TR BLOCK SECURITIZADORA S.A. e LIQI DIGITAL ASSETS S.A.

("Grupo Liqi")

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

("Política")

NOVEMBRO/2024

Elaboração: Compliance
Aprovação: Diretora de Compliance e PLD-FTP
Versão: 3.0

Código: P.00010
Vigente Desde: Junho/2022
Última Versão: Novembro/2024

TR BLOCK

liqi

ÍNDICE

1. OBJETIVO

A presente Política tem como objetivo estabelecer as diretrizes e responsabilidades gerais relacionadas ao processo de gestão de informação e segurança no ambiente de tecnologia da informação da **LIQI DIGITAL ASSETS S.A.** ("Liqi") e da **TR BLOCK SECURITIZADORA S.A.** ("Securitizadora" e em conjunto com a Liqi, "Grupo Liqi"), com vista a atender às exigências da Resolução da Comissão de Valores Mobiliários ("CVM") nº 60, de 23 de dezembro de 2021 ("Resolução CVM nº 60") e demais disposições legais e infralegais aplicáveis.

As medidas de segurança da informação têm por objetivo minimizar as ameaças aos negócios do Grupo Liqi e às disposições desta Política, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais (conforme abaixo definido).

As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador (conforme abaixo definido) responsável por seu computador. As regras e procedimentos dispostas nesta Política são efetivos e consistentes e levam consideração o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pelo Grupo Liqi.

2. INTERPRETAÇÃO

Para fins de interpretação da presente Política, deverão ser consideradas as definições descritas ao final deste documento. As expressões possuirão o mesmo significado quando utilizadas no singular ou no plural.

Estão vinculados a essa Política os seguintes documentos: (i) Política de Cookies e Proteção de Dados; (ii) Política de Resposta a Incidentes de Segurança; (iii) Política de Uso do Patrimônio Tecnológico da Liqi; e (iv) Política de Consequências.

Ademais, são consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins desta Política, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre o Grupo Liqi, sobre as empresas pertencentes ao seu conglomerado, conforme aplicável, seus sócios, Investidores e parceiros comerciais, incluindo:

(i) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) Informações técnicas, financeiras, estratégicas ou comerciais;

(iii) Operações estruturadas, demais operações e seus respectivos valores, independentemente de terem sido apenas analisadas ou efetivamente realizadas;

(iv) Estruturas, planos de ação, relação de Investidores, contrapartes comerciais, fornecedores e prestadores de serviços;

(v) Informações estratégicas, mercadológicas ou de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários do Grupo Liqi ou, ainda, junto a seus representantes, consultores, assessores, Investidores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação do Grupo Liqi e que ainda não foi devidamente levado à público;

(vi) Informações a respeito de resultados financeiros das empresas emissoras ou adquirentes de direitos creditórios que sejam lastro para a emissão de títulos securitizados antes da publicação dos respectivos balanços, balancetes e/ou demonstrações financeiras, se aplicável;

(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

(viii) Outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários ou jovens aprendizes do Grupo Liqi ou, ainda, junto a seus representantes, consultores, assessores, Investidores, fornecedores e prestadores de serviços em geral.

3. APLICABILIDADE

Esta Política é aplicável a todos os administradores (incluindo diretores executivos), membros do Conselho de Administração e membros dos Comitês e/ou Comissões de Assessoramento ao Conselho de Administração, sócios, colaboradores, estagiários, bem como a qualquer pessoa que possua cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança no Grupo Liqi (“Colaboradores).

Esta Política abrange todos os recursos computacionais e de informações disponíveis nos ambientes, sistemas, computadores, servidores, smartphones, tablets e redes do Grupo Liqi e aplica-se a todos Colaboradores que tiverem acesso aos equipamentos e sistemas utilizados pelo Grupo Liqi.

4. RESPONSABILIDADE E OBRIGAÇÕES

A coordenação direta das atividades relacionadas a esta Política é uma responsabilidade da área sob coordenação da responsável pelo cumprimento das regras, procedimentos e controles internos ("Área de Compliance e PLD-FTP" e "Diretora de Compliance e PLD-FTP"), que, em conjunto com a Área de Segurança da Informação e de Tecnologia ("Área de SI"), serão responsáveis por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito. A Área de SI, por sua vez, é coordenada pelo *Chief Technology Officer* ("CTO").

