LIQ	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
	Classificação da Informação: Restrita	Vigente a partir de: 26/07/2017

1. OBJETIVO

Estabelecer diretrizes de Segurança da Informação de modo a sustentar os pilares de confidencialidade, disponibilidade e integridade das informações, pautadas nos requisitos do negócio, nos riscos envolvidos, na legislação e regulamentação vigente.

2. ABRANGÊNCIA

É destinado a todos os colaboradores da Liq e suas controladas, fornecedores e/ou clientes, que possuam acesso às informações e/ ou ambientes da Liq e suas controladas.

3. REGRAS

3.1 OBJETIVO

A informação, independentemente de sua natureza ou de sua origem, é um ativo valioso de extrema importância para a Liq e suas controladas, sendo um elemento fundamental para o sucesso dos seus negócios, merecendo, portanto, proteção adequada.

Segurança da Informação consiste na adoção de medidas para proteção das informações existentes no Plano Diretor de Segurança da Informação_v1.0, em qualquer forma e suporte que se apresente – física ou digital - das diversas ameaças existentes, a fim de evitar seu uso indevido, inadequado, ilegal ou em desconformidade com as políticas e procedimentos internos.

3.2 PRINCÍPIOS

A segurança da informação é caracterizada pela preservação dos seguintes princípios:

- Propriedade da Informação: a informação da Liq e suas controladas é de propriedade da Companhia e deve ser utilizada exclusivamente para o atendimento dos objetivos do negócio, sendo proibida a sua utilização para fins particulares ou que viole direitos da Companhia e/ou de terceiros;
- Confidencialidade: a informação deve ser conhecida somente por pessoas autorizadas, que precisem conhecê-la para o desenvolvimento de suas atividades profissionais, exclusivamente para o atendimento dos objetivos do negócio;
- Integridade: a informação deve ser armazenada de forma a garantir a exatidão e completude de seu conteúdo.
- Disponibilidade: a informação deve estar disponível para o acesso de pessoas autorizadas, quando necessário.

3.3 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é parte integrante do Sistema de Gestão de Segurança da Informação, em cumprimento à norma ISO 27001, em concordância com a Política do Sistema de Gestão de Segurança da Informação.

3.4 TREINAMENTO

Antes de assumir qualquer função na Liq e suas controladas, todo colaborador deve receber treinamento em Segurança da Informação, bem como treinamentos adequados para a realização das suas atividades, objetivando minimizar o risco de falhas em procedimentos operacionais.

Os treinamentos em Segurança da Informação devem ser aplicados periodicamente a todos os colaboradores, de modo a garantir a reciclagem em relação ao tema, não ultrapassando o período máximo de 12 meses.

Campanhas de conscientização devem ser aplicadas a cada 6 meses, com abrangência corporativa.

3.5 AVALIAÇÃO DE CONFORMIDADE

Avaliações internas de aderência à Política de Segurança da Informação devem ser realizadas, periodicamente, dentro de um prazo máximo de 12 meses.

3.6 VULNERABILIDADE E RISCOS

Os sistemas, processos, serviços e terceiros devem ser avaliados de forma periódica com o objetivo de identificar riscos, falhas, vulnerabilidades e descumprimentos das medidas de segurança da informação.

3.7 MONITORAMENTO

Os equipamentos, meios de comunicação e sistemas da Companhia devem estar sujeitos ao monitoramento, devendo o colaborador ser formalmente cientificado da inexistência de privacidade.

O monitoramento deve ser realizado de acordo com os parâmetros legais e regulamentares e não deve constituir qualquer violação à intimidade, vida privada, honra ou imagem do colaborador monitorado.

3.8 DEVER DE SIGILO

a. Colaborador Liq e de suas controladas

No momento de assinatura do Contrato de Trabalho, deve assinar o Termo de Confidencialidade e Adesão à Política de Segurança da Informação. O termo assinado pelo colaborador deve ser armazenado por 2 anos a contar do encerramento do vínculo empregatício.

b. Fornecedor

Deve se comprometer a agir de acordo com a Política de Segurança da Informação, sendo imprescindível que o contrato firmado entre as empresas possua cláusula que assegure a confidencialidade das informações e a adesão à Política de Segurança da Informação.

c. *NDA* (*Non-Disclosure Agreement* / Acordo de Confidencialidade)

- Todos os Para terceiros, incluindo-se neste conceito os fornecedores, parceiros, e clientes, deverão firmar *NDA* para que seja liberado qualquer acesso ao ambiente tecnológico Liq, sendo que a apresentação do NDA devidamente assinado à equipe de Segurança da Informação consiste em condição para a liberação de acesso;
- Terceiros com contrato firmado com clientes, fornecedores ou parceiros da Liq e suas controladas, deverão firmar *NDA* tripartite antes que liberado qualquer acesso ao ambiente tecnológico Liq, sendo que a apresentação do NDA tripartite devidamente assinado à equipe de Segurança da Informação consiste em condição para a liberação de acesso.
- O NDA deverá seguir o modelo padrão Liq, validado por seu Departamento Jurídico. Alterações no NDA padrão somente poderão ser formalizadas mediante prévia aprovação dos departamentos de Segurança da Informação e Jurídico da Liq.

