



MANUAL DE PROTEÇÃO DE DADOS PESSOAIS

MAIO/2024

ÍNDICE

1. INTRODUÇÃO E OBJETIVOS	3
2. SEGURANÇA DA INFORMAÇÃO	4
3. SEGURANÇA CIBERNÉTICA	9
4. SEGURANÇA FÍSICA DO AMBIENTE.....	10
5. NORMAS DE UTILIZAÇÃO.....	10
6. GESTÃO DE ACESSOS.....	13
7. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD).....	14
8. TRATAMENTO E PLANO DE RESPOSTAS A INCIDENTES	16
9. ENCARREGADO DE DADOS PESSOAIS	16
10. <i>PHISHING</i>	16
11. BACKUP	17
12. TESTE DE STRESS.....	18
13. TREINAMENTO	18
14. ESTRUTURA DE GOVERNANÇA	19
15. HISTÓRICO DE ATUALIZAÇÕES	20
ANEXO I.....	21

1. INTRODUÇÃO E OBJETIVOS

A informação é um dos principais bens de toda organização. O fluxo e uso adequado da informação é essencial para o funcionamento eficiente da organização, bem como o gerenciamento dos riscos e ameaças inerentes à crescente facilidade de acesso à informação.

Sendo assim, o maior objetivo desta Política é a redução das vulnerabilidades da 3Q a ameaças à segurança da informação, assim como a prevenção, detecção e redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Este Manual de Proteção de Dados Pessoais ("Manual") da **3Q ASSET LTDA.** ("Gestora") visa a atender as diretrizes mínimas com relação ao tratamento de dados pessoais de acordo com a Lei nº 13.709/2018, alterada pela Lei 13.853/2019 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD"), ISO 27001/2013 e Guia de Cibersegurança ANBIMA (Programa de Segurança Cibernética da ANBIMA), no âmbito das atividades exercidas pela Gestora, sem prejuízo de outras providências que se façam necessárias para a integral conformidade com a LGPD, tais como mapeamento de atividades de tratamento de dados pessoais e diagnóstico da maturidade da Gestora com relação à proteção de dados pessoais.

A observância das regras e obrigações contidas neste Manual é dever de todos os colaboradores da Gestora, incluindo sócios, administradores, funcionários e estagiários da Gestora ("Colaboradores").

As regras descritas neste Manual são aplicáveis em favor de todas as pessoas físicas que venham a se relacionar com a Gestora e forneçam Dados Pessoais (abaixo definido), quer sejam, dentre outros, investidores, contrapartes e demais agentes envolvidos nas operações das carteiras sob gestão da Gestora ou Colaboradores (todos em conjunto "Titulares de Dados"), cujos dados demandem o Tratamento (abaixo definido) adequado.

Este Manual é parte integrante das regras que regem a relação societária, de trabalho ou contratual, conforme o caso, dos Colaboradores, os quais deverão firmar o termo de recebimento e compromisso constante do Anexo I a este Manual ("Termo de Recebimento e Compromisso"). Por esse documento, o Colaborador reconhece e confirma a leitura, o conhecimento, compreensão, concordância e adesão aos termos deste Manual e às normas e procedimentos aqui contidos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o seu conhecimento e concordância com os termos deste Manual.

Este Manual e todos os demais materiais informativos e diretrizes internas poderão ser consultadas pelos Colaboradores por intermédio do drive de compartilhamento, e quaisquer dúvidas deverão ser dirimidas junto ao Encarregado (abaixo definido).

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas e procedimentos estabelecidos neste Manual deverão ser levados para apreciação do Encarregado. Competirá ao Encarregado aplicar as sanções decorrentes de tais desvios, garantido ao Colaborador amplo direito de defesa.

Os Colaboradores, desta forma, estarão sujeitos, entre outras, às penas de advertência, suspensão, desligamento, exclusão ou demissão por justa causa, ou, ainda, rescisão contratual, conforme o regime aplicável, sem prejuízo de eventuais outras medidas adicionais no âmbito cível e criminal que se fizerem cabíveis.

2. SEGURANÇA DA INFORMAÇÃO

Os gestores de cada equipe são responsáveis pela aderência dos membros dos seus times aos princípios e procedimentos necessários. Os Colaboradores da área de TI são responsáveis por administrar as instalações e os procedimentos de segurança dos equipamentos e acessos.

