AQUA GESTORA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

ESCOPO E APLICABILIDADE

OBJETIVO DO DOCUMENTO

O objetivo desta política é definir as diretrizes para a segurança da informação e privacidade da AQUA GESTORA, de acordo com suas necessidades de negócio e legais, dentro do escopo de seu sistema de gestão de privacidade da informação (SGPI).

APLICAÇÃO DO DOCUMENTO

As definições deste documento norteiam as normas e procedimentos de segurança da informação e privacidade da AQUA GESTORA e se aplicam a toda a equipe da empresa, seus prestadores de serviços e usuários dos seus sistemas de tecnologia da informação.

Normas e procedimentos detalhados para a aplicação de diretrizes aqui definidas poderão ser apresentadas em documentos correlatos, com a finalidade de facilitar a manutenção e a organização desta política de segurança da informação e privacidade.

DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO/IEC 27701:2019
- Lei 13709/18 (Lei de Proteção de Dados Pessoais - LGPD)

ASPECTOS GERAIS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

COMPROMETIMENTO DA EMPRESA

Esta política de segurança da informação e privacidade expressa o comprometimento da AQUA GESTORA, de sua diretoria executiva, dos gestores de suas equipes e de todos os seus colaboradores e prestadores de serviços com a segurança dos seus ativos de informação e com a privacidade dos titulares cujos dados estejam em poder da empresa durante todo o seu ciclo de vida na organização.

COMPROMETIMENTO DA ALTA DIREÇÃO

A diretoria executiva está de acordo com as diretrizes definidas nesta política e tomará todas as ações necessárias e cabíveis para que ela seja aplicada com sucesso.

COMPROMETIMENTO DA EQUIPE DE TRABALHO

Todos estão cientes de que a aplicação de uma política de segurança da informação e privacidade é feita de comportamentos diários e de pequenos detalhes com o objetivo de garantir o melhor funcionamento da empresa e a segurança e a privacidade de toda a equipe. Desta forma, é compromisso assumido por todos seguí-la, adequar seus processos de trabalho a suas diretrizes e zelar para que ela seja cumprida, reportando imediatamente qualquer situação que a comprometa.

CONTROLE E SANÇÕES

O uso dos ativos da AQUA GESTORA, de acordo com a legislação vigente, poderá ser monitorado pela empresa para verificar sua adequação a esta política de segurança da informação e privacidade.

Infrações às diretrizes aqui estabelecidas estão sujeitas a sanções, que serão aplicadas pela diretoria executiva de acordo com o estabelecido pelas leis e pelos contratos assinados entre as

partes. Estas sanções serão aplicadas sem prejuízo de outras ações legais que, eventualmente, precisem ser tomadas pela empresa em decorrência das infrações.

TERMOS E DEFINIÇÕES

Ativo: Tudo o que tem valor para a AQUA GESTORA.

Ativos de informação: Todos os ativos tangíveis e intangíveis da AQUA GESTORA que estão relacionados à informação. Os ativos podem ser a informação propriamente dita, o *hardware* onde ela é processada, o *software* que a processa, as redes de comunicação utilizadas, os locais onde estes ativos estão localizados e os recursos humanos envolvidos.

Ciclo de vida da informação: Todas as fases pelas quais a informação passa dentro dos processos de negócio da AQUA GESTORA (produção, distribuição, armazenamento, processamento, transporte, consulta e destruição) e da infraestrutura (sistemas e redes) que a processa (análise, projeto, desenvolvimento, implantação, exploração e manutenção).

Classificação do ativo: É a indicação da importância do ativo dentro do Sistema de Gestão de Privacidade da Informação (SGPI).

Comitê Gestor do SGPI: É o órgão colegiado responsável pelo sistema de gestão de privacidade da informação.

Controle: É toda forma de gerenciar o risco a que está submetido um ativo.

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável.

Incidente de privacidade: Todo evento que, de alguma forma, constitua uma violação da política de segurança da informação e privacidade e envolva dados pessoais.

Incidente de segurança da informação: Todo evento que, de alguma forma, constitua uma violação da política de segurança da informação e privacidade.

Informação: A informação é um conjunto organizado de dados sobre um determinado fenômeno, entidade ou evento. A informação é o principal ativo da AQUA GESTORA e a base de todos os seus processos de negócio.

Proprietário: É a pessoa responsável pelo ativo de informação perante o SGPI. Ao proprietário cabe classificar o ativo e autorizar o acesso a ele.