3.9 RESCISÃO DO CONTRATO DE TRABALHO DO COLABORADOR

É de responsabilidade da área de Recursos Humanos rescindir o contrato de trabalho do colaborador ou oficializar a mudança de área do empregado.

Em caso de desligamento a área de Recursos Humanos deverá recolher todos os ativos da Liq e suas controladas que estejam sob a posse do colaborador.

3.10 DEFINIÇÃO DA INFORMAÇÃO

Conjunto organizado de dados que constitui uma mensagem sobre um acontecimento, fato, objeto ou fenômeno, que em seu contexto possui um determinado significado. Ex.: Comunicado corporativo.

A informação pode existir em diversos formatos tais como: impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio eletrônico e/ou por outros meios eletrônicos, mostrada em filmes ou falada em conversas.

Independentemente da forma apresentada ou do meio pelo qual a informação é compartilhada ou armazenada, ela deve estar protegida de acordo com sua relevância em relação ao negócio da Liq e suas controladas.

3.11 CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação deve ser classificada no ato da sua criação ou aquisição, em conformidade com as normas legais e contratuais aplicáveis, considerando as exigências de negócio da Liq e suas controladas, o valor da informação e os possíveis impactos causados por sua divulgação indevida.

Apenas o responsável pela classificação ou seus superiores podem alterar o grau de sigilo atribuído às informações.

Os ativos assumem automaticamente a classificação de maior nível de segurança atribuída a uma informação suportada por eles, sendo que, todo ativo deve ter um proprietário definido.

As informações devem ser protegidas contra perda, destruição, falsificação e vazamento de informação de acordo com sua classificação, conforme o procedimento "*Segurança no manuseio de dados*".

É fundamental que todos os profissionais da Liq, fornecedores e/ou clientes, tenham conhecimento e sigam as regras explanadas no anexo "*Classificação da Informação*" complementar da Política de Segurança da Informação.

3.12 PAPÉIS E RESPONSABILIDADES

Cabe a todos os colaboradores, fornecedores e clientes cumprirem as seguintes obrigações, de acordo com o seu perfil:

Papéis	Perfil Associado	Responsabilidades
Colaboradores, Fornecedores e Clientes	Colaborador Liq, Fornecedores e Clientes	• Cumprir as orientações do nível de sigilo adequado às informações disponíveis, conforme explicitado no anexo "*Classificação da Informação*" complementar à Política de Segurança da Informação; • Envolver Segurança da Informação nos projetos de natureza corporativa, tecnológica e de negócio; • Zelar pela segurança das informações da Liq e suas controladas, informando quaisquer anormalidades percebidas ao superior imediato, ao Canal Direto ou à Segurança da Informação; • Devolver todos os ativos da Liq e suas controladas que estejam em sua posse após o encerramento do contrato, conforme explicitado no anexo "*Segurança em Ativos*" complementar à Política de Segurança da Informação.
Gestores	Supervisor, Coordenador, Gerente, Diretor, Diretor Executivo	• Classificar as informações, definir os direitos de acesso e os critérios de geração da informação sob sua responsabilidade, bem como garantir a exatidão das informações, conforme explicitado no anexo "*Classificação da Informação*", "*Controle Seguro de Acesso Lógico*" e "*Controle Seguro de Acesso Físico*" complementar à Política de Segurança da Informação; • Garantir que todos os procedimentos de segurança dentro da área de sua responsabilidade sejam executados corretamente, em conformidade com à Política de Segurança da Informação; • Envolver Segurança da Informação nos projetos de natureza corporativa, tecnológica e de negócio; • Atuar sobre as inconformidades sob sua responsabilidade, identificadas e notificadas pela Segurança da Informação; • Garantir que todos os colaboradores sob sua gestão possuam o conhecimento adequado da Política de Segurança da Informação e exerçam suas respectivas atividades de trabalho de acordo com estas regras.
Segurança da Informação	Área Segurança da Informação e terceiros sob sua gestão.	• Elaborar a Política de Segurança da Informação, bem como os anexos necessários para a adequação do ambiente ao nível de Segurança pertinente ao bom desenvolvimento do negócio da Liq e suas controladas, identificando e confirmando continuamente se as exigências de leis, regulamentos e contratos locais e internacionais se encontram publicadas nos documentos da Política de Segurança da Informação; • Buscar as metodologias e processos específicos para a Segurança da Informação, tais como avaliação de risco e sistemas de classificação de segurança; • Buscar e apoiar iniciativas de Segurança da Informação aplicáveis a toda a organização, como por exemplo, o programa de conscientização de segurança; • Fomentar que a segurança seja parte do processo de planejamento da informação; • Analisar e emitir parecer consultivo dos projetos corporativos, tecnológicos e de negócio; • Apoiar a implantação de controles específicos de Segurança da Informação para novos sistemas ou serviços;

