POLÍTICA E NORMAS DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1.Introdução

A Segurança da Informação evoca a proteção dos ativos de informação, sistemas, recursos e serviços contra desastres, erros, uso indevido, roubos e manipulação não autorizada, visando minimizar os danos ao negócio e maximizar o retorno dos investimentos e das oportunidades de negócio. Independentemente do ambiente em que se encontra armazenada a informação (ambiente computacional, papel, outros), como todo ativo da empresa, ela tem valor e precisa ser adequadamente protegida de uma forma profissional e estruturada.

O Diretor de *Compliance* apoiará e fomentará as iniciativas necessárias ao alcance dos objetivos, norteado pelas Diretrizes e Políticas de Segurança estabelecidas. Sendo que a aplicação e monitoramento da Política de Segurança da Informação cabem ao Diretor de *Compliance*, que nomeará para seu auxílio Gestor de Tecnologia, membro devidamente qualificado para a gestão da segurança da informação e suporte tecnológico.

A política de Segurança da Informação deve ser revisada e atualizada, no mínimo anualmente, pelo Gestor de Tecnologia, com o apoio das áreas Administrativas e de Tecnologia, a fim de incorporar medidas relacionadas a atividades e riscos novos ou anteriormente não abordados. Desta forma, cabe a Diretoria de *Compliance*, por meio da aprovação das medidas apontadas pelo Gestor de Tecnologia, reeditar a Política e Normas da Segurança da Informação.
Esta Política configura instrumento de orientação para a conduta pessoal e profissional dos Membros. A Política deve ser analisada e aplicada em conjunto com os demais Manuais e Politicas da Lastro.

A efetividade da Política de Segurança da informação depende de sua ampla adesão pelos Membros da Lastro, portanto, a disseminação desta política e da cultura de Segurança da Informação constituem atribuições essenciais do Diretor de *Compliance*, atuando com apoio da equipe de Tecnologia e Informática e do Gestor de Tecnologia.

Os objetivos a que se refere o parágrafo acima se cumprem pela disponibilização de material informativo, a ser realizadas segundo os parâmetros estabelecidos nesta política, e comprovado pela assinatura do Termo de Ciência que compõe o Anexo I desta Política.

2.Aplicabilidade

Esta Política de Segurança da Informação aplica-se aos Diretores, Colaboradores, Assemelhados, Parceiro de negócio, Consultores, Prestadores de serviço, e Fornecedores (“Membros”) que se utilizam dos ativos de informação da Lastro, os quais são também responsáveis pela referida segurança, estando cientes de seu compromisso com a proteção e o uso adequado da informação.

A Política de Segurança da Informação é aplicável tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação. Abrange todos os equipamentos possuídos ou utilizados contendo informações da Lastro.

3.Definições referentes à Informação e sua segurança

Os termos que nesta Política de Segurança da Informação são grafados com inicial maiúscula possuem as definições avançadas neste item 3, salvo quando especificado de maneira distinta no corpo dos demais itens que compõe esta política.

Ativos de Informação: é o ativo que é produzido pela dinâmica da organização, fruto de suas transações negociais e de seus controles operacionais. Utilizado como instrumento e suporte à decisão. A percepção material da informação é aquela que estiver contida nos seguintes meios de armazenamento:

formulários, relatórios, telas de aplicativos, tutoriais, documentos em geral, e-mail, arquivos em meio magnético e digital, quadros de aviso, memorandos, normas, comunicações internas e correspondências.

Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;

Custodiante: pessoa com atribuição, definida pelo titular da área, de proteger adequadamente esta informação;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes;

Incidente de segurança: concretização do ato de exploração de uma vulnerabilidade;

Informação: é um recurso fundamental para o desenvolvimento das atividades da Lastro, e, como tal, necessita ser protegida. A segurança da informação visa preservar a confidencialidade, a integridade e a disponibilidade da informação;

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

PSI: Política de Segurança da Informação;

Responsável pelo processo: gestor responsável por um conjunto de procedimentos que manuseia informações logicamente relacionadas para alcançar determinado fim. Propõe o nível de classificação da informação;

Vulnerabilidade: fraqueza de um ativo informacional ou grupo de ativos que podem ser explorados por uma ameaça;

Equipe de Informática: Equipe compostas pelos seguintes Membros: Gestor de Tecnologia e terceiros contratados para a prestação de suporte em serviços de tecnologia e informática.

PADCN: Processamento e Armazenamento de Dados e Computação em Nuvem

RTM: RTM - Rede Telecomunicações para o Mercado Ltda.

4. Regras

As Informações relativas às operações, dados pessoais, dados de clientes, atividades e procedimentos são classificadas, salvo quando seu caráter público seja notório, como confidenciais, e devem ser armazenadas, copiadas, transmitidas, manuseadas, descartadas e destruídas, nos termos dessa política.

As divulgações das informações não são somente aquelas materializadas por meios físicos, mas também aquelas que forem verbalizadas; estas, tanto quanto as outras, exigem o mesmo comportamento ético de confidencialidade.

Todos que fazem uso das informações da Lastro devem ter acesso físico e lógico liberado somente aos recursos de informação necessários e indispensáveis ao desempenho de suas atividades, e em conformidade com os interesses da Lastro.

O uso de equipamentos para tratamento e operações das informações da Lastro devem ser compatíveis com o Manual de Boas Práticas do uso da Tecnologia da Informação.

É competência do Diretor de *Compliance*, solicitar o acesso à rede ao Gestor de Tecnologia. A instalação e execução de *software* e aplicações devem estar sujeitas à sistema de execução e controle de processos, de forma que, apenas usuários previamente autorizados possam autorizar tais operações.

Conforme a Resolução 4.658/2018 do Banco Central do Brasil, para a contratação de serviços de PADCN, a Lastro assegura-se um procedimento efetivo para a aderência às regras previstas na regulamentação, a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Para garantia da integridade e disponibilidade das Informações, dados, e serviços a Lastro, para além das disposições específicas abarcadas nesta Política, contrata os serviços:

RTM para a hospedagem em cloud nos sistemas;

A RTM é a maior provedora de serviços para integração do mercado financeiro brasileiro, oferecendo infraestrutura de telecomunicações e soluções de tecnologia em ambiente de nuvem privada com total segurança e alta taxa de disponibilidade.
Em parceria com a Embratel, fornecemos a estrutura de gerenciamento da RSFN, uma das redes do Sistema de Pagamentos Brasileiro.

Os controles de Segurança da Informação descritos em todo framework de políticas e procedimentos da RTM consistem em um conjunto amplo de medidas de segurança, visando a minimizar os riscos presentes nos ativos de informação.
Todos os controles são baseados em normas e padrões internacionais de segurança (Família ISO 27000 e NIST – National Institute of Standart and Technology) e boas práticas adotadas pelo mercado financeiro.
Os controles atendem aos requisitos determinados por leis e regulamentações nacionais e internacionais, quando aplicáveis.

Equipe especializada que realiza a gestão dos eventos de rede através de softwares específicos, prestando suporte em diversos níveis e monitorando os alertas gerados pelos ativos, roteadores, links e gateways, por exemplo.
O NOC atua de forma proativa, sempre disponível – em atendimento 24x7x365 – com o objetivo de manter o ambiente estável e seguro.

Nossas redes são segmentadas com blocos dedicados e isolados para cada serviço e cliente.

Utilizamos Firewalls em toda infraestrutura segregando os ambientes – desta forma todos os acessos são controlados e monitorados

Análise de vulnerabilidade

Todos os ativos gerenciados pela RTM passam por um processo de análise de vulnerabilidade, com rotinas pré-agendadas em uma ferramenta de scan. Em novos ativos, realizamos o escaneamento antes da entrada na rede com o objetivo de mapear ameaças, por meio de um procedimento de hardening no ativo.