Nesse contexto, serão responsabilidades da Área de Compliance e da Área de SI, sob coordenação da Diretora de Compliance e PLD-FTP e do CTO:

(i) Coordenar os esforços relacionados à proteção de dados pessoais;
(ii) Propor e revisar documentos principais de segurança da informação, incluindo políticas de segurança, classificação, controle de acesso, uso aceitável de ativos, e metodologias de análise e tratamento de risco;
(iii) Coordenar a análise/avaliação de riscos e propor medidas para mitigá-los.
(iv) Preparar e realizar treinamentos e campanhas de conscientização sobre segurança da informação;
(v) Comunicar os benefícios da segurança da informação e propor objetivos de segurança;
(vi) Reportar resultados de auditorias e propor melhorias de segurança;
(vii) Definir cláusulas de segurança para acordos de terceirização;
(viii) Coordenar a resposta a incidentes de segurança e preparar evidências para ações legais decorrentes de incidentes;
(ix) Estabelecer métodos de proteção para dispositivos móveis e redes de computadores;
(x) Definir princípios para o desenvolvimento seguro de sistemas de informação;
(xi) Monitorar *logs* de atividades de usuários para identificar comportamentos suspeitos;
(xii) Assegurar que os recursos tecnológicos sejam utilizados de forma segura e eficiente;
(xiii) Implementar e manter sistemas de segurança, incluindo antivírus, backups e controle de acesso

Os Colaboradores têm a obrigação de proteger a segurança e a integridade das informações e equipamentos de informática, sendo proibido o uso de dados do Grupo

Liqi ou de clientes e de outros parceiros comerciais para propósitos incoerentes com as necessidades do negócio ou para fins que possam violar o disposto nesta Política e demais disposições legais e infralegais aplicáveis.

Nesse sentido, todos os Colaboradores que tiverem acesso aos sistemas e equipamentos utilizados pelo Grupo Liqi comprometem-se a:

(i) Não transmitir quaisquer dados, incluindo dados pessoais, ou informações da Liqi que está em sua posse, ou ainda, que tenha a habilidade de acessar, para terceiros não autorizados, seja de maneira verbal, escrita, impressa ou digital;

(ii) Utilizar somente softwares originais e devidamente licenciados, bem como dispositivos e meios de comunicação previamente autorizados e recomendados pelo Grupo Liqi;

(iii) Não usar dados ou dados pessoais ou informações do Grupo Liqi ou quaisquer de seus recursos e equipamentos para fins pessoais ou diversos daqueles necessários ao desempenho da função contratada;

(iv) Zelar pela segurança de seu login e senha (ID) de acesso individual aos ambientes de sistemas da Liqi, ficando proibido usar como próprio o ID de terceiro ou ceder o seu a outrem;

(v) Observar e cumprir com o disposto nesta Política e demais políticas relacionadas do Grupo Liqi;

(vi) Zelar por todo e qualquer dado, dado pessoal e informação armazenada na rede corporativa contra alteração, destruição, transmissão, divulgação, cópia e acessos não autorizados;

(vii) Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;

(viii) Respeitar a propriedade intelectual do Grupo Liqi e/ou de terceiros, sendo proibido, sem se limitar, copiar, modificar, usar ou divulgar em todo ou em parte, textos, artigos, programas ou qualquer outro material ou mídia protegida, sem a permissão expressa, por escrito, do detentor de tais direitos;

(ix) Zelar pelos equipamentos que utiliza, não sendo permitido qualquer, remoção, desconexão de partes, substituição ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;

(x) Utilizar computadores, sistemas de telefonia, redes e outros serviços de informática (como sistema ERP) apenas e exclusivamente para fins profissionais, ficando vedado sua utilização para fins particulares ou para beneficiar outras empresas que não tenham relação com o Grupo Liqi, salvo se autorizado por escrito pela empresa;

(xi) Não tomar atitude ou ação que possa direta ou indiretamente indisponibilizar os recursos da rede;

(xii) Não executar programas que tenham como finalidade a decodificação de senhas, a monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços;

(xiii) Não executar programas, instalar equipamentos ou executar ações que possam facilitar o acesso à rede de usuários não autorizados;