Através da equipe de TI, a 3Q efetuará avaliações de risco regulares do ambiente de segurança da informação, para estimar a vulnerabilidade em potencial e garantir que as medidas de segurança reduzam os riscos e estabeleçam patamares apropriados. Os riscos da avaliação interna incluem:

- a) Usuários com nível de acesso superior ao necessário;
- b) Garantir a segurança de cada terminal e dos materiais impressos em nome da 3Q;
- c) Uso da internet ou de aplicativos que permitam invasão;
- d) Mensagens eletrônicas forjadas – como Phishing;
- e) Uso de credenciais ou acesso de terceiros.

O compromisso da 3Q com o tratamento adequado das informações de dados pessoais está fundamentado nos seguintes princípios:

- a) Confidencialidade: garantimos que o acesso aos dados pessoais seja obtido somente por pessoas autorizadas e quando for necessário;
- b) Disponibilidade: garantimos que as pessoas autorizadas tenham acesso aos dados pessoais, somente quando necessário;
- c) Integridade: garantimos a exatidão e a completude dos dados pessoais e dos métodos de seu processamento;

- d) Finalidade: realização do tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- e) Adequação: compatibilidade do tratamento de dados pessoais com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- f) Necessidade: limitação do tratamento de dados pessoais ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;
- g) Livre acesso: garantia aos titulares de dados pessoais de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais;
- h) Qualidade dos dados: garantia aos titulares de dados pessoais de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- i) Transparência: garantia aos titulares de dados de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- j) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- k) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- l) Não discriminação: impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos;
- m) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas.

Esta Política se aplica a todas as informações presentes na 3Q, que podem existir de diversas maneiras:

- a) Escrita em papel;
- b) Armazenada e/ou transmitida por meios eletrônicos;
- c) Exibida na mídia;
- d) Falada em conversas formais e informais.

Independente da forma ou o meio pelo qual a informação for apresentada/compartilhada, ela sempre deverá estar protegida adequadamente, de acordo com controles definidos nesta Política.

Todos os usuários que utilizam Sistemas de Informação (“SI”) e fazem parte da 3Q devem, obrigatoriamente, conhecer e obedecer a esta Política, sendo responsabilidade de cada Colaborador o seu cumprimento. Caso algum usuário perceba qualquer incidente de segurança da informação, deve informar o ocorrido imediatamente às áreas de Compliance e TI.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários na utilização dos SI na 3Q.

As informações de propriedade da 3Q devem ser utilizadas apenas para os propósitos devidos. Os usuários não podem, em qualquer hipótese, apropriar-se dessas informações, seja em CDs, uploads, downloads, pen drives ou qualquer outra mídia de armazenamento de dados. Todos os documentos produzidos por qualquer SI na 3Q são de propriedade exclusiva da 3Q.

A identificação do usuário (por meio de seu usuário de rede, senha, ou outro meio qualquer) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas utilizando tal identificação.

A 3Q, por meio de suas áreas de Compliance e Tecnologia da Informação, reserva-se o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à internet, o uso do correio eletrônico e a obediência às normas/procedimentos escritos nesta Política.

Todas as informações deverão ter classificação de segurança, para que haja proteção adequada quanto ao seu acesso e uso.

A informação deve receber proteção adequada em observância aos princípios e diretrizes de segurança da informação da 3Q em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transferência, transporte; e descarte.

Os acessos a plataformas e equipamentos são disponibilizados pela 3Q, enquanto o Colaborador integre seu quadro. Não é permitido o compartilhamento a terceiros e o uso que não atenda exclusivamente aos objetivos da 3Q

A 3Q tem o direito irrestrito, independentemente de qualquer aviso prévio, notificação ou formalidade, de inspecionar quaisquer dados pessoais contidos nos equipamentos, na rede e nos sistemas a ela licenciados para prevenir, detectar ou minimizar os impactos decorrentes do uso inadequado ou em descumprimento às suas políticas e a legislação que lhe for aplicável.

