nas cópias.

6.1. Infraestrutura de Comunicação

O Infinity busca adotar tecnologias de segurança da informação com o objetivo de impedir:

- ✓ Acesso e/ou transmissão de informações e/ou arquivos confidenciais para pessoas não autorizadas;
- ✓ Liberação de senhas e códigos de identificação de usuários; e
- ✓ Ocorrência de ataques cibernéticos.

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.

6.2. 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.

6.3. 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.

O serviço de mensagens de e-mail é terceirizado e fornecido pela Microsoft com uma solução denominada Exchange Online, 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 é 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 expediente, para isso fazendo logoff de todos os sistemas, bem como a manter documentos físicos trancados. Quaisquer documentos, mídias, como por exemplo: DVD, CD ou Discos Rígidos, quando não mais utilizados, são “triturados” antes do descarte.

Como forma de minimizar o risco de roubo de informações ou contaminações dos sistemas, não é permitido ou utilizado 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.

6.4. Serviços de Nuvem

A Infinity assegura que toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem será previamente comunicada ao Banco Central

do Brasil.

Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados possuem acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.

Os acessos são controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada usuário colaborador ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

6.5. 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 e nas melhorias contínuas dos procedimentos relacionados com a segurança cibernética registradas nesta política.

7. Treinamento

É atribuição da área de Compliance criar monitoramento específico no sistema de Controles Internos obtendo, de forma eletrônica, respostas de cada colaborador quanto a leitura e entendimento e a adesão desta Política, bem como, monitorar a veracidade das respostas registradas no sistema.

Ainda, aplicar, em parceria com a área de Tecnologia, treinamento anual com consecutiva avaliação e assinatura em lista de presença;

8. Atualizações desta e demais 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.

Esta e demais políticas 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
- ✓ Avaliação e aprovação do Diretor responsável por esta Política.

A versão atualizada desta Política será publicada na Internet e Intranet e deverá ser lida por todos os colaboradores.

9. Controle de revisões

Revisão da Política	Data	Motivo
Segurança da Informação	07/11/2011	Elaboração
Segurança da Informação	05/03/2015	Revisão e Publicação
Segurança da Informação	07/12/2017	Revisão
Segurança da Informação	27/12/2018	Revisão
TI e Compliance	08/02/2019	Revisão (Cibernética)