Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Qive

POLÍTICA

Geral de Segurança da Informação

Políticas Qive
Informação Pública

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Sumário

03 Apresentação
04 Abrangência
05 Objetivo
06 Definições
07 Introdução
08 Princípios de Segurança da Informação
09 Medidas organizacionais
10 Políticas e normas de Segurança da Informação
11 Treinamentos periódicos
11 Cláusulas contratuais
11 Monitoramento e auditorias
12 Medidas técnicas e operacionais
13 Aquisição, desenvolvimento e manutenção de sistemas da informação
14 Gestão de Incidentes de Segurança da Informação
15 Papéis e responsabilidades
17 Continuidade de negócio
18 Casos omissos e sanções
19 Canal de escuta
20 Ordem de importância
20 Aceite na Política e documentos complementares
22 Revisão da Política
22 Aprovadores

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Apresentação

Estamos comprometidos em desenvolver os maiores esforços para garantir a segurança das nossas informações. Por isso, elaboramos esta Política Geral de Segurança da Informação (“Política”), que traz diretrizes basilares que Você precisa saber quando estiver tratando informações confidenciais ou não, além de estabelecer comportamentos esperados. Alinhado a esta Política, também elaboramos diversas Normas que tratam do tema da Segurança da Informação de maneira específica.

Em um cenário de crescente digitalização e ameaças cibernéticas, a proteção da informação se tornou um aspecto crucial para a sustentabilidade e sucesso de qualquer organização. Por meio desta política, buscamos não apenas proteger a Qive contra ameaças e vulnerabilidades, mas também garantir a continuidade dos negócios e o fortalecimento da confiança junto a clientes, parceiros e outras partes interessadas.

Leia atentamente as orientações aqui previstas, pois contamos com a sua dedicação no entendimento e aplicação das suas diretrizes. Caso tenha qualquer dúvida, entre em contato com a sua gestão ou por meio do infosec@qive.com.br.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Abrangência

Esta Política é aplicável a todas as pessoas que possuam relacionamento com a Qive ou estejam agindo em nosso nome, sejam elas sócias, diretoras, executivas, investidoras, membros do conselho, empregadas, colaboradores, prestadores de serviços ou fornecedores (“Você” ou “Qiver”).

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Objetivo

Esta Política tem por propósito estabelecer orientações e Normas de Segurança da Informação que permitam a Você adotar padrões de comportamento seguro, adequados às nossas metas e necessidades.

- Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
- Resguardar as nossas informações, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;
- Prevenir possíveis causas de Incidentes e responsabilidade legal da Qive e também dos nossos Qivers, clientes e parceiros;
- Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no nosso negócio como resultado de falhas de segurança.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Definições

Aqui definiremos os principais termos, que, quando escritos com a primeira letra em maiúscula (seja no singular ou no plural), têm os significados a seguir:

Ativo de Informação - Patrimônio intangível, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal, natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a Qive por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela nossa infraestrutura computacional, ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Comitê Gestor de Segurança da Informação – CGSI - Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da Qive, que tem por finalidade tratar questões ligadas a Segurança da Informação.

Gestor da Informação - Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de Segurança da Informação - Evento adverso, suspeito ou confirmado, que comprometa a confidencialidade, integridade ou disponibilidade de informações ou dados pessoais/dados pessoais sensíveis, colocando em risco nossas atividades. Também será considerado Incidente violações à nossa Política Geral de Segurança da Informação.

Risco de Segurança da Informação - Potencial de perda, dano ou comprometimento de ativos de informação devido a ameaças que exploram vulnerabilidades em sistemas, processos ou pessoas. Ele representa a probabilidade e o impacto de um evento negativo que possa afetar a confidencialidade, integridade ou disponibilidade da informação.

Para conhecer mais termos, consulte o Glossário disponível na nossa plataforma de governança.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Introdução

O nosso foco é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à Segurança da Informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos à Qive.

Todos nós estamos comprometidos com uma gestão efetiva, o que inclui a Presidência, a Diretoria Executiva e o Comitê Gestor de Segurança da Informação. Adotam, assim, todas medidas cabíveis para garantir que esta Política seja adequadamente comunicada, entendida e seguida em todos os níveis da Qive.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Princípios de Segurança da Informação

Esta política foi elaborada com base nos três principais princípios da Segurança da Informação, por isso, tenha sempre eles em mente quando estiver lidando com um ativo de informação.

CONFIDENCIALIDADE

O Princípio da Confidencialidade é o que traz **privacidade** às informações. Por meio dele é que garantimos que os dados compartilhados dentro da nossa organização só possam ser acessados por **aqueles legitimados** para tanto.

Esses legitimados podem ser usuários, processos, sistemas, máquinas, entre outros.

INTEGRIDADE

O Princípio da Integridade é o que garante que, durante a transferência de uma informação, ela não sofra com alterações que a violem ou corrompam.