Para assegurar que os dados pessoais tratados estejam adequadamente protegidos, a 3Q adota os seguintes processos:

- a) **Gestão de Ativos da Informação:** Entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e até excluir informações. Podem ser tecnológicos (software e hardware) e não tecnológicos (pessoas, processos e dependências físicas). Os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente e tecnologicamente, e ter documentação e planos de manutenção atualizados anualmente. Métodos de proteção e segurança são aplicados aos ativos da informação para proteger acessos indevidos ou não autorizados vindos de meio externo ou interno, como dispositivos móveis (pendrives, cartões de memória, HD externo ou equivalentes) ou mídias removíveis (smartphones, câmeras, gravadores e equivalentes). Estes dispositivos estão sob atenção especial e restrições para evitar infiltração de fragilidades ou facilitar vazamento de informações. Os equipamentos pertencentes à 3Q de uso pessoal/coletivo, servidores de dados e aplicativos, de qualquer porte, estão dotados de mecanismos de proteção contra vírus e malwares.
- b) **Transferência de Informações/Dados:** Estabelece diretrizes e padrões para os procedimentos de transferência de dados internamente e externamente, com proteção e segurança, através de análises e investigação de vulnerabilidades nos recursos de processamento da informação, permitindo correções/adequações tempestivas, minimizando os riscos de violação de dados e mitigando o vazamento dos dados tratados. Os recursos adotados constam de itens técnicos dos contratos com fornecedores.

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias nos seguintes níveis:

- a) **Informação Restrita:** é toda informação associada aos interesses estratégicos da 3Q, de posse da diretoria, dos comitês e dos gestores das áreas. Seu acesso deve ser limitado a um número reduzido de pessoas autorizadas. Se revelada ou adulterada, pode trazer sérios prejuízos financeiros, favorecer a concorrência e gerar impactos negativos nos negócios e à imagem da 3Q ou dos demais agentes do negócio. Essas informações requerem medidas de controle e proteção rigorosas contra acessos, cópias ou reproduções não autorizadas. Em geral, seu acesso é limitado à diretoria, gerentes das áreas, jurídico, auditoria e Colaboradores previamente designados.
- b) **Informação Confidencial:** é toda informação transmitida por meios escritos, eletrônicos, verbais ou quaisquer outros e de qualquer natureza, cujo conhecimento está limitado à Colaboradores que, pela natureza da função,

dela necessitam para o exercício profissional. Sua divulgação ou adulteração pode trazer impactos negativos aos negócios e na gestão de processos, ou prejuízos à imagem da 3Q ou aos demais agentes do negócio.

- c) Informação de Uso Interno: é toda informação cujo conhecimento e uso estão restritos exclusivamente ao ambiente interno e aos propósitos da 3Q, estando disponível aos Colaboradores e podendo ser revelada ao público externo apenas mediante autorização do gestor da informação.
- d) Informação de Uso Público: é toda informação que pode ser divulgada para o público externo à 3Q, sem implicações de proteção e controle de acesso. Tais informações somente serão publicadas com permissão da 3Q, na figura de um dos seus administradores.

Caso um Colaborador tenha acesso a qualquer informação à qual não tenha sido previamente autorizado, este deverá, imediatamente, abster-se de usar tal informação em seu favor, para clientes da 3Q ou para terceiro, além de informar a Diretoria acerca do ocorrido.

Caso um Colaborador mude de atividade dentro da 3Q, deverá ter seu acesso às informações de sua antiga área restringidos, não sendo mais uma pessoa autorizada a lidar com as informações que antes tinha acesso. Na hipótese de desligamento, o Colaborador terá seus acessos à 3Q restritos e não poderá utilizar nenhuma informação de que tenha conhecimento, seja Informação Restrita, Informação Confidencial, Informação de Uso Interno, Informação de Uso Público ou qualquer outra.

A 3Q veda expressamente aos Colaboradores efetuar qualquer tipo de operação nos mercados financeiros e de capitais baseada em informações privilegiadas, bem como recomendá-las ou sugerir-las a terceiros. Fica ressaltado que a realização de operações nos mercados financeiro e de capitais mediante o emprego de informações privilegiadas fere as regras estabelecidas pela Comissão de Valores Mobiliários, sendo punível cível e criminalmente.

Todas as Informações Confidenciais recebidas devem ser analisadas pelo Colaborador atentamente, principalmente, mas não limitado a:

- a) Insider Trading: significa a compra e/ou venda de títulos e valores mobiliários com o uso de informação privilegiada, com a intenção de auferir benefício para si ou para terceiros;
- b) Front Running: significa a realização de operações de compra e/ou venda de títulos e valores mobiliários de forma a concluir e/ou obter vantagem econômica antecipadamente a outros;
- c) Qualquer outra prática que não esteja alinhada com os interesses da 3Q e seus clientes.

Na classificação de um conjunto de informações que apresentam diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente no conjunto.

Para isto, devem ser consideradas as necessidades relacionadas aos negócios, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. Tal classificação será atribuída inicialmente pelo gestor da informação devendo ser obedecida por quem recebê-la.

3. SEGURANÇA CIBERNÉTICA

A aplicação do programa de segurança cibernética da 3Q é norteada pelos seguintes fatores:

- a) Identificação/avaliação de riscos (risk assessment) – identificação dos riscos internos e externos, dos ativos de hardware, software e processos que precisam de proteção. A mensuração destes riscos é mapeada e evidencia os sistemas críticos da 3Q para protegê-los de forma mais abrangente. São considerados sistemas críticos os sistemas: de bancos vinculados a 3Q, o sistema de banco de dados interno.
- b) Ações de prevenção e proteção – estabelecimento de um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles. As ações de prevenção já realizadas pela 3Q são: atualização de antivírus, backups (tanto cloud quanto físico), a realização de assessment para mensurar possíveis falhas ainda existentes, a execução de sistemas de mapeamento e mitigação de phishing, dentre outros.
- c) Monitoramento e testes – detecção das ameaças em tempo hábil, de forma a reforçar os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados. A 3Q realiza monitoramento, em todo o ambiente cibernético existente, de forma física e em nuvem. Dessa forma, caso ocorra quaisquer falhas, perdas ou inconsistências, há ação direta da área de TI e do Compliance, se necessário. Já no tocante aos testes de funcionamento dos ambientes de tecnologia e seus desdobramentos, estes são realizados tanto pela área de Auditoria Interna como pela área de Controles Internos.
- d) Criação do plano de resposta – ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário. O plano de resposta a incidentes consta disposto, especificamente, no Manual de Plano de Contingência. Já o plano de resposta aos demais itens/falhas detectadas, são endereçados com as áreas carentes junto dos departamentos de Auditoria e de Controles Internos.

- e) Governança – manutenção do programa de segurança cibernética, continuamente atualizado, garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida.

Conforme sua criticidade, as ações do programa de segurança cibernética dividem-se em:

- a) Ações Críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- b) Ações de Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite ao risco da 3Q e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- c) Ações Estruturantes: Iniciativas de médio/longo prazo que tratam a causa dos riscos e que preparam a 3Q para o futuro.

O acesso às dependências físicas da 3Q são controladas por biometria.

Todos os dispositivos e todo o tráfego de informação estão gerenciados e monitorados de forma centralizada pela área de Tecnologia da Informação e auditado pelo time de suporte. Os dispositivos estão no domínio da 3Q.

4. SEGURANÇA FÍSICA DO AMBIENTE

A segurança física do ambiente refere-se a medidas de segurança adotadas no ambiente físico da 3Q, onde contém, ou pretende-se disponibilizar, acessos a ativos de informações sensíveis. Visa a proteção de ativos sensíveis (dados e informações) contra acesso não autorizado, modificação ou destruição, assim como, a proteção do próprio sistema de tecnologia da informação contra uso não autorizado ou danos físicos.

O processo de segurança física estabelece controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas.

Uma das formas de proteção das instalações e das áreas seguras é realizada por meio do estabelecimento de perímetros de segurança física. O estabelecimento da 3Q possui uma entrada restrita para pessoas autorizadas, sendo necessário o cadastramento biométrico. Em caso de visitantes, o controle de acesso é realizado na recepção do prédio onde se localizada a 3Q.

5. NORMAS DE UTILIZAÇÃO

Da internet:

- a) O acesso à internet na 3Q é uma concessão feita aos usuários e não um direito. Disto decorre que se deve utilizá-la prioritariamente para atividades ligadas ao trabalho, quando em horário comercial.
- b) Os usuários devem utilizar a internet de forma adequada e diligente, em conformidade com a lei, a moral e a ordem pública, abstendo-se de objetivos ou meios para a prática de atos ilícitos, lesivos aos direitos e interesses da 3Q ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos e documentos de qualquer tipo.
- c) É proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão, bate-papo ou softwares de mensagens eletrônicas.
- d) Usuários com acesso à internet não podem efetuar upload de qualquer software cuja licença pertence à 3Q, o mesmo ocorrendo para dados de propriedade da 3Q. Exceção feita a casos especiais, mediante autorização do(s) responsável(is) pelo(s) software(s) e/ou dado(s).
- e) Downloads serão autorizados desde que a fonte seja confiável. Para a instalação de softwares oriundos da internet, será necessária autorização da área de Compliance.
- f) Cada usuário é responsável por zelar pelo cumprimento da presente Política e por todas as atividades realizadas por intermédio de seu usuário de rede. As contas de serviço têm acesso restrito a determinadas pastas de rede na 3Q.
- g) Não é permitida a utilização de software peer-to-peer, acesso a sites de pornografia, pedofilia e outros contrários à lei.

De Meios de Comunicação Informais:

- a) De acordo com a regulamentação aplicável, certas ligações telefônicas e mensagens instantâneas, em nome da 3Q, são registradas, monitoradas e armazenadas. Os Colaboradores estão cientes do sistema de gravação telefônica e de mensagens instantâneas, e, por isso, concordam que os usos de comunicação autorizados são monitorados, independentemente de sua ciência e anuência, não sendo reservado ao usuário qualquer direito sobre o material coletado.

Do Correio Eletrônico:

- a) Por ser uma ferramenta de trabalho, as contas de correio eletrônico têm titularidade única e exclusiva, o que determina a responsabilidade direta do usuário. As contas de serviço, por sua vez, possuem um ou mais responsáveis pelo seu uso. A utilização do correio deve ser feita de forma adequada e diligente.

- b) É vedada a qualquer usuário a utilização do correio eletrônico para quaisquer das seguintes atividades:
- I. Envio de mensagens não autorizadas, divulgando informações sigilosas;
 - II. Acesso não autorizado à caixa postal de outro usuário ou de serviços;
 - III. Envio, manuseio e armazenamento de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos (seja pela lei, seja pela presente Política), lesivos aos direitos e interesses da 3Q, que possam danificar, inutilizar, sobrecarregar ou deteriorar hardware e/ou software, documentos e arquivos de qualquer tipo, ou que contrariem a moral, os bons costumes e a ordem pública;
 - IV. Envio intencional de mensagens do tipo “corrente”, “spam” ou que contenham vírus eletrônico ou qualquer forma de programação (arquivos executáveis ou do tipo script) que sejam prejudiciais ou danosas aos destinatários das mensagens;
 - V. Utilização de listas e/ou caderno de endereços para distribuição de mensagens que não tenham relação com o interesse funcional da 3Q ou a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
 - VI. Todo e qualquer uso do correio eletrônico não previsto nesta Política que afete a 3Q de forma negativa.
- c) Qualquer violação aos itens dispostos neste capítulo não garante a preservação sigilosa dos dados constantes no correio eletrônico em questão.

De Contas e Senhas para Usuários:

- a) Com o intuito de controlar a distribuição de direitos de acesso a sistemas de informação e serviços, a 3Q estabelece estas normas para evitar o uso inapropriado de senhas e, conseqüentemente, diminuir o risco de falhas e violações de sistemas.
- b) Todas as senhas de rede são pessoais e intransferíveis, devendo ser mantidas em sigilo. Cada usuário é responsável por sua senha e será responsabilizado pelo mau uso dessa senha.
- c) A 3Q efetua o estabelecimento de senhas da seguinte forma:
 - I. Senha de rede - Os usuários finais deverão estabelecer senhas de acesso ao notebook ou ao desktop de forma a respeitar o seguinte padrão: ter, no mínimo, seis a oito caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais (@ % ^; .).
 - II. Senha de sistemas críticos - são considerados sistemas críticos os sistemas de bancos vinculados a 3Q; sistema de banco de dados interno. Os parâmetros mínimos de configuração de senha deverão seguir o mesmo padrão estabelecido para as senhas de rede, com exceção dos usuários de bancos, os quais possuem critérios básicos próprios.

Todos os sistemas e aplicações instalados na 3Q possuem mecanismo que oculta a visualização das senhas para utilização desses sistemas/aplicações.

Os usuários de rede terão privilégios administrativos que se enquadrem às suas atividades, o mesmo ocorrendo nas permissões aos diretórios de rede e seus conteúdos. É vedado, de forma a resguardar a segurança da informação da 3Q, a utilização de usuários não nominais por Colaboradores, assim como a utilização de usuários que não sejam em nome próprio.

Instalações de softwares de qualquer natureza devem ser solicitadas à área de TI, que irá analisar o impacto dessa instalação, executando-a ou não, de acordo com o resultado dessa avaliação.

O histórico de acessos dos usuários é controlado de forma individualizada, através do recurso que detém a informação. No caso de acessos a dados armazenados em servidores, os eventos de segurança evidenciam os acessos.

6. GESTÃO DE ACESSOS

Os acessos são concedidos pela área de tecnologia e autorizados pela área de Compliance. As concessões, revisões e exclusões de acesso são mapeados e respeitam a segregação da 3Q.

Além disso, os acessos são rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador responsável pela ação, para sua devida responsabilização.

Na contratação ou na transferência de área, cada gestor de área é responsável pelo pedido de acesso aos recursos necessários aos seus Colaboradores geridos, de modo que as áreas de TI e Compliance, juntamente, estejam cientes e concordem com a habilitação adequada. É de responsabilidade de cada Colaborador a leitura e a compreensão dos funcionamentos dos recursos aos quais tem acesso. A revisão de acessos atuais é feita anualmente, buscando sanar conflitos de interesse e manter a matriz de acessos atualizada.

Em caso de identificação de conflitos dos acessos aprovados pelo gestor, em relação à matriz de segregação de funções, o gestor de TI encaminhará uma solicitação à área de Compliance, para avaliação da concessão.

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da 3Q, para que sejam recomendadas as proteções adequadas.

A identificação dos cenários de riscos de segurança da informação é discutida nos Comitês Executivo e de Riscos e Compliance.

Os testes de identificação de vulnerabilidades e fragilidades na infraestrutura interna e externa da 3Q são realizados anualmente e são avaliados pela alta direção tendo seus planos de ação considerados e adotados conforme deliberação desses comitês.

7. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei Geral de Proteção de Dados Pessoais de 14 de agosto de 2018 (“LGPD”) regula todo tratamento de dados pessoais na 3Q e visa a promoção de uma proteção igualitária dos dados pessoais de todos os cidadãos.

A disciplina da proteção de dados pessoais tem como fundamentos:

- a) o respeito à privacidade;
- b) a autodeterminação informativa;
- c) a liberdade de expressão, de informação, de comunicação e de opinião;
- d) a inviolabilidade da intimidade, da honra e da imagem;
- e) o desenvolvimento econômico e tecnológico e a inovação;
- f) a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A legislação se fundamenta em diversos valores e tem como principais objetivos:

- a) Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais;
- b) Estabelecer regras claras sobre o tratamento de dados pessoais;
- c) Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo;
- d) Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

Os dados confidenciais podem ser classificados de acordo com a sua natureza, são eles:

- a) Dados pessoais - qualquer informação que possa tornar uma pessoa física identificada ou identificável;
- b) Dados sensíveis - qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.

O consentimento é definido na LGPD como uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Assim, esse tipo de autorização poderá ser livre (o titular não pode ser obrigado a dar o seu consentimento e este também não pode ser obtido de forma automática, como em caixas de textos já préselecionadas ou em casos em que a própria navegação na plataforma já pressupõe o aceite de todas as condições); informada (o titular deve compreender exatamente o que ele está consentindo, por que e para que antes de tomar qualquer decisão. Além disso, a informação deve ser passada de forma completa, transparente e simples). E inequívoca (não pode haver dúvidas sobre a verdadeira aceitação daquelas condições pelo titular e as empresas devem se esforçar ao máximo para garantir essa compreensão).

O consentimento necessita ser documentado de forma a demonstrar a manifestação de vontade do titular. A autorização deverá ter finalidades determinadas. Textos genéricos, enganosos, abusivos ou que não tenham sido apresentados com transparência em momento anterior serão considerados nulos.

O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Em caso de mudança de finalidades, condições ou compartilhamento dos dados pessoais, a 3Q informará o fato de forma destacada, tendo o titular o direito de revogar o consentimento caso discorde das alterações.

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- b) fim do período de tratamento;
- c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da Lei de LGPD, resguardado o interesse público; ou
- d) determinação da autoridade nacional, quando houver violação ao disposto na LGPD.

8. TRATAMENTO E PLANO DE RESPOSTAS A INCIDENTES

Os incidentes de segurança da informação e cibernéticos da 3Q devem ser reportados à área de Compliance. O processo de tratamento destes incidentes resta mapeado em documento exclusivo denominado Manual de Gestão de Incidentes, o qual está sob posse das áreas envolvidas. Para casos de incidentes de vazamento de informações o DPO deverá ser imediatamente comunicado e acionado para realizar a gestão deste processo.

A 3Q possui procedimentos em caso de incidentes, devendo tomar providências dentro de prazos e de forma razoável e apropriada ao caso concreto, identificando a vulnerabilidade e os riscos em questão. Ademais, há salvaguardas reativas contra ocorrências de quaisquer intrusões, para reparar e reportar ameaças caso haja um incidente.

Em caso de incidente, além da comunicação às áreas internas, a área de Compliance prosseguirá com a comunicação às autoridades competentes que se fizer necessária.

9. ENCARREGADO DE DADOS PESSOAIS

O Encarregado será indicado pela Gestora (na qualidade de Controlador) e sua identidade e informações de contato deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do Controlador. Assim, caso o Titular queira entrar em contato com o encarregado, será possível.

O Encarregado possui algumas atividades específicas, tais como, aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar providências, receber comunicações da ANPD e adotar providências, orientar os Colaboradores a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais e executar as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

Por fim, o Diretor de Compliance, Risco e PLD é o encarregado em manter as práticas da Gestora atualizadas em relação às melhores práticas e à regulamentação vigente, inclusive com treinamentos periódicos

10. PHISHING

O phishing é uma técnica utilizada por cibercriminosos para driblar os usuários, através de envio de emails maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros.

O e-mail de phishing possui o objetivo de atração da atenção dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade.

Modalidades de Phishing:

- a) Quando tentam se passar pela comunicação oficial de instituições conhecidas como: bancos, lojas de comércio eletrônico, entre outros sites populares;
- b) Quando tentam induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;
- c) A 3Q recomenda aos usuários de seus sistemas (diretores, sócios, Colaboradores etc.) que não clique em links suspeitos (por exemplo com erros de português, ofertas e benefícios extraordinários) através de computadores e dispositivos móveis relacionados a 3Q; que não exponha dados pessoais em redes sociais.

Caso, por motivos diversos, o usuário clique na comunicação fraudada, é obrigatório entrar em contato com a área de Compliance para que estas tomem as ações mitigadoras cabíveis, e possam mapear/impedir maiores danos, caso tenha havido vazamento de credenciais.

11. BACKUP

Este capítulo estabelece diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados realizados em caso de crise. O backup é executado de forma automática e abrange os dados gravados nos diretórios de rede privativos de cada equipe e nos servidores de dados e aplicativos.

A 3Q conta com backup nos servidores de Arquivos e Disaster Recovery. Todos os serviços e Colaboradores estão com a proteção de backup ativos, garantindo a disponibilidade dos dados, conforme a regulação aplicável exige.

Além disso, para parte de sistema de banco de dados interno, a 3Q possui backups em 4 (quatro) camadas, conforme se segue:

- a) Backup Local no servidor
- b) Backup na Nuvem Google Arq 5 com dados criptografados
- c) CloudBack (dados criptografados)
- d) Backup físico em Hard Disk externo

12. TESTE DE STRESS

É de responsabilidade de todos os Colaboradores observar as regras desta Política, para evitar a facilitação de possível ação criminosa a partir das informações geridas pela 3Q. De todo modo, foi definido um programa de segurança cibernética com as seguintes etapas:

- a) Identificação e avaliação de riscos;
- b) Ações de prevenção e proteção;
- c) Monitoramento e testes;
- d) Vigência.

A responsabilidade pela implementação, validação e testes caberá à área de Compliance e poderá contar com o auxílio externo especializado para melhorar a segurança do ambiente em questão, bem como de analistas de tecnologia para avaliar e identificar potenciais riscos da estrutura empregada. A partir da identificação dos riscos, serão analisados os princípios da confidencialidade, integridade e disponibilidade.

13. TREINAMENTO

Considerando que o nível de segurança depende da cooperação de todos os Colaboradores, é promovido treinamento anual, com o intuito de orientar sobre:

- a) As responsabilidades e os procedimentos relacionados a cada área de atuação;
- b) Acessos e limites de uso de forma apropriada; e
- c) Os requerimentos e obrigações de confidencialidade.

A 3Q se empenha para aderência aos requerimentos regulatórios e as diretrizes desta Política, de modo que orienta seus Colaboradores sobre a estrutura e os procedimentos de gerenciamento.

Considerando que todos os Colaboradores são devidamente instruídos e auxiliados, sempre que houver a ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nas normas internas e, ou, nas regulações aplicáveis às atividades da 3Q, de acordo com os procedimentos estabelecidos, o Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico disponíveis para verificar a conduta dos Colaboradores envolvidos, sendo facultado o acesso a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na 3Q, ou que transitem pela sua infraestrutura de TI. Eventualmente, medidas internas podem ser tomadas em caso de necessidade.

Realizamos ações de disseminação de questões sobre segurança da informação e cibernética por meio de treinamentos e e-mail corporativo.