(xiv) Utilizar quaisquer recursos, sejam eles microcomputadores, impressoras, ou outros equipamentos não autorizados pelo Grupo LIQI;

(xv) Não utilizar os recursos do Grupo Liqi para fazer download ou distribuição de software ou dados "piratas" (sem licença/autorização de uso);

(xvi) Não utilizar os recursos do Grupo Liqi para deliberadamente propagar qualquer tipo de vírus, *worms*, cavalos de tróia, *malwares* ou programas de controle de outros computadores;

(xvii) Não realizar cópia de arquivos para quaisquer tipos de mídia (pen-drives, CD´s, DVD´s etc.), salvo se autorizado pelo Grupo Liqi, por meio da área de Infraestrutura;

(xviii) Não efetuar qualquer tipo de acesso ou alteração não autorizada a dados, dados pessoais e informações dos recursos computacionais pertencentes ao Grupo Liqi;

(xix) Não violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;

(xx) Não fazer o uso de qualquer tipo de software de acesso remoto, salvo quando expressamente autorizado pelo Grupo Liqi ou na prestação de suporte à distância, sendo terminantemente proibido aos usuários fazer o uso de qualquer solução nesse sentido;

(xxi) Informar prontamente ao superior imediato, sem prejuízo da comunicação direta à Área de SI, por meio do da central de suporte (https://liqi.atlassian.net/servicedesk/customer/portals) com a Diretora de Compliance e PLD e o CTO em cópia, sobre a ocorrência ou suspeita de quaisquer falhas, incidentes de segurança ou condutas inadequadas e/ou ilícitas, brechas de segurança ou desvios das regras estabelecidas nesta Política, bem como sobre a ocorrência de qualquer violação à presente Política praticada em atividades relacionadas ao trabalho, dentro ou fora das dependências do Grupo Liqi, para que sejam tomadas as medidas cabíveis.

O Grupo Liqi exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em eventuais processos investigatórios que tenha como origem a inobservância das regras e procedimentos estabelecidos nesta Política, bem como adotar as medidas legais cabíveis.

5. IDENTIFICAÇÃO DE RISCOS (*risck assessment)*

No âmbito de suas atividades, o Grupo Liqi identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de Investidores, parceiros comerciais, Colaboradores e do próprio Grupo Liqi, operações realizadas ou em análise, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
(ii) Sistemas: informações sobre os sistemas utilizados pelo Grupo Liqi e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
(iii) Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio do Grupo Liqi; e
(iv) Contingência e Continuidade dos Negócios: a eficácia dos planos de contingência e de continuidade de negócios do Grupo Liqi.

Ademais, no que se refere especificamente à segurança cibernética, o Grupo Liqi identificou as seguintes principais ameaças:

(i) *Malware*: *softwares* desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
(ii) Engenharia social: métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e Acesso Pessoal);
(iii) Ataques de DDoS (distributed denial of services) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
(iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, o Grupo Liqi avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

6. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Após a identificação dos riscos, o Grupo Liqi adota as medidas a seguir descritas para proteger suas informações e sistemas.

Regra Geral de Conduta:

O Grupo Liqi realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede do Grupo Liqi e

circulem em ambientes externos ao Grupo Liqi com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses do Grupo Liqi. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores do Grupo Liqi deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, a Área de SI, em conjunto com a Equipe de Compliance e PLD-FTP deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico do Grupo Liqi qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno do Grupo Liqi.

O Grupo Liqi não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar *pen-drivers*, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no Grupo Liqi. É proibida a conexão de equipamentos na rede Grupo Liqi que estejam restritos pela área de informática e pelos administradores do Grupo Liqi.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação do Grupo Liqi.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores do Grupo Liqi.

A visualização proposital de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

Acesso Escalonado do Sistema

O acesso como “administrador” de área de desktop é limitado aos usuários aprovados pela Diretora de Compliance e PLD-FTP e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

O Grupo Liqi mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede do Grupo Liqi necessária ao exercício de suas atividades. Assim, os colaboradores deverão ter seus perfis de acesso limitados de acordo com as necessidades exigidas pela sua função, conforme definido pelo gestor imediato.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas do Grupo Liqi em caso de violação.