Risco: É o efeito das incertezas sobre os objetivos. Expressa o potencial que uma ameaça tem de trazer prejuízos para a AQUA GESTORA. É estimado com base na probabilidade da ameaça se concretizar e no impacto que poderá causar se isso ocorrer.

Segregação de funções: É o princípio de que, onde houver necessidade para o controle mais apurado dos riscos, cada pessoa seja encarregada e possa executar apenas uma parte do processo.

Segurança da informação: É a proteção da informação, garantindo que apenas as pessoas autorizadas tenham acesso a ela (confidencialidade), que esteja disponível quando necessário (disponibilidade) e com seu conteúdo correto (integridade).

Sistema de Gestão de Privacidade da Informação (SGPI): É o conjunto de processos de trabalho que garantem que a empresa tem um controle efetivo e funcional da segurança da informação e da privacidade em seus ativos de informação.

Titular de dado pessoal: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

GESTOR DE SEGURANÇA DA INFORMAÇÃO

Será o encarregado por supervisionar a execução das ações de segurança da informação definidas pela alta direção e implementar os controles e ações necessários para o cumprimento de todas as políticas e procedimentos relacionados ao tema.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Será o encarregado por supervisionar a execução das ações referentes à privacidade no tratamento dos dados pessoais pela AQUA GESTORA, bem como terá o papel de interlocução com os titulares de dados pessoais e com os organismos reguladores.

GESTÃO DE ATIVOS DE INFORMAÇÃO

PROPRIETÁRIO DO ATIVO

Para efeitos de segurança da informação, todo ativo de informação da empresa ou sob sua guarda, independente de sua localização, deve ser inventariado e ter um responsável por ele. Este responsável é denominado proprietário do ativo.

Poderão assumir o papel de proprietário de ativos os diretores e gestores de equipes. Um proprietário poderá ter mais de um ativo sob sua responsabilidade.

O proprietário é o responsável pela forma como este ativo é utilizado, por sua segurança e pelas decisões sobre os riscos que se aplicam a ele. Caberá também ao proprietário autorizar o acesso ao ativo.

CLASSIFICAÇÃO DO ATIVO

A classificação do ativo, para efeitos do Sistema de Gestão da Privacidade da Informação (SGPI), será feita pelo proprietário considerando os seguintes aspectos:

CONFIDENCIALIDADE

Confidencial: Tem caráter sigiloso ou contém dados pessoais e, portanto, deve ter o acesso, obrigatoriamente, controlado, registrado e restrito a pessoas autorizadas.

Restrito: Não tem caráter sigiloso para pessoas internas à empresa e não contém dados pessoais; entretanto, por sua relevância para o negócio, seu acesso deve ser controlado, registrado e restrito a colaboradores da empresa e parceiros de negócios autorizados.

Público: Seu acesso não precisa ser controlado, registrado e não exige a implementação de mecanismos de segurança. Ativos que contenham dados pessoais, como regra geral, não devem receber esta classificação.

CRITICIDADE

Alta: É imprescindível para a operação dos processos de negócios da empresa e, por isso, todas as medidas devem ser tomadas para garantir sua integridade e disponibilidade.

Média: Sua integridade e disponibilidade são importantes para os processos de negócios da empresa, porém não são imprescindíveis para estes processos.

Baixa: Falhas em sua integridade ou disponibilidade não afetam significativamente os processos de negócios da empresa.

CONTROLE DE ACESSO

O acesso aos ativos de informação será feito através de mecanismos de controle de segurança de rede, de sistema operacional ou de aplicação que o restrinjam de acordo com a identificação do usuário e com os direitos a ele concedidos pelo proprietário do ativo.

A identificação dos usuários deverá ser garantida pelo uso de uma senha pessoal e intransferível e, sempre que possível, por um fator adicional de autenticação.

REGISTROS DE ACESSO

Os acessos aos ativos deverão ser registrados para fins de auditoria, monitoração e rastreabilidade. O tempo de retenção destes registros será proposto pelo gestor de segurança da informação ou pelo encarregado pelo tratamento de dados pessoais e aprovado pelo proprietário do ativo de informação de acordo com sua classificação, necessidade de negócio e requisitos contratuais e legais.