IPS – Intrusion Prevention System

Utilizamos nos perímetros de nossa rede dispositivos de IPS dedicados. Através deles podemos identificar e bloquear ameaças minimizando os riscos de intrusão.

Gestão de acessos

Utilizamos uma ferramenta de PAM (Privileged Access Management) para gerenciar nossos servidores, garantindo que somente analistas autorizados realizem o acesso. Para servidores críticos, os acessos passam por workflow e dupla aprovação.

Anti-malware

Todos os nossos servidores e workstations possuem anti-malware instalados e são gerenciados de forma centralizada. Os dispositivos são controlados por políticas de DLP, que bloqueiam porta USB e outros recursos conforme definido em nossa política de segurança interna.

- Grade de sistemas, hospedados na RTM:
  - JDCCS JUD
  - JDBACEN
  - VIRTUAL – RENDA FIXA
  - VIRTUAL – V-CASH
  - CORRETOR, CHANGEWEB – EXCHANGE
  - Advice – Eguardian
  - Advice - Suity

- Realização de BackUps do File Server e demais sistemas; seguindo as seguintes diretrizes:
  - BackUp Incremental realizado de segunda a quinta feira, com cópia diária com funcionalidade de retenção por até 07 dias.
  - BackUp semanal na sexta-feira com cópia semanal com retenção de 27 dias.
  - BackUp Mensal com retenção de 365 dias.
  - BackUp anual com retenção do último ano com retenção de 5 anos.
  - Os arquivos de backup e a documentação dos sistemas devem ser armazenados em lugar diferente ao do escritório, seguro, e de acesso facilitado, somente aos colaboradores autorizados.;
  - Verificar a integridade da informação armazenada;
  - Avaliar a funcionalidade dos procedimentos;
  - Identificar procedimentos desatualizados ou ineficazes;
  - Identificar falhas ou defeitos.
  - Monitoramento das evidências dos backups pelo Gestor de T.I., o qual recepciona e arquiva em diretório especifico os relatórios evidenciando os bakups realizados.

- Geração e Manejo de senhas de acesso da rede, sendo que tal serviço obedece aos seguintes parâmetros:
  - Renovação Mensal das senhas de todos os Membros;
  - As senhas obedecem a padrões alto de complexidade e nível de segurança;
  - Os eventos de login e alteração de senhas são auditáveis e rastreáveis, através do suporte da RTM.

Para a proteção e prevenção de ameaças a Lastro conta com os seguintes mecanismos: filtros de pacotes e firewalls nas redes de Internet da Lastro, sob o controle da RTM, e firewalls e filtro de pacotes nas instalações da RTM; software de proteção contra malware, instalados nos computadores da Lastro sob controle do Gestor de T.I.; e nos servidores, contratados da RTM, no pacote “Serviços de Terceiros”, também são implementados *software* de proteção contra malware.

O Gestor de Tecnologia deverá realizar periodicamente o teste para monitoração dos serviços prestados pela PADCN:

- Solicitar a restauração de um backup do sistema legado de produção e restaurar em base de homologação para evidenciar a efetivação do serviço
- Solicitar a restauração de um diretório ou arquivo do File Server e evidenciar

- Monitorar a qualidade do serviço prestado e se esta em acordo com o contrato firmado.

Compete ao Gestor de Tecnologia, sempre com a aprovação do Diretor de *Compliance*, assegurar a manutenção de nível adequado de segurança de hardware. O que se cumpre com a observância dos seguintes elementos:

a. Os equipamentos devem ser instalados em locais adequados, protegidos de raios solares, altas temperaturas e de incidência de poeira;

b. Devem ser instalados estabilizadores, devidamente dimensionados, para garantir a uniformidade da tensão na rede em casos de picos de energia, e, o salvamento de dados e o desligamento adequado dos equipamentos quando da ocorrência de falhas na rede elétrica.

c. Devem ser instalados no-breaks nos links de Internet e dispositivos de conexão do datacenter;

d. O acesso aos espaços em que estejam localizados servidores seja restrito às pessoas autorizadas com nível de acesso.