Este princípio é que faz com que todas as características da mensagem original sejam mantidas durante qualquer operação, entre a sua origem e destino. Desse modo, há a garantia de que **os dados não sejam indevidamente alterados.**

DISPONIBILIDADE

O Princípio da Disponibilidade está relacionado à garantia de que a informação esteja **sempre disponível e acessível**, quando requerida, ou seja, permite que usuários autorizados tenham acesso a informações de seus interesses sempre que necessário, para o seu **uso legítimo**.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Medidas organizacionais

Para uma gestão de Segurança da Informação eficaz, é indispensável a junção de medidas organizacionais e técnicas de proteção da informação.

Por isso, adotamos os mais altos níveis de medidas organizacionais para os dados que estão sob nossa responsabilidade. O que inclui, mas não se limita a:

- Políticas e normas corporativas
- Treinamentos periódicos
- Cláusulas contratuais de proteção
- Mapeamentos e auditorias

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Políticas e normas de Segurança da Informação

Criamos uma estrutura de governança corporativa orgânica e adaptável à nossa realidade para que a Segurança da Informação seja, de fato, eficaz. Por meio de plataformas específicas de governança e privacidade, publicamos, implementamos e acompanhamos a aplicabilidade de todas as nossas normas, procedimentos e demais documentos de Segurança da Informação, garantindo que os requisitos básicos de **confidencialidade, integridade** e **disponibilidade** da nossa informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.

Disponibilizamos as nossas políticas, normas e procedimentos também para o público externo, garantindo a educação e conscientização sobre as práticas que adotamos aqui na Qive de Segurança da Informação, reforçando não só os princípios basilares de Segurança da Informação, mas também a confiança com os nossos clientes e demais parceiros de negócio.

Atender os requisitos de Segurança da Informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais é a nossa realidade e também o nosso comprometimento contínuo.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Treinamentos periódicos

Através da nossa plataforma de cibersegurança promovemos uma cultura de segurança corporativa através de diversos tipos de treinamentos, fundamental para a continuidade do nosso negócio.

Cláusulas contratuais

As nossas relações com Qivers, clientes e demais parceiros de negócios é pautada em cláusulas de confidencialidade e proteção de dados em todas as fases da nossa atividade empresarial.

Monitoramento e auditorias

Periodicamente realizamos monitoramentos e auditorias nas atividades da Qive para garantir a segurança das nossas informações.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Medidas técnicas e operacionais

Como adoção de medidas técnicas e operacionais de segurança, são nossas diretrizes:

1. Tratar integralmente Incidentes de Segurança da Informação, garantindo que estes sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas.

2. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

3. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Aquisição, desenvolvimento e manutenção de sistemas da informação

A aquisição de um novo sistema ou aplicação deverá passar por **análise prévia** em relação aos requisitos de segurança e privacidade definidos por nossas normas internas.

Importante lembrar que, em relação ao tratamento dos dados pessoais, a legislação aplicável prevê regulamentação para qualquer meio, físico ou digital. Portanto, dados armazenados em arquivos de papel também estão sujeitos às disposições legais.

A solicitação de uso de novo sistema deve ser feito através de pedido ao time de Infra da Qive. Consulte a sua gestão imediata ou entre em contato através dos nossos canais de comunicação interna para mais informações.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Gestão de Incidentes de Segurança da Informação

Casos de Incidentes de Segurança da Informação e vulnerabilidades associadas aos sistemas de informação da Qive devem ser informadas ao CGSI de maneira imediata por meio do infosec@qive.com.br. Após recebida a notificação, a Qive tomará todas as ações corretivas apropriadas, elaborando relatórios formais de Incidentes e escalonamento serão implementadas.

Também seremos responsáveis por manter equipe qualificada para atender aos Incidentes de segurança e vulnerabilidades com processos, procedimentos e tecnologias para corrigir e prevenir tais eventos. Conduziremos resposta adequada para os Incidentes, envolvendo os times necessários, analisando as causas e impactos, além de registrar e controlar os efeitos de Incidentes relevantes.

Normas complementares são elaboradas para detalhar o tratamento e a resposta em casos de Incidentes de Segurança da Informação. Todos os Qivers, pessoas parceiras, terceiras contratadas e terceirizadas serão informadas dos procedimentos para relatar Incidentes de segurança ou vulnerabilidades que podem ter um impacto na segurança de nossos ativos.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Papéis e responsabilidades

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI

Fica constituído o Comitê Gestor de Segurança da Informação (CGSI), contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das áreas consideradas estratégicas da Qive, com sua composição a ser descrita em norma complementar.

É responsabilidade do CGSI:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à Segurança da Informação
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação.
- Garantir que as atividades de Segurança da Informação sejam executadas em conformidade com esta Política.
- Promover a divulgação desta Política e tomar as ações necessárias para disseminar uma cultura de Segurança da Informação em nossos ambientes.