		• Analisar criticamente e propor regulamentação interna sobre as formas de tratamento de incidentes de segurança ocasionados por colaboradores e terceiros; • Manter contatos apropriados com autoridades relevantes, grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais; • Identificar e reportar os riscos referentes à segurança das informações à gestão da Liq e suas controladas; • Implantar e executar melhoria contínua no Sistema de Gestão da Segurança da Informação (SGSI).
CSIRT	Grupo de Resposta a Incidentes de Segurança da Informação	• Coordenar as ações de mitigação dos impactos decorrentes dos incidentes de segurança; • Coordenar o uso de recursos no tratamento e resposta contra os incidentes de segurança; • Propor melhorias processuais e tecnológicas e com o objetivo de evitar a reincidência de incidentes; • Divulgar alertas de segurança e vulnerabilidades recebidos; • Fornecer apoio técnico para tratamento preventivo e/ou corretivo.
Comitê de Segurança da Informação	Comitê de Segurança da Informação	• Disseminar a cultura de Segurança de Informação; • Alinhar os objetivos estratégicos de Segurança da Informação com os objetivos de negócio da Liq e suas controladas; • Avaliar a Política de Segurança da Informação e seus anexos e submeter a aprovação do COMEX, bem como definir o plano de ação para sua aplicação; • Definir controles e ferramentas para a gestão da Segurança da Informação; • Dirimir dúvidas e deliberar sobre questões não contempladas pela política de Segurança da Informação ou outros ou pelos documentos normativos a ela relacionados, bem como sugerir as alterações necessárias; • Aprovar a elaboração e alterações de procedimentos para a Continuidade de Segurança da Informação; • Apoiar e aprovar atividades de melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI).
Comitê Executivo COMEX	Alta administração	• Assegurar que a Política e os objetivos de Segurança da Informação estão estabelecidos e compatíveis com a direção estratégica da Liq e suas controladas; • Aprovar a Política de Segurança da Informação e seus anexos; • Aprovar o tratamento do risco, quanto à exposição dos ativos das informações da Liq e suas controladas e de nossos clientes às principais ameaças; • Aprovar as principais iniciativas e investimentos para aumentar o nível de Segurança da Informação na Liq; • Propor e validar avaliações de conformidade no ambiente da Liq, no intuito de aferir o nível de segurança dos respectivos sistemas de informação; • Apoiar a disseminação da cultura de Segurança da Informação na Liq; • Comprometer-se com a melhoria contínua e analisar criticamente o Sistema de Gestão da Segurança da Informação (SGSI) da Liq e suas controladas a intervalos planejados, para assegurar a sua contínua adequação, pertinência e eficácia.

3.13 CANAL DE ATENDIMENTO

Ações que violam o sistema de gestão de segurança da informação sendo incidentes de segurança de informação poderão ser feitas por meio do e-mail ***csirt@liq.com.br***.

3.14 DISPOSIÇÕES FINAIS

Qualquer necessidade de ação em desacordo com as regras estabelecidas na Política de Segurança da Informação e seus anexos deve ser direcionada à Segurança da Informação para análise do risco, seu registro, e envio para a apreciação pela alçada competente e/ou Comitê de Segurança da Informação.

O colaborador que fizer uso indevido ou não autorizado dos recursos da Liq e suas controladas, violar controle de segurança, ou de qualquer modo agir em desacordo com os termos dessa política, fica sujeito à aplicação de medidas disciplinares legalmente previstas, podendo haver responsabilização penal, civil e/ou administrativa, na

forma da legislação em vigor.

É responsabilidade da Segurança da Informação a análise e apuração das denúncias de violação à Política de Segurança da Informação, devendo recomendar o plano de ação de melhorias e apoiar os gestores na aplicação de medidas disciplinares definidas pelo Comitê de Ética e Conduta.

A Segurança da Informação deve divulgar este documento, visando garantir a sua eficácia.

4. ANEXOS

I. Classificação da Informação
Anexo que estabelece regras que garantam que todas as informações, independente de seus meios de armazenamento ou transmissão, recebam níveis adequados de sigilo

II. Ambiente Seguro de Trabalho
Anexo que estabelece regras e controles para que os recursos disponibilizados pela Liq e suas controladas aos colaboradores sejam utilizados de forma segura.