Aplicações que contratam hospedagem em nuvem, para utilização de sua plataforma:

A Lastro contrata empresas que no caso da execução do sistema por meio da internet, assegura que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades, e deve ser hospedados em um ambiente seguro que usa um firewall, e outras tecnologias para evitar a interferência ou acesso de intrusos. O data center deverá atender a qualidade assegurada por um sistema de gestão de certificado, prezando continuamente pela segurança e qualidade de seus serviços. O mesmo deve sofrer avaliações periódicas para garantir a conformidade com os padrões de segurança da indústria de data center, inclusive atendendo a resolução 4.658 de 2018 :

O acesso às bases de produção é restrito a um número limitado de pontos e as bases de produção não compartilham uma senha mestre.

Os colaboradores da empresa contratada não podem ter acesso direto ao ambiente de produção, exceto quando necessário para manutenção do sistema, monitoramento e backups.

O sistema deve atuar em plantão 24x7, 365 dias por ano, no monitoramento e tratamento de eventos relacionados a potenciais tentativas de quebra de segurança, anti-malware e Ddos.

Os dados são armazenados em tempo de operação em cluster de banco de dados, tendo backup incremental diário e backup absoluto semanal.

5. Responsabilidades

Todo usuário deve, obrigatoriamente, notificar de forma imediata ao superior direto ou ao Diretor de *Compliance*, casos de suspeita ou de violação das regras e falhas na segurança da informação.

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob esta identificação. Os colaboradores, assemelhados, parceiros de negócio, consultores, prestadores de serviço e fornecedores que necessitem fazer uso desses recursos, devem ter uma identificação única, com prazo e restrição de acesso limitado à execução da sua atividade. O usuário de recurso portátil obriga-se à assinatura de termo de custódia que determina os direitos e deveres quanto à utilização, posse e guarda do recurso e das informações nele armazenadas.

Todos os usuários são responsáveis pela segurança da informação, devendo conhecer os controles estabelecidos sob sua responsabilidade, agindo em conformidade com a PSI estabelecida. Todos os colaboradores devem ser devidamente orientados sobre a PSI da Lastro. Os usuários devem estar devidamente capacitados quanto à correta e eficiente utilização dos recursos oferecidos pela organização necessários ao desempenho de suas funções, respeitando as recomendações para utilização e de acordo com as normas de segurança.

As decisões de âmbito corporativo sobre segurança da informação devem ser comunicadas e compartilhadas junto com os titulares das áreas para sua divulgação, devendo esta participação ser garantida e registrada.

Manutenção de regra de privacidade, estabelecendo mecanismos de controle e responsabilidade de acesso e utilização às informações pertencentes à Lastro, por parte de pessoas jurídicas e pessoas físicas.

6. Penalidades

A Lastro se reserva no direito de:

- Os recursos corporativos são para fins exclusivos do negócio da Lastro, podendo sua utilização ser monitorada e auditada obedecendo aos princípios éticos e ao interesse da segurança, a fim de garantir esta finalidade.

- Comunicação de descumprimento: Será encaminhado ao usuário, por escrito um comunicado informando o descumprimento das regras aqui estabelecidas, com a indicação precisa da violação praticada. Cópia deste comunicado permanecera arquivada junto ao departamento de recursos humanos na respectiva pasta do usuário;
- Advertência ou suspensão: A pena de advertência ou suspensão será aplicada por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na pratica de infrações de menor gravidade;
- Demissão por justa causa: Nas hipóteses prevista no artigo 482 da Consolidação das Leis do Trabalho, alienas “a” à “f”. Fica estabelecido que não a progressividade como requisito para a configuração da dispensa por justa causa, podendo a diretoria, no uso de seus poderes de direção e disciplina que lhe é atribuído, aplicar a pena que entender devida quando praticada a falta grave.