Senha e Login

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas conforme aviso fornecido pelo responsável pela área de informática.

Ademais, por segurança, as senhas de rede, sistemas e aplicações devem seguir um padrão de segurança considerando os requisitos da política de uso do patrimônio tecnológico da Liqi, como também dos seguintes requisitos:

(i) Expiração de senha a cada 90 (noventa) dias;

(ii) Senhas fortes com no mínimo de 09 caracteres, contendo: números, letras (maiúsculas e minúsculas) e caracteres especiais, não podendo repetir as 03 últimas senhas utilizadas;
(iii) Uso da autenticação multifator para logar na conta de domínio do Grupo Liqi.

Todo colaborador deve ter identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. Os colaboradores assumem a responsabilidade quanto ao sigilo de suas credenciais de acesso. Assim, não devem anotá-los em papéis ou *post its* nem os compartilhar com terceiros, ainda que sejam Colaboradores do Grupo Liqi. O Colaborador poderá ser responsabilizado, caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins, sendo o único responsável pela correta utilização e por eventuais usos inadequados dos direitos de acesso que lhes são atribuídos.

Os acessos aos sistemas de informação, base de dados e demais recursos de tecnologia devem ser concedidos somente pelo Grupo Liqi. Além disso, a concessão de acesso a dados, Dados Pessoais, informações e sistemas deve se basear na necessidade comprovada para o desempenho da função.

O Grupo Liqi poderá a qualquer momento efetuar o bloqueio de acesso de Colaboradores em caso da ocorrência ou suspeita de ocorrência de Incidente de Segurança de qualquer natureza ou violação a essa Política, bem como para a realização de investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do Grupo Liqi.

Cabe à área de Recursos Humanos informar pelo e-mail infra@liqi.com.br, de maneira imediata a contratação, mudança de cargo, função, suspensão ou o desligamento de Colaboradores para que as providências de criação, ajustes no perfil ou cancelamento dos acessos concedidos sejam tomadas.

Instalação de Software

Os computadores serão configurados exclusivamente com softwares licenciados e necessários para a execução das atividades do Grupo Liqi. Qualquer necessidade específica deverá ser previamente solicitada à empresa, pela central de Suporte Liqi, que fará análise da necessidade e acionará a área ou profissional responsável. Em nenhum caso será permitida a utilização de softwares sem as devidas licenças.

É considerada falta grave, instalar no computador qualquer *software* sem autorização e/ou as devidas licenças corporativas, por se tratar de atividade ilegal, assim como os não autorizados, pelos riscos de segurança causados aos sistemas como um todo.

Uso de Equipamentos e Sistemas

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A utilização dos ativos e sistemas do Grupo Liqi, incluindo computadores, internet, *e-mail* e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar à Área de SI e à Área de Compliance e PLD-FTP.

Nesse contexto, é terminantemente proibido ao Colaborador:

(i) Enviar mensagens de correio eletrônico cujo conteúdo seja confidencial a terceiros que não estão autorizados a receber tais mensagens;
(ii) Divulgar informações não autorizadas, como por exemplo, fotos, imagens de tela, dados de sistemas, documentos e afins, sem autorização expressa e formal do Grupo Liqi;
(iii) Divulgar material protegido por ou que contenha qualquer informação protegida por propriedade intelectual sem a permissão do Grupo Liqi ou do detentor dos direitos;
(iv) Enviar e-mails não solicitados (SPAM);
(v) Falsificar qualquer informação da mensagem original que está sendo enviada;
(vi) Abrir ou executar arquivos anexados enviados por remetentes desconhecidos ou suspeitos, com as extensões .bat, .exe, .src, .lnk, .com e .dmg. Em caso de dúvida sobre a legitimidade do e-mail, entre em contato pelo e-mail infra@liqi.com.br antes de qualquer ação;
(vii) Utilizar o e-mail profissional para fins e/ou assuntos pessoais. Por exemplo, os endereços de e-mail do Grupo Liqi não devem ser utilizados em lojas virtuais ou em cadastros de lojas ou promoções de qualquer natureza.

O e-mail corporativo e as informações nele contidas são de propriedade do Grupo Liqi e, como tal, poderão ser auditados sem prévio aviso. O Grupo Liqi também poderá realizar o monitoramento contínuo da rede e dos e-mails, visando evitar a perda de informações da empresa.