CONTINUIDADE DOS NEGÓCIOS

LISTA DE CONTATOS

Para garantir a continuidade das operações da AQUA GESTORA em caso de eventos ou desastres que inviabilizem o acesso a algum de seus ativos, deverá ser mantida uma lista atualizada dos colaboradores que devem ser acionados para executar as ações necessárias e garantir que o funcionamento das operações críticas não seja interrompido.

COMUNICAÇÃO INTERNA

Em caso de um evento ou desastre que inviabilize o acesso a algum ativo da AQUA GESTORA, a comunicação entre os colaboradores será feita, preferencialmente, por telefone. Em caso de impossibilidade no uso deste canal, os planos preliminares serão enviados para a conta de e-mail corporativa dos colaboradores, podendo haver cópia para suas contas pessoais de e-mail.

A coordenação da comunicação interna ficará a cargo do sócio responsável pelas operações da AQUA GESTORA. Em sua ausência ou indisponibilidade, um dos outros sócios assumirá esta função.

COMUNICAÇÃO EXTERNA

Em caso de um evento ou desastre que requeira a comunicação com pessoas ou entidades externas, incluindo investidores, a comunicação deverá ser coordenada pela alta gestão da AQUA GESTORA, que poderá envolver os colaboradores seniores e os conselheiros legais sempre que houver necessidade.

A comunicação deverá ser conduzida por um membro da alta direção ou por alguém designado por ela, ficando vedado aos demais colaboradores o repasse de informações para fora da AQUA GESTORA.

Qualquer comunicação com a imprensa sem prévia autorização está vedada.

INSTALAÇÕES

Em caso de indisponibilidade das instalações da AQUA GESTORA por prazo superior a 07 (sete) dias, período no qual as operações da AQUA GESTORA deverão ser mantidas de forma regular

por meio de trabalho remoto, caberá à alta direção definir uma localidade alternativa para a continuidade das operações ou estabelecer um modelo de trabalho remoto.

Em caso de trabalho remoto, se houver a necessidade, a alta direção poderá autorizar o uso de equipamentos pessoais dos colaboradores (por exemplo, telefones ou computadores) para acesso às informações da AQUA GESTORA. Neste caso, caberá ao Gestor de Segurança da Informação e ao Encarregado pelo Tratamento de Dados Pessoais garantir as condições necessárias para que a confidencialidade, integridade, disponibilidade e privacidade dos ativos de informação sejam resguardados.

O acesso a partir dos equipamentos pessoais dos colaboradores deve ser interrompido assim que possível e quaisquer informações neles armazenadas deverão ser repassadas à AQUA GESTORA e apagadas.

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

TIME DE RESPOSTA A INCIDENTES

O time de resposta a incidentes é o grupo de pessoas responsáveis por tratar os incidentes de segurança da informação e privacidade. Fazem parte deste time:

- Representante da alta direção da AQUA GESTORA
- Gestor de Segurança da Informação
- Encarregado pelo Tratamento de Dados Pessoais
- Responsável pela operação e suporte de TI
- Responsável pelo Departamento Jurídico

Este time se subordinará diretamente à alta direção da AQUA GESTORA.

MONITORAÇÃO

O ambiente de tecnologia da AQUA GESTORA será monitorado através de ferramentas automáticas que identificarão e alertarão sobre:

- Acessos administrativos
- Alterações de direitos e permissões
- Tentativas de invasão
- Uso de direitos privilegiados
- Instalações de aplicativos e mudanças de configurações
- Acessos diretos a bases de dados ou a dados pessoais
- Ações incomuns ou fora dos padrões regulares

Estes alertas serão repassados aos responsáveis pela operação e suporte ao ambiente de tecnologia para investigação e, se necessário, haverá o acionamento do time de resposta a incidentes.

TRATAMENTO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Os incidentes de segurança da informação e privacidade reportados por colaboradores da empresa ou identificados pela monitoração serão tratados pelo time de resposta a incidentes de acordo com os processos que serão estabelecidos.

GESTÃO DE RISCOS

RISCOS DE SEGURANÇA DA INFORMAÇÃO

O gestor de segurança da informação será responsável por conduzir, anualmente, um levantamento das ameaças aos ativos de informação da AQUA GESTORA e os riscos decorrentes delas. O resultado desta análise, na forma de um relatório de avaliação de riscos, deverá ser apresentado à alta direção da AQUA GESTORA, que será responsável por aprovar o relatório e decidir sobre a execução das medidas sugeridas para o controle dos riscos.