7. DISPOSIÇÕES FINAIS

Conformidade

A utilização das informações delegadas aos usuários se destina exclusivamente a atingir os objetivos da Lastro, sendo vedado qualquer tipo de divulgação fora dos conceitos desta PSI. Ao usuário não é dado o direito de desconhecimento das normas de Segurança da Informação da Lastro, devendo cumprir rigorosamente o disposto nos documentos normativos.

A inobservância das Diretrizes, Políticas e Normas de Segurança da Informação sujeita o infrator às sanções previstas no processo disciplinar e às medidas legais cabíveis.

ANEXO I

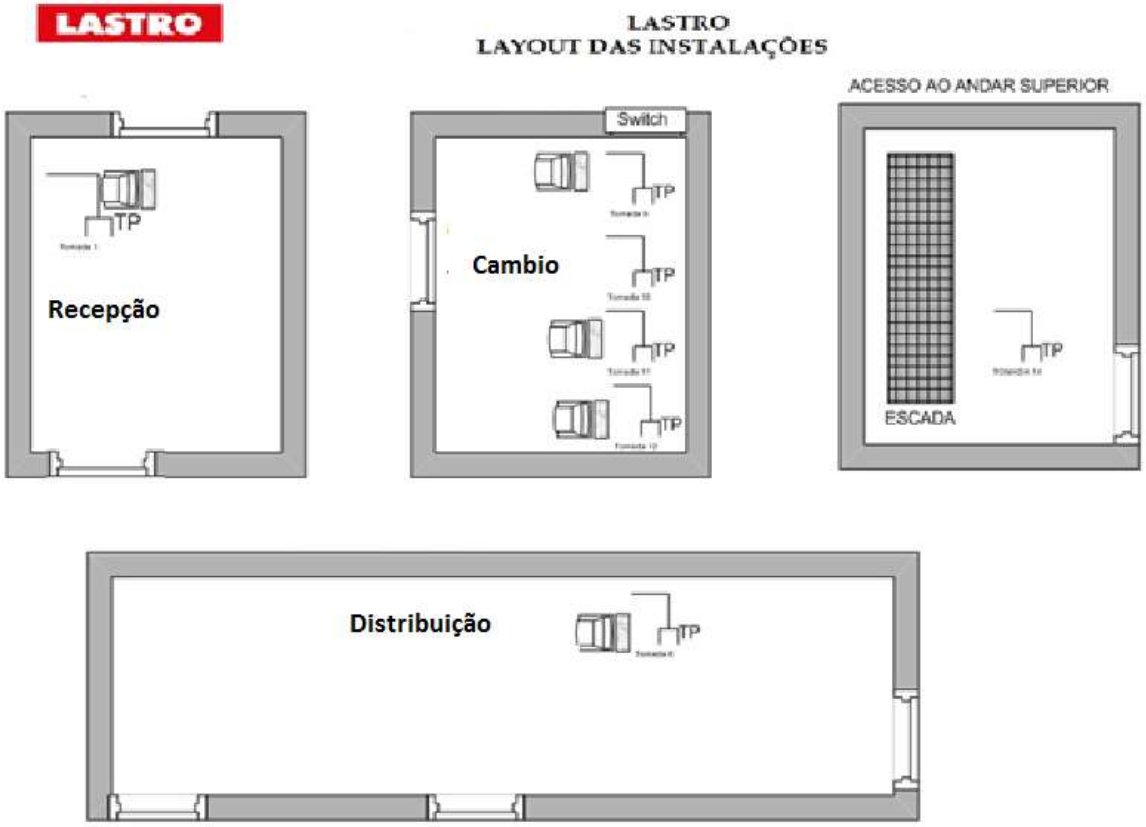
Termo de Ciência.