O Grupo Liqi poderá restringir a entrada de arquivos suspeitos como prevenção contra vírus de computador.

Adicionalmente, o Grupo Liqi disponibiliza, a depender da função, equipamentos eletrônicos móveis, como smartphones e notebooks. É responsabilidade do Colaborador autorizado manter esses equipamentos em condições seguras, evitando danos ou furtos. Ademais, é vedada a utilização do e-mail pessoal nos computadores e celulares disponibilizados e/ou instalar aplicativo ou configurar recursos e serviços não autorizados, ou utilizar a rede de internet do Grupo para esses fins.

Todo Colaborador que utiliza um ou mais equipamentos disponibilizados pelo Grupo Liqi está sujeito às seguintes regras:

(i) O uso de smartphones é permitido, desde que sejam conectados na rede Wi- Fi própria autorizada do Grupo Liqi, configurada pela área responsável;

(ii) A sessão de trabalho deve ser encerrada no final do expediente, com desligamento do equipamento ou logout e suspensão do equipamento. O uso do dispositivo deve ser restrito à jornada normal de trabalho, salvo quando autorizado pela Liqi;

(iii) É obrigatório manter todos os arquivos originais salvos nos sistemas do Grupo Liqi, sendo proibido que esses sejam mantidos em unidades de armazenamento locais ou móveis (exemplo: drive "C", pen drive, HD externos, área de trabalho dos computadores, CD etc.). Em caso de necessidade de cópia para armazenamento temporário em unidades móveis para transporte, por favor informar na Central de Suporte para verificação da necessidade de adoção de possíveis medidas de segurança, como criptografia ou bloqueio por senha;

(iv) O usuário deverá, obrigatoriamente, utilizar bloqueio automático e senhas de acesso para seus dispositivos móveis;

(v) Havendo necessidade de transporte do equipamento, o Colaborador deve tomar todos os cuidados possíveis para a proteção do equipamento contra furtos;

(vi) Ao se conectar em sua residência, o Colaborador deve garantir que seu roteador esteja com a senha de administrador diferente da fornecida pelo fabricante. Além disso, deve o Colaborador verificar com o fornecedor da rede Wi-Fi a aplicação de configurações de segurança como, por exemplo: habilitação do protocolo WPA2;

(vii) É responsabilidade do usuário, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Grupo Liqi, notificar imediatamente seu gestor imediato, bem pela Central de Suporte registrar um boletim de ocorrência (BO);

O Grupo Liqi, na qualidade de proprietário ou possuidor indireto ou direto dos dispositivos móveis, reserva-se o direito de inspecioná-los a qualquer tempo, sem prévio aviso.

Controle de Acesso

O acesso de pessoas estranhas ao Grupo Liqi a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pela Diretora de Compliance e/ou pelo CTO.

Tendo em vista que a utilização de computadores, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, o Grupo Liqi monitora a utilização de tais meios.

Firewall, Software, Varreduras e Backup

O Grupo Liqi utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. A Área de Compliance e PLD-FTP, com o auxílio da Área de SI, é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

O Grupo Liqi mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras periódicas para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede do Grupo Liqi.

O Grupo Liqi utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. A Área de Compliance e PLD-FTP, com o auxílio da Área de SI, é responsável por patches regulares nos sistemas do Grupo Liqi.

Todos os arquivos devem ser salvos pelos Colaboradores dentro do banco de dados utilizado pelo Grupo Liqi, a fim de mantê-los seguros e sem possibilidade de perda ou exclusão. O Grupo Liqi mantém e testa regularmente medidas de *backup* consideradas apropriadas pela Diretora de Compliance e PLD-FTP com o apoio do Área de SI. O processo de execução de Backup é realizado diariamente de forma a evitar ou minimizar a perda de dados em hipótese de ocorrência de incidentes.

Uso da Internet e Mídias Sociais

O uso da Internet deve se limitar a pesquisas e necessidades específicas do trabalho do Colaborador. Acessos não relacionados com a prática profissional são proibidos.