III. Segurança em Ativos
Anexo que assegura que todos os ativos de tecnologia sejam controlados durante todo o ciclo de vida até seu descarte.

IV. Controle Seguro de Acesso Lógico
Anexo que estabelece regras e controles que previnem o acesso não autorizado do colaborador aos sistemas de informações, concedendo apenas o acesso aos sistemas que tenha sido especificamente autorizado a usar.

V. Controle Seguro de Acesso Físico
Anexo que estabelece regras e controles físicos que restringem o acesso não autorizados nos ambientes da Liq e suas controladas.

VI. Ambiente Seguro de TI
Anexo que estabelece regras e requisitos mínimos de segurança para o correto funcionamento do processamento de informações no ambiente tecnológico da Liq e suas controladas.

VII. Ambiente Seguro de Rede
Anexo que estabelece a forma segura, como as redes de comunicações devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações da Liq e suas controladas e de seus Clientes.

VIII. Aquisição e Desenvolvimento Seguro de Aplicações
Anexo que estabelece requisitos para o processo de aquisição e desenvolvimento de aplicações no ambiente da Liq e suas controladas.

IX. Gestão de Incidentes de Segurança da Informação
Anexo que estabelece regras de gerenciamento dos incidentes de segurança da informação.

X. Continuidade de Segurança da Informação
Anexo que estabelece regras para aplicação da continuidade de segurança da informação nos ambientes da Liq e suas controladas

XI. Termo de Confidencialidade e Adesão à Política de Segurança da Informação – PF[1]
Documento pelo qual o contratado Pessoa Física, se compromete a conhecer a Política de Segurança da Informação e cumpri-la.

XII. Termo de Adesão à Política de Segurança da Informação – PJ[2]
Documento pelo qual o contratado Pessoa Jurídica, se compromete a conhecer a Política de Segurança da Informação e cumpri-la.

5. GLOSSÁRIO

[1] PF – Pessoa Física

[2] PJ – Pessoa Jurídica

6. FICHA TÉCNICA

Nome da POL: Política de Segurança da Informação.
Código da POL: 40.2.1
Número e data da versão: 10| 26/07/2017.
ARD: Segurança da Informação.
Referências: Normas referenciais da família ISO 27000, Lei Nº 9.609 Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
Nome e cargo do colaborador que elaborou a POL: Roberto Toscani – Gerente de Segurança da Informação e Osvaldo Junior – Analista Pleno de Segurança da Informação.
Nome e cargo do colaborador da COP que revisou a POL: Letícia Prebianca – Gerente de *Compliance*.
Nome e cargo do colaborador do JUR que revisou a POL: Camila de Vito -Gerente Jurídico Consultivo e Contratos**.**
Nome dos integrantes do Comitê Executivo que aprovaram a POL: Ana Coelho; Marcelo Chianello; Pedro Miranda; Cristiane Barreto; Cristiane Cé e João Mendes.
Data de aprovação da POL: 20/06/2017.
Data de publicação da POL: 26/07/2017.
Data de divulgação da POL: 26/07/2017.
Vigência a partir de: 26/07/2017.
Prazo para a revisão da POL: 25/07/2019.
Classificação informação: Restrita.
Áreas relacionadas com o processo disciplinado: Todas as áreas da Liq e suas controladas.
Processo: Segurança da Informação.
Risco Associado: Não cumprimento da Política de Segurança da Informação.

Histórico das Versões

Versão	Data	Alterações
08	05/09/2016	Definição de novas regras.
09	02/03/2017	Adicionado o Item 3.1 Sistema De Gestão De Segurança Da Informação
09	02/03/2017	Removido o Item 3.2 Adesão À Política De Segurança Da Informação
09	02/03/2017	Adicionado o Item 3.3 Dever de Sigilo
09	02/03/2017	Alteração no item 3.7 Papéis e Responsabilidades, definição de novas regras.
09	02/03/2017	Alteração no item 3.7 Canal de Atendimento.
09	02/03/2017	Alteração no item 4. Anexos, mudança do nome do anexo X.
09	02/03/2017	Substituído o termo “Prestadores de Serviço” para Fornecedores.
10	03/05/2017	Alteração do item 1. Objetivo
10	03/05/2017	Adicionado o item 3.1 Objetivo
10	03/05/2017	Adicionado o item 3.2 Princípios
10	03/05/2017	Adicionado o item 3.5 Avaliação de Conformidade
10	03/05/2017	Adicionado o item 3.6 Vulnerabilidade e Risco
10	03/05/2017	Adicionado o item 3.7 Monitoramento
10	03/05/2017	Alteração no item 3.7 Papéis e Responsabilidades, inclusão da equipe de CSIRT
10	03/05/2017	Alteração do item 3.14 Disposições Finais