Eu,_____, portador do RG no. _____, declaro que recebi e li o documento "POLÍTICA E NORMAS DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA" bem como os seus documentos complementares por ela citados, me comprometo a segui-la, e desde já estou ciente das punições que podem ocorrer pelo não cumprimento das regras aqui estabelecidas.

Lastro DTVM Ltda

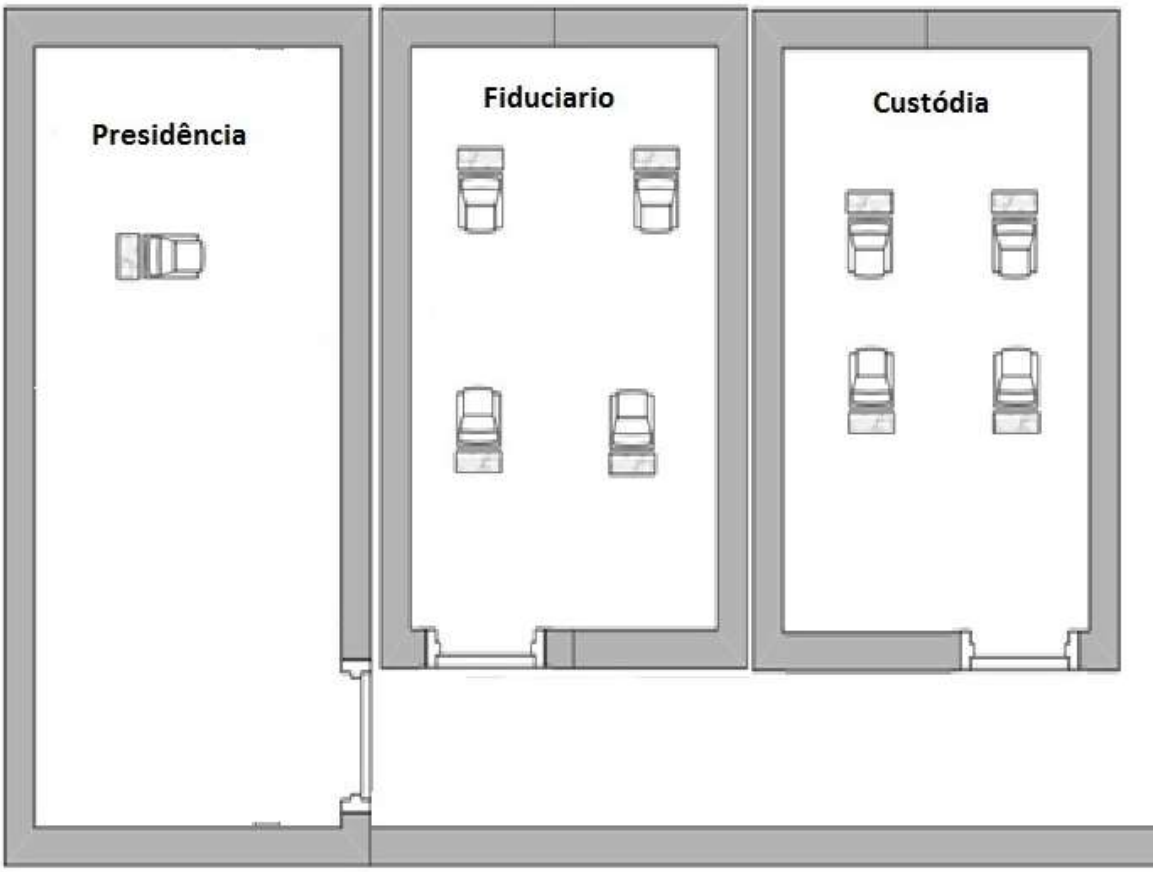
Recebi: _____ Data ___/___/____
(Assinatura do colaborador)

Anexo II
Layout das Instalações da Matriz



LASTRO

LASTRO
LAYOUT DAS INSTALAÇÕES



LASTRO

LASTRO
LAYOUT DAS INSTALAÇÕES