14. ESTRUTURA DE GOVERNANÇA

A Diretoria Executiva é o órgão máximo de deliberação da 3Q. Sua atuação é pautada pelo comprometimento da 3Q com as melhores práticas na governança e no processo de segurança da informação, melhorando continuamente esta Política, sua governança, seus processos, seus procedimentos, os controles internos e a cultura organizacional sobre este assunto. Neste sentido, são atribuições da Diretoria Executiva:

- a) Estabelecer e revisar as diretrizes da Política de Segurança da Informação, no mínimo, anualmente;
- b) Prover recursos para que toda equipe atuante no processo possa alcançar seus objetivos;
- c) Zelar pela prevenção incidentes relacionados à segurança da informação;
- d) Avaliar a efetividade desta Política e dos procedimentos relacionados à segurança da informação;
- e) Investimento em recursos necessários ao processo de prevenção de incidentes;
- f) Incentivo e prática contínua a disseminação de uma cultura de gestão de riscos;
- g) Manutenção de Colaboradores experientes, qualificados, motivados, continuamente treinados e comprometidos com suas atribuições e responsabilidades; com os objetivos e metas estabelecidos pela administração e com a prestação de serviços de qualidade; e
- h) Incentivo a segregação de funções nas diversas áreas envolvidas no processo de prestação desses serviços.

São atribuições do Comitê de Riscos e Compliance:

- a) Aprovar os manuais de procedimentos que envolvem segurança da informação;
- b) Analisar os relatórios de Compliance e decidir pela comunicação do(s) cliente(s) enquadrado(s) como sensíveis;
- c) Analisar as demandas levadas a pauta das reuniões do Comitê de Risco e Compliance emitindo pareceres e decisões de acordo com esta Política e com a legislação aplicável; e
- d) Zelar pelos manuais que envolvem a segurança da informação, descritos neste documento.

É de responsabilidade da área de Tecnologia da Informação:

- a) A manutenção contínua do ambiente tecnológico seguro e que suporte a operação da 3Q;
- b) Oferecer suporte técnico e operacional às demais áreas nos assuntos relacionados à segurança da informação; e
- c) Manter seus processos aderentes às disposições estabelecidas nesta Política.

É de responsabilidade da área de Compliance:

- a) Divulgar e dar conhecimento a todos os Colaboradores sobre as normas e os procedimentos relativos à segurança da informação;
- b) Dar manutenção aos controles internos e manuais relativos ao tema;
- c) Orientar todos os Colaboradores de acordo com as regras estabelecidas nesta Política;
- d) Prover adequado treinamento aos Colaboradores com programação permanente e de amplo alcance; e
- e) Executar rotinas de diligência sobre a aderência dos processos estabelecidos às diretrizes da presente Política.

É de responsabilidade área de Controles Internos:

- a) Realizar testes, mapear falhas e conduzir planos de ação para correção.

15. HISTÓRICO DE ATUALIZAÇÕES

A primeira versão desse Manual foi elaborada em 04/01/2021, levando em consideração as normas e disposições aplicáveis publicadas à época. Na hipótese de alteração ou atualização legislativa, será emitida nova versão contemplando as novas disposições.

O presente Manual deverá ser revisto, no mínimo, anualmente, levando-se em consideração, dentre outras questões, mudanças regulatórias ou eventuais deficiências encontradas. Este Manual poderá ser também revisto a qualquer momento, sempre que o Encarregado entender necessário.

Histórico das atualizações desta Política		
Data	Versão	Responsável
Janeiro de 2021	1ª	Diretor Risco e Compliance
Agosto de 2021	2ª	Responsável por Compliance e Alta Administração
Junho de 2023	3ª	Responsável por Compliance e Alta Administração
Março de 2024	4ª	Responsável por Compliance e Alta Administração
Maio de 2024	5ª e atual	Responsável por Compliance e Alta Administração

ANEXO I
TERMO DE RECEBIMENTO E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____.____.____-____, DECLARO para os devidos fins:

- (i) Ter recebido, na presente data, o Manual de Proteção de Dados (“Manual”) da **3Q ASSET LTDA.** (“Gestora”);
- (ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual, incluindo as possíveis sanções decorrentes de condutas contrárias à regulamentação e as responsabilizações daí advindas;
- (iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e
- (iv) Estar ciente do meu compromisso de comunicar ao Encarregado, conforme definido no Manual, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras descritas nesta Manual.

São Paulo, [==] de [==] de [==]

[COLABORADOR]