O uso e acesso à Internet é proibido, inclusive, mas sem limitação, para:

(i) Acessar sites suspeitos, não confiáveis, que não adotem protocolo de segurança ou sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados, sendo certo que a tentativa do acesso será monitorada;

(ii) Divulgar e compartilhar dados ou informações do Grupo Liqi em listas de discussão (fóruns), sites ou comunidades de relacionamento, salas de bate-papo, chat, comunicadores instantâneos ou qualquer outra Rede Social ou tecnologia correlata que venha surgir na Internet;

(iii) Copiar ou distribuir quaisquer materiais, incluindo *software*, que viole direitos de propriedade intelectual de terceiros ou fazer o *download* ou distribuição de software ou dados pirateados ou qualquer atividade considerada ilegal;

(iv) Usar ferramentas de *torrent* e de troca de informação e conteúdo *on-line* em redes P2P (*Peer-to-peer*);

(v) Usar nos computadores corporativos ferramentas de mensagens instantâneas não autorizadas pelo Grupo Liqi;

(vi) Utilizar serviços de vídeos em tempo real (como *Vimeo* e afins) não autorizados pelo Grupo Liqi;

(vii) Acessar sites de redes sociais nos computadores corporativos (como *Facebook, Instagram* e *Twitter*), exceto pelas áreas que possuam autorização;

O uso de redes de internet *Wi-Fi* públicas ou que exijam o acesso de dados para a conexão:

O uso de Mídias Sociais por Colaboradores das áreas que possuam autorização deverá considerar as seguintes diretrizes;

(i) Ter ciência de que sua imagem pode ser relacionada ao Grupo Liqi, especialmente, quando identificado nas redes sociais como Colaborador do Grupo Liqi;

(ii) Assumir a responsabilidade pelo conteúdo publicado e escrito nas mídias sociais, sendo vedada a publicação em nome de terceiros;

(iii) Respeitar a confidencialidade, privacidade e a proteção de dados pessoais;

(iv) Abster-se de divulgar Informações Confidenciais, sigilosas e de propriedade exclusiva do Grupo Liqi.

O Grupo Liqi possui canais oficiais, áreas responsáveis por criar estratégias de Marketing, zelar pela imagem da empresa e divulgar materiais publicitários para demonstrar serviços nas mídias sociais, gerar engajamento e aumentar a confiabilidade e integridade do Grupo Liqi. Portanto, não é permitido aos colaboradores, sem prévia autorização, criar perfis, páginas e grupos utilizando a marca, nome empresarial ou qualquer sinal visual de titularidade do Grupo Liqi.

Os colaboradores se declaram cientes de que as redes disponibilizadas pelo Grupo Liqi para o exercício de sua atividade poderão ser monitoradas para fins de, mas não se limitando, segurança, auditoria.

Uso de Antivírus

Todas as estações de trabalho devem conter um antivírus instalado, atualizado e operando automaticamente. Caso o Colaborador identifique que o antivírus não está instalado, deve informar à Central de Suporte para que sejam adotadas as medidas necessárias.

Nenhum equipamento deve ser conectado na rede sem o antivírus padrão. O Colaborador não está autorizado, em hipótese alguma, a desabilitar ou interromper o antivírus.

Os colaboradores devem executar a verificação com o antivírus, de acordo com as orientações recebidas pela área de Infraestrutura. Em hipótese alguma o Colaborador deverá tentar obstruir, esquivar ou dificultar o funcionamento deste serviço ou de outros relativos aos filtros de segurança instalados nos computadores e telefones do Grupo Liqi.

7. MONITORAMENTO E TESTES

A Diretora de Compliance e PLD-FTP (ou pessoa por ela incumbida), com o auxílio da Área de SI, adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e

(ii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Diretora de Compliance e PLD-FTP poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

8. PLANO DE IDENTIFICAÇÃO DE RESPOSTAS

Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos do Grupo Liqi (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretora de Compliance e PLD-FTP prontamente. A Diretora de Compliance e PLD-FTP determinará quais membros da administração do Grupo Liqi e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, a Diretora de Compliance e PLD-FTP determinará quais Investidores e parceiros comerciais, conforme o caso, deverão ser contatados com relação eventual à violação.