As medidas aprovadas serão implementadas nas condições e prazos estabelecidos pela alta direção da AQUA GESTORA e seu acompanhamento, juntamente com o registro das aprovações, servirão de base para os processos seguintes de avaliação de riscos.

SEGURANÇA FÍSICA E DO AMBIENTE

ACESSO FÍSICO AO AMBIENTE

O acesso aos ambientes da AQUA GESTORA será restrito e deverá ser controlado, podendo ser concedido nas seguintes modalidades:

Acesso permanente: é concedido aos colaboradores de forma permanente, pessoal e intransferível e permite acesso ao espaço físico e às áreas de trabalho da AQUA GESTORA.

Acesso de prestadores de serviço: é concedido em caráter temporário a prestadores de serviços, com acesso ao espaço físico e às áreas de trabalho da AQUA GESTORA de acordo com as necessidades do trabalho a ser desenvolvido.

Acesso de visitantes: é concedido durante o período da visita, com acesso restrito ao ambiente (preferencialmente, com acesso apenas a salas de reunião).

O acesso às salas de computadores, *data centers*, salas de instalações elétricas, salas de bancos de bateria e outras dependências essenciais para a infraestrutura da AQUA GESTORA devem ser restritos às equipes de suporte autorizadas.

ACESSO DE VISITANTES AO ESCRITÓRIO

O visitante deverá, obrigatoriamente, ser recebido por uma pessoa da equipe da AQUA GESTORA e conduzido para uma sala de reuniões, preferencialmente sem passar pelos ambientes internos de trabalho. Nenhum visitante deve transitar desacompanhado pelas dependências da empresa.

Caso o visitante tenha necessidade de acessar o ambiente interno de trabalho, a equipe deverá ser avisada previamente para poder retirar eventuais informações confidenciais ou restritas de locais onde possam ser vistas pelo visitante. Também neste caso, deve-se garantir que o visitante não esteja desacompanhado.

ACESSO DE TERCEIROS À INFRAESTRUTURA DE TI

O acesso de visitantes à internet deverá ser feito através de uma rede isolada das redes internas da AQUA GESTORA.

Caso algum parceiro externo ou prestador de serviços precise acessar os sistemas internos da AQUA GESTORA, o acesso deverá ser feito com por meio de usuário e senha temporários,

concedidos mediante aprovação do proprietário do ativo a ser acessado, e devem ser supervisionado por alguém da equipe da empresa. As credenciais de acesso devem ser revogadas imediatamente após o uso.

A retirada de qualquer ativo de informação da empresa por um visitante deverá ser autorizada por escrito por seu proprietário e reportada ao Gestor de Segurança da Informação e, se houver dados pessoais envolvidos, ao Encarregado pelo Tratamento de Dados Pessoais.

MESA LIMPA

Deve-se evitar imprimir ou anotar em papéis informações confidenciais ou de uso restrito. Havendo esta necessidade, devem ser armazenadas em local seguro (como, por exemplo, armários e gavetas com chave) e nunca deixadas sem supervisão sobre a mesa, bancadas ou nas impressoras.

Documentos contendo informações confidenciais ou restritas devem ser picotados para descarte e não devem, em nenhuma hipótese, ser reciclados.

Os equipamentos da AQUA GESTORA devem estar configurados para bloquear suas telas automaticamente quando ficarem sem uso por 10 minutos, evitando que informações confidenciais ou restritas sejam acessadas em equipamentos que estejam desassistidos quando os usuários se afastam temporariamente.

PROTEÇÃO CONTRA INCÊNDIOS

A AQUA GESTORA terá uma brigada de incêndio ou indicará representante para a brigada de incêndio do condomínio em que estiver instalada, participará das ações de treinamento necessárias e terá os dispositivos recomendados em suas instalações.

GERENCIAMENTO DE OPERAÇÕES E COMUNICAÇÕES

SEGURANÇA DE REDE

As redes de comunicação de dados, internas ou externas, serão utilizadas pela AQUA GESTORA de forma a garantir a segurança das informações que trafeguem por elas:

- As redes *wireless* internas serão protegidas por criptografia e senha;
- O acesso à rede local será protegido por usuário e senha;
- Os acessos à internet e outras redes externas serão controlados por *firewalls*;
- Dados que necessitam de proteção deverão trafegar criptografados pela internet;
- Todos os equipamentos deverão receber configurações de segurança adequadas aos ativos de informação que processam;
- A contratação de prestadores de serviço de rede levará em conta os requisitos de segurança da informação e os níveis de serviço aceitáveis.

