# POLÍTICA DE SEGURANÇA A INFORMAÇÃO E PRIVACIDADE, RESPOSTA A INCIDENTES E ANÁLISE DE VULNERABILIDADES

Rua: Alexandre Dumas, 1671 – Chácara Santo Antônio – 3° Andar – Ala A São Paulo/SP – CEP: 04717-004
www.ciclic.com.br

## 1. OBJETIVO

A presente Política tem como objetivo estabelecer as principais diretrizes, a fim de, garantir a segurança das informações e a privacidade das informações, visando preservar a sua integridade, confidencialidade e disponibilidade, bem como garantir sua legalidade, não repúdio, privacidade e rastreabilidade. Descrevendo, portanto, a conduta mais adequada ao trato das informações de negócios da Ciclic Corretora de Seguros S/A., objetivando sua proteção contra destruição, modificação, divulgação indevida e acessos não autorizados, seja acidental ou intencional, buscando assegurar que somente as pessoas certas tenham acesso às informações necessárias. Sendo aplicável, a todo o ciclo das informações, abrangendo meios eletrônicos e físicos, compreendendo seu processamento, armazenamento, comunicação e descarte. A segurança cibernética, da informação e privacidade diz respeito a todos indistintamente, sejam eles, colaboradores, fornecedores, parceiros e prestadores de serviços, gestores e diretores da Ciclic, sendo de responsabilidade de cada um o seu cumprimento. As informações a serem divulgadas, sejam elas interna ou externa, devem ser cuidadosamente avaliadas, levando em consideração a importância e os possíveis impactos negativos nos negócios da Ciclic, especialmente as que tenham como destinatário o público externo.

## 2. DEFINIÇÕES, CONCEITOS E SIGLAS

A presente Política adotará os seguintes termos, expressões e palavras, de acordo com as definições ora estabelecidas:

- **Colaborador**: são os funcionários da Ciclic, por ele diretamente contratados com base na legislação trabalhista vigente;

- **Prestador de Serviço**: é a pessoa física ou jurídica que, por força de contrato firmado com este objetivo, preste serviços de qualquer natureza à Ciclic;

- **Fornecedor**: é a pessoa física ou jurídica que, por força de contrato firmado com este objetivo, forneça bens ou produtos de qualquer natureza à Ciclic;

- **Cliente**: é a pessoa física ou jurídica que contrata os serviços prestados pela Ciclic;

- **Visitante**: é a pessoa física que não se enquadre em qualquer outra definição é que, por breve período, tenha acesso aos recursos de tecnologia da informação da Ciclic;

- **Usuário**: é o colaborador, prestador de serviço, fornecedor, cliente ou visitante que, por qualquer meio e ainda que momentaneamente, tenha acesso aos recursos de tecnologia de informação da Ciclic;

- **Gestor**: é a pessoa que se posiciona em hierarquia superior aos colaboradores de determinado setor dentro da Ciclic, sendo por ele responsável;

- **Recursos de Tecnologia da Informação (T.I.)**: é o conjunto de bens ou recursos materiais ou imateriais que integra o sistema de tecnologia da informação da Ciclic, tais como os computadores de mesa (desktop) e seus acessórios, os computadores portáteis (tais como notebooks, netbooks, laptops, palmtops, tablets), os servidores de rede, as redes de dados, as redes de telefonia, as redes de conexão à internet, os Sistemas Corporativos, os softwares, os Dispositivos de Armazenamento, os scanners, as impressoras, os aparelhos de áudio e videoconferência, as Mídias Sociais, Nuvens Corporativas e os manuais técnicos, bem como quaisquer outros recursos tecnológicos utilizados para execução das atividades profissionais;

- **Sistemas Corporativos**: são todos os sistemas e aplicativos utilizados, in-loco ou nas nuvens corporativas, no âmbito da Ciclic, para o exercício das atividades profissionais;

- **Correio eletrônico corporativo (e-mail corporativo)**: é o endereço de e-mail corporativo adotado pela Ciclic, devidamente atribuído pelo setor de Tecnologia da Informação;

- **Conta de Usuário**: é a conta utilizada pelos Usuários para acesso aos Sistemas Corporativos, vinculada a um nome de login atribuído individualmente a cada Usuário pelo setor de Tecnologia da Informação e uma senha;

- **Setor de Tecnologia da Informação (Setor de T.I.)**: setor responsável pelo gerenciamento e pela administração dos recursos de tecnologia da informação;

- **Setor de Relacionamento com o Cliente e Comunicação**: é o setor responsável pela criação de soluções de marketing, que satisfaçam o público-alvo da Ciclic, trabalhando para que as informações cheguem ao público supra, de maneira eficiente e direcionada;

- **Mídias Sociais**: são todas as estruturas pertencentes à rede mundial de computadores que permitem o compartilhamento de informações via redes sociais, ferramentas, wikis, blogs, microblogs, sites de compartilhamento de vídeos, entre outras. São exemplos de tais mídias: Facebook, Instagram, Twitter, Snapchat, Blogger, Wordpress, LinkedIn, Youtube, Wikipedia, Flickr; etc.