Procedimentos de Resposta

A Diretora de Compliance e PLD-FTP responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos do Grupo Liqi de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, Investidores e parceiros comerciais afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente;

(vii) Determinação do responsável (ou seja, o Grupo Liqi ou Investidor ou parceiro comercial afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo da Diretora de Compliance e PLD-FTP, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

9. PROPRIEDADE INTELECTUAL

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto ao Grupo Liqi, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação e análise, em qualquer formato, são e permanecerão sendo propriedade exclusiva do Grupo Liqi, razão pela

qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades no Grupo Liqi, devendo todos os documentos permanecer em poder e sob a custódia do Grupo Liqi, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento do Grupo Liqi, salvo se autorizado expressamente pelo Grupo Liqi e ressalvado o disposto abaixo.

10. IOLAÇÃO E PENALIDADES

O descumprimento desta Política implica em falta grave e será passível de responsabilização, conforme Política de Consequências.

O colaborador que violar esta Política poderá ser notificado e a ocorrência da transgressão será prontamente comunicada ao seu gestor imediato, sem prejuízo do dever de comunicação à Diretora de Compliance e PLD, dependendo do nível da violação.

Em caso de dúvidas relacionadas a esta Política ou, caso queira relatar qualquer violação ou suspeita de descumprimento das disposições contidas neste documento, deve-se entrar em contato pelo Canal de Denúncias.

11. TREINAMENTOS

A Diretora de Compliance e PLD-FTP, com o auxílio da Área de SI, organizará treinamento anual dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme descrito no item 3 do Manual de Compliance e Controles Internos do Grupo Liqi).

12. REVISÃO DA POLÍTICA

A Diretora de Compliance e PLD-FTP realizará a revisão desta Política a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais. A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais do Grupo Liqi e acontecimentos regulatórios relevantes.

13. CONSIDERAÇÕES GERAIS

Esta Política entra em vigor imediatamente na data de sua aprovação pelo Comitê de Compliance e PLD-FTP e por ele poderá ser modificada a qualquer momento.

Em caso de conflito entre esta Política e o Código de Ética e Conduta, este último prevalecerá.

O Grupo Liqi pode analisar e revisar periodicamente as práticas, as políticas e os procedimentos de proteção de dados, inclusive esta Política. Se forem feitas quaisquer alterações significativas, o Grupo Liqi: (i) tomará as medidas razoáveis para informar todos os colaboradores e demais pessoas afetadas por essas alterações; e (ii) publicará avisos apropriados referentes às alterações, conforme necessário.

14. HISTÓRICO DAS ATUALIZAÇÕES DESTE MANUAL

Histórico das atualizações		
Data	Versão	Responsável
Novembro de 2024	3ª e atual	Diretora de Compliance e PLD-FTP
Maio de 2024	2ª	Diretora de Compliance e PLD-FTP
Junho de 2022	1ª	Diretora de Compliance e PLD-FTP

TR Block Securitizadora_Política de Segurança da Informação e Cibernética_21.11.2024.docx.pdf

Documento número #13cfe9aa-afff-4b95-8f3d-616c39949a50

Hash do documento original (SHA256): 4c7f7d209544cbcaa6af5540e8da1f5d05a097dc6d07634f857c9fd2618ae7db

Assinaturas

Rita Di Cascia Casolato
CPF: 268.200.268-46
Assinou em 28 nov 2024 às 16:42:01

Log

27 nov 2024, 15:25:04	Operador com email adriana@liqi.com.br na Conta ffb255c9-b8f1-4a75-b1db-3f2e5e7174a3 criou este documento número 13cfe9aa-afff-4b95-8f3d-616c39949a50. Data limite para assinatura do documento: 27 de dezembro de 2024 (15:25). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
27 nov 2024, 15:25:37	Operador com email adriana@liqi.com.br na Conta ffb255c9-b8f1-4a75-b1db-3f2e5e7174a3 adicionou à Lista de Assinatura: rita@liqi.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rita Di Cascia Casolato e CPF 268.200.268-46.
28 nov 2024, 16:42:01	Rita Di Cascia Casolato assinou. Pontos de autenticação: Token via E-mail rita@liqi.com.br. CPF informado: 268.200.268-46. IP: 187.59.61.16. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5669504 e longitude -46.5459273. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1059.0 disponibilizado em https://app.clicksign.com.
28 nov 2024, 16:42:02	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 13cfe9aa-afff-4b95-8f3d-616c39949a50.