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

- Conduzir a Gestão e Operação da Segurança da Informação, tendo como base esta Política e demais resoluções do CGSI.
- Elaborar e propor ao CGSI as normas e procedimentos de Segurança da Informação, necessários para o cumprimento desta Política.
- Identificar e avaliar as principais ameaças à Segurança da Informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco.
- Realizar a gestão dos Incidentes de Segurança da Informação, garantindo tratamento adequado.
- Tomar as ações cabíveis para se fazer cumprir os termos desta Política.
- Apoiar o CGSI em suas deliberações.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Papéis e responsabilidades

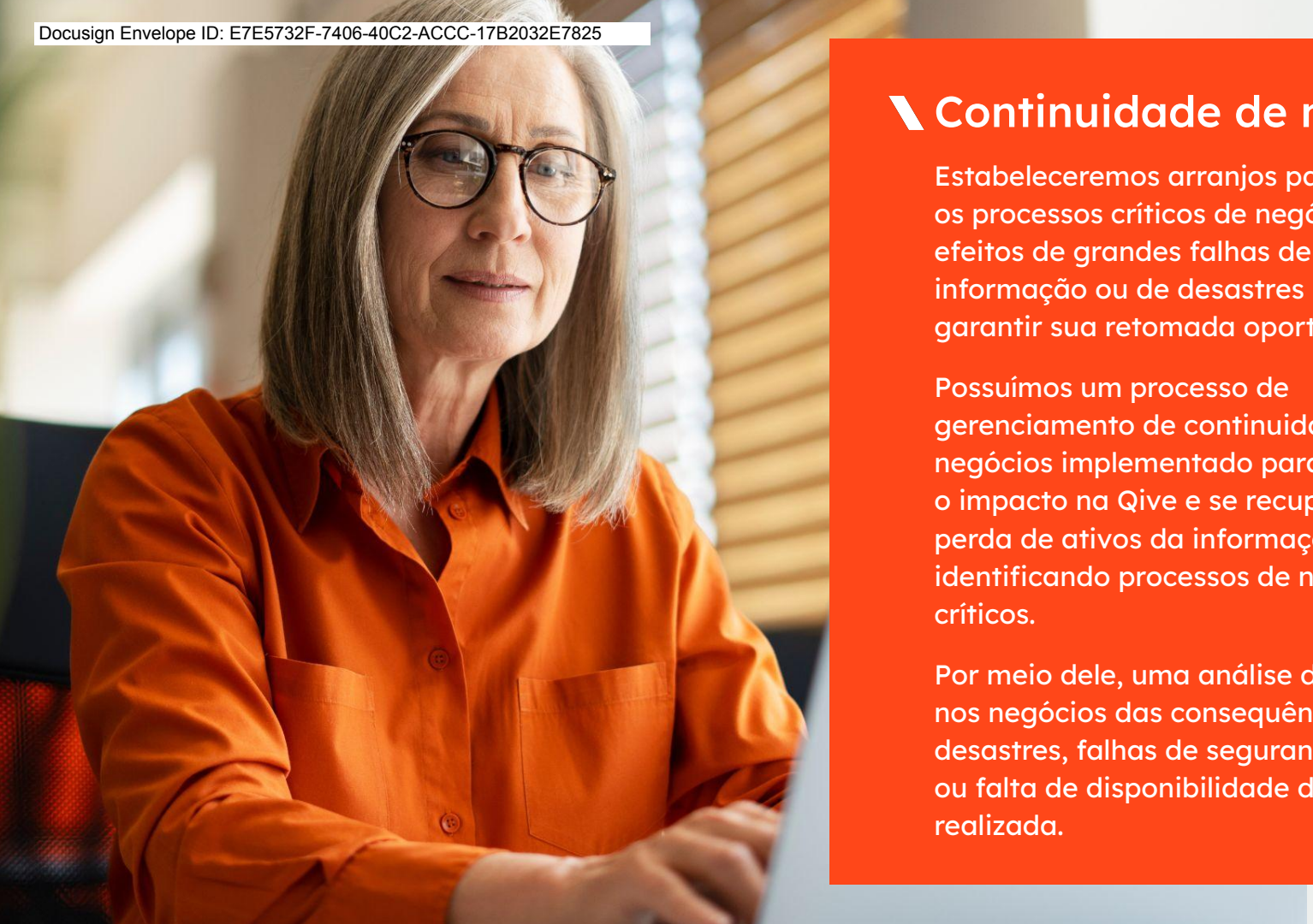
GESTORES DA INFORMAÇÃO

- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as nossas normas.
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme nossas normas, critérios e procedimentos adotados.
- Periodicamente, revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário.
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade.
- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos que adotamos.