FORNECEDORES DE INFRAESTRUTURA

Fornecedores de infraestrutura que hospedam ativos de informação da AQUA GESTORA deverão atender a requisitos de segurança da informação e privacidade equivalentes ou superiores aos apresentados nesta política.

AMBIENTES OPERACIONAIS

Os ativos da informação, de acordo com sua utilização nos processos de trabalho da AQUA GESTORA, estarão instalados em um dos seguintes ambientes:

Produção: Ambiente sob responsabilidade da equipe de TI, nas instalações da AQUA GESTORA ou nos provedores de infraestrutura contratados, onde estão instalados os sistemas que atendem aos processos de negócios da empresa.

Homologação: Ambiente sob responsabilidade da equipe de TI, com características similares ao ambiente de Produção (porém, em escala reduzida), onde a equipe de TI e os usuários podem fazer testes de novas funcionalidades ou mesmo de novos sistemas antes de sua implantação.

Desenvolvimento: Ambiente próprio ou de terceiros onde é feito o desenvolvimento de novos sistemas ou de funcionalidades que serão adicionadas a sistemas existentes.

SEGURANÇA DOS AMBIENTES

Apenas a equipe de TI responsável pela operação dos equipamentos terá acessos com privilégios administrativos aos servidores e equipamentos de infraestrutura dos ambientes de Produção e Homologação.

Se estiverem nas instalações da AQUA GESTORA, os servidores, equipamentos de infraestrutura e equipamentos utilizados para a gestão dos ambientes de Produção e Homologação deverão ficar em salas separadas, com acesso controlado e restrito.

END USER COMPUTING

Todos os dispositivos de acesso aos ativos de informação usados na empresa deverão estar protegidos contra *software* malicioso (vírus, *spyware*, *ransomware* e outros) por sistemas de antivírus. O acesso a eles deverá estar restrito por usuário e senha aos colaboradores que necessitam deles para o exercício de suas funções.

Os equipamentos usarão *software* que garanta funcionalidade de volumes protegidos ou deverão ter seus discos rígidos criptografados.

A utilização de portas USB e de unidades externas de gravação poderá ser autorizada para as finalidades de trabalho e o usuário é responsável pelo uso que faz deles. Como regra geral, dados confidenciais e restritos não devem ser copiados para estes dispositivos e, quando isto for absolutamente necessário, devem ser criptografados e protegidos por senhas. O uso destes recursos está sujeito a monitoração.

A gravação de informações em nuvem deve ser restrita às soluções autorizadas pela AQUA GESTORA. Não devem usadas outras soluções e, a critério da alta direção da AQUA GESTORA, o acesso a tais soluções pode ser bloqueado.

Todos os sistemas usados na empresa devem ser licenciados corretamente ou de uso livre. Documentos e arquivos protegidos por direitos autorais devem ser adquiridos de forma regular ou devem ter seu uso autorizado pelos detentores dos direitos. São expressamente proibidos a baixa e o armazenamento de qualquer conteúdo considerado ilegal nas jurisdições em que a AQUA GESTORA atuar.

DESCARTE SEGURO

A equipe de TI será responsável pelo descarte seguro dos equipamentos usados pela AQUA GESTORA.

Todos os dispositivos descartados que contenham unidades de armazenamento de informações, ainda que sejam destinados a doação, deverão ter seus dados previamente apagados. Deverão ser utilizados aplicativos que fazem a remoção dos dados de forma segura, impedindo que sejam recuperados posteriormente.

TRABALHO REMOTO

O acesso remoto aos ativos de informação da AQUA GESTORA deverá seguir as seguintes regras:

- Deverão ser usados apenas dispositivos sob gestão da equipe de TI da AQUA GESTORA;
- O acesso está sujeito às regras de controle de acesso da AQUA GESTORA;
- Deve-se evitar o acesso a informações da AQUA GESTORA por meio de redes públicas, como aeroportos, bares, restaurantes ou outros;
- É proibido o armazenamento de informações confidenciais ou restritas da AQUA GESTORA em equipamentos que não estejam sob gestão da equipe de TI da empresa;
- Ao final do contrato de trabalho, todos os direitos de acesso dos colaboradores devem ser retirados e os dispositivos da empresa devem ser recolhidos.