- **Mídias de Armazenamento**: são os recursos materiais ou eletrônicos utilizados para o armazenamento de informações, incluindo dispositivos eletrônicos como fitas, discos, HDs externos (dispositivos de armazenamento magnético), pen drives (além de outros dispositivos que utilizam memória flash), CDs e DVDs (dispositivos de armazenamento óptico), nuvens corporativas, bem como documentos impressos ou manuscritos;

- **Ativos intangíveis**: são uma grande variedade de informações armazenadas em formato digital, compreendendo documentos, imagens, áudio, vídeo, bancos de dados e outros bens imateriais cujo conteúdo é de titularidade exclusiva da Ciclic;

- **Dados pessoais**: informações relacionadas a uma pessoa natural identificada ou identificável;

- **Tratamento de dados pessoais**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Encarregado pelo Tratamento de Dados Pessoais**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

- **Informações Secretas**: Informações classificadas como “secretas” representam o mais alto nível de criticidade dentro da Ciclic. São informações cujo comprometimento pode causar severos danos financeiros ou de imagem. Seu acesso é limitado a um número restrito de pessoas e o controle sobre o seu uso é o mais elevado. O acesso não autorizado a esse tipo de informação configura violação grave das políticas da organização. Uma informação “secreta", somente pode ser enviada, encaminhada ou divulgada por seu proprietário. Deste modo, caso você receba uma informação classificada como “secreta” você não pode divulgá-la, qualquer que seja o meio. Devem ser restritas ao ambiente da Ciclic;

- **Informações Confidenciais**: São informações cuja divulgação ou perda pode ocasionar desequilíbrio operacional, perdas financeiras de magnitude moderada, perda de confiabilidade de clientes externos, ou até mesmo conferir vantagens aos concorrentes. O acesso a esses sistemas e informações é feito de acordo com estrita necessidade, ou seja, os colaboradores somente recebem autorização de acesso necessário ao desempenho de suas funções na instituição e sua circulação geralmente é departamental;

- **Informações Internas**: Estas informações são de uso interno da Ciclic, não devendo ser enviadas para fora da instituição. Na eventual ocorrência de comprometimento deste tipo de informação, não é esperado impacto crítico, no entanto, pode repercutir em danos à imagem da instituição ou causar prejuízos indiretos e não desejáveis. É esperado que uma informação “interna” circule livremente entre departamentos da instituição sem prejuízos;

- **Informações Públicas**: Informações que não possuem restrições podendo ser divulgadas para o público em geral, incluindo clientes, fornecedores, imprensa. Entretanto, toda divulgação de informação e classificação como pública deve estar autorizada pela diretoria da Ciclic;

- **Incidente de Segurança da Informação e Privacidade**: é indicado por um ou vários eventos de segurança da informação e privacidade, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança das informações;

- **Fragilidades em Sistemas ou Serviços**: são vulnerabilidades encontradas em softwares e aplicativos que podem ser exploradas por ameaças colocando em risco a confidencialidade, disponibilidade e integridade das informações;

- **Departamento de Segurança da Informação e Privacidade (S.I.)**: é o departamento responsável pelo gerenciamento e pela administração dos recursos de segurança cibernética, da informação e privacidade da Ciclic;

- **Encarregado pelo tratamento de dados pessoais (DPO)**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Função exercida pelo gestor do Departamento de Segurança da Informação e Privacidade;

**3. ABRANGÊNCIA**

A presente Política estabelece diretrizes e normas cujo principal objetivo é a proteção das informações que estão armazenadas ou que circulam no âmbito dos Recursos de T.I., buscando resguardá-las de acesso lógico não autorizado, da ação de vírus de computador, de erros ou omissões em sua utilização, de uso indevido, do extravio ou vazamento de informações, de sabotagem, de falhas de hardware e da indisponibilidade de serviços ou informações.

**4. PRINCÍPIOS**

A Ciclic concede a disponibilidade da informação a seus colaboradores, no momento e local que este determinar conforme autorização do gestor direto, objetivando a plena execução de suas atividades. Da mesma forma, aplica-se todos os esforços para que referidas informações sejam confiáveis, corretas e mantidas fora do alcance de pessoas não autorizadas. Estas premissas reafirmam, os princípios da segurança da informação e privacidade adotados pela Ciclic, sendo pautadas nos seguintes pilares:

a. **Autenticidade:** o controle de autenticidade está associado à identificação de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos.

b. **Confidencialidade:** consiste em proteger as informações contra acessos indesejados, para leitura ou cópia, por alguém não autorizado, seja interna ou externamente. A informação deve ser protegida qualquer que seja a mídia que a contenha, seja mídia impressa ou digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso das redes de computadores, isto significa que os dados, enquanto em trânsito, não serão acessados, interceptados, modificados, interrompidos ou personificados por pessoas não autorizadas.

c. **Integridade:** consiste em evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros, fitas magnéticas etc. Esta integridade é pré-requisito para que o sistema seja inviolável, visando garantir a confidencialidade de arquivos e informações.

d. **Disponibilidade**: consiste na proteção dos serviços prestados pelo sistema, garantindo que eles não sejam degradados, nem se tornem indisponíveis, assegurando ao usuário o acesso aos dados sempre que precisar. Atacar a disponibilidade significa viabilizar a negação do acesso a um serviço ou informação. A área de Infraestrutura do Setor de Tecnologia da Informação da Ciclic visa a manutenção dos acessos às informações almejadas e necessárias, fazendo com que toda a informação chegue aos usuários em tempo hábil e de forma íntegra e confiável.

## 5. PAPÉIS E RESPONSABILIDADES

Os papéis e as responsabilidades inerentes a presente Política, são distribuídos entre diferentes níveis hierárquicos da seguinte forma:

### 5.1 **DIRETORIA:**