USUÁRIOS DA INFORMAÇÃO

- Ler, compreender e cumprir integralmente os termos desta Política, bem como as demais normas e procedimentos de segurança
- Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das nossas informações ou recursos computacionais.
- Encaminhar dúvidas e/ou pedidos de esclarecimento sobre esta Política, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao CGSI.
- Responder pela inobservância desta Política, normas e procedimentos de segurança, conforme definido no item sanções e punições.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825



Continuidade de negócio

Estabeleceremos arranjos para proteger os processos críticos de negócios dos efeitos de grandes falhas de sistema da informação ou de desastres para garantir sua retomada oportuna.

Possuímos um processo de gerenciamento de continuidade de negócios implementado para amenizar o impacto na Qive e se recuperar da perda de ativos da informação, identificando processos de negócio críticos.

Por meio dele, uma análise de impacto nos negócios das consequências de desastres, falhas de segurança, perda ou falta de disponibilidade de serviço é realizada.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Casos omissos e sanções

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação. As diretrizes estabelecidas nesta Política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.

Por isso, **as diretrizes aqui estabelecidas não são as únicas que você deve levar em consideração**. Sempre que possível, adote medidas de segurança adicionais com o objetivo de garantir proteção das nossas informações. Lembre-se, em temas de Segurança da Informação todo cuidado é pouco!

Fique de olho no cumprimento desta Política. Em caso de violações, será analisada a ocorrência e deliberado sobre a efetivação das medidas aplicadas, conforme previsão contratual e na nossa **Norma de Medidas Disciplinares**. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à Qive, **a pessoa infratora será responsabilizada pelos prejuízos, cabendo aplicação das medidas que se fizerem necessárias.**

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Canal de escuta

Possuímos o Canal de Escuta Qive, um meio seguro e confidencial para que Você e/ou outras partes interessadas possam fazer relatos sobre situações que envolvam má conduta, atos ilícitos e até mesmo descumprimento desta Política.

Os relatos feitos dentro da plataforma poderão ser anônimos ou não, e serão avaliados por uma equipe multidisciplinar de Qivers que fará o tratamento preliminar e a investigação adequada.

NÃO RETALIAÇÃO

Rejeitamos qualquer forma de punição, ações disciplinares ou retaliações contra qualquer pessoa que, de boa-fé, denuncie ou apoie na resolução de qualquer problema relacionado à conduta empresarial.

A Qive não tolera nenhuma violação às nossas políticas internas, portanto, caso ocorra, as pessoas envolvidas em alguma violação estarão sujeitas à aplicação de medidas disciplinares internas, e sanções previstas em lei, se necessário. Leia a Política com atenção e replique para seu time.

Se Você presenciar ou souber de qualquer comportamento antiético, ou suspeito, entre em contato imediatamente usando o nosso Canal de Escuta.

Deseja utilizar o Canal de Escuta?

Entre em contato através das nossas ferramentas de comunicação interna ou no canaldeescuta@qive.com.br.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Ordem de importância

Esta Política não pretende e não substitui qualquer lei aplicável ou qualquer termo de um contrato entre a Qive e Você. Em caso de qualquer conflito, prevalecerá a regulação mais restritiva.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Aceite na Política e documentos complementares

Para garantir a conformidade com legislações aplicáveis e a integridade de nossas operações, a Qive poderá criar documentos complementares a esta Política (normas, procedimentos, manuais, dentre outros). Todos ficarão disponíveis em nossa plataforma de governança.

Ao aceitar esta Política, Você declara que:

1. Leu, compreendeu e concorda em cumprir esta Política e todos os eventuais documentos complementares.
2. Compromete-se a consultar regularmente a plataforma de governança da Qive para se manter em atualização constante sobre as orientações vigentes.
3. Participará dos treinamentos relacionados e relatará quaisquer violações ou suspeitas através dos canais internos adequados.
4. Está ciente de que o não cumprimento pode resultar em ações disciplinares conforme as nossas diretrizes internas.

O aceite eletrônico implica na concordância com todos os termos aqui descritos e documentos complementares. Este aceite será registrado em nossos sistemas para fins de conformidade e auditoria.

Para esclarecimentos, utilize os canais de comunicação internos oficiais da Qive ou consulte o Jurídico Qive.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825

Revisão da Política

Avaliaremos, periodicamente, a eficácia da presente Política, realizando a revisão a cada ciclo de 12 (doze) meses, com equipe interna ou por meio de contratação de empresa de auditoria independente. Não havendo necessidade de modificação do seu conteúdo, permanecerá vigente a sua última versão.

Aprovadores

Daniel Chieddi Paschino

5/12/2024

Filipe Mateus Rossi Risso

5/12/2024

Data de Publicação: 12/2024.

Nº da versão: 03.

Docusign Envelope ID: E7E5732F-7406-40C2-ACCC-17B2032E7825