GESTÃO DE VULNERABILIDADES TÉCNICAS

A equipe de TI ficará responsável pela aplicação, de maneira tempestiva, de *patches* de correção e atualizações de *software* disponibilizados pelos fabricantes dos sistemas utilizados pela AQUA GESTORA, bem como pela manutenção e atualização dos sistemas anti *malware*.

Nenhuma versão de *software* descontinuada ou sem suporte pelo fabricante poderá ser mantida em ambiente de Produção. Qualquer exceção deve ser justificada e autorizada pela alta direção da AQUA GESTORA.

SEGURANÇA EM RECURSOS HUMANOS

CONTRATAÇÃO

Durante o processo de contratação de novos colaboradores, os candidatos deverão ser informados que a AQUA GESTORA tem uma política de segurança da informação e privacidade e que todos os colaboradores devem se comprometer a cumpri-la integralmente.

Uma cópia desta política deverá ser disponibilizada ao colaborador juntamente com seu contrato de trabalho e deverá por ele ser assinada, atestando ciência dos termos aqui contidos.

CONSCIENTIZAÇÃO

Esta política deverá estar disponível em um repositório de fácil acesso para consulta dos usuários.

Colaboradores terceirizados e prestadores de serviços serão informados sobre esta política e deverão comprometer-se a cumpri-la antes de efetuarem qualquer acesso ao ambiente de TI da AQUA GESTORA.

Atualizações e alterações nesta política deverão ser informadas aos colaboradores e prestadores de serviços.

USO RESPONSÁVEL

Os recursos fornecidos pela AQUA GESTORA, como acesso à internet, e-mail corporativo, estações de trabalho e dispositivos móveis, dentre outros, são destinados à utilização nos processos de trabalho e para a condução dos negócios da empresa. Portanto, é vedado seu uso para negócios particulares ou outras atividades que não estejam relacionadas ao desempenho das funções profissionais dos colaboradores.

O uso dos recursos está sujeito a monitoração pela AQUA GESTORA e o mau uso sujeita o usuário a sanções, de acordo com a legislação vigente.

Em caso de roubo ou extravio de equipamentos, o incidente deverá ser registrado tão logo quanto possível junto às autoridades competentes e uma cópia do registro deverá ser encaminhada à equipe de TI para que seja providenciado o bloqueio do acesso aos equipamentos e, quando possível, a remoção das informações nele existentes.

Ao final de seu período de utilização ou da vida útil do equipamento, o recurso deverá ser devolvido para a empresa para seu devido reaproveitamento ou descarte.

USO DE RECURSOS PRÓPRIOS

É vedado o uso de recursos dos próprios colaboradores para a condução de atividades de trabalho ou processos de negócios da AQUA GESTORA, exceto quando previamente autorizado pela alta direção da empresa.

Quando autorizado, o uso destes recursos para acesso aos ativos de informação da AQUA GESTORA estará sujeito a monitoração e deverá seguir as diretrizes estabelecidas por esta política de segurança da informação e privacidade.

APLICABILIDADE, COMPLIANCE, EXCEÇÕES E REVISÃO

APLICABILIDADE

As situações em que as diretrizes deste documento não puderem ser implementadas, por inviabilidade técnica, financeira ou outra razão de força maior, deverão ser justificadas e aprovadas pela alta direção da AQUA GESTORA.

COMPLIANCE

Nos processos de negócios da empresa, no desenho de seus sistemas, nos pontos onde há coleta, tratamento e armazenamento de informações pessoais, devem ser tomados todos os cuidados para que não ocorram alterações indevidas nos dados, modificações acidentais ou vazamento de informações, de modo que se mantenham em compatibilidade com a legislação vigente, em especial com aquelas referentes à privacidade de dados pessoais.

EXCEÇÕES

Qualquer exceção às diretrizes deste documento, bem como a definição sobre aspectos que não estejam contemplados, deverá ser apresentada à alta direção da AQUA GESTORA, a quem caberá a decisão sobre o assunto.

REVISÃO

Este documento deverá ser revisado sempre que houver necessidade, seja como resultado da análise de riscos, do tratamento de incidentes de segurança da informação e privacidade, da implantação de novos ativos de informação ou de mudanças significativas nos processos de negócios da AQUA GESTORA.

CONTROLE DE VERSÕES

Versão	Data	Descrição
0.1	06/07/2021	Versão inicial para revisão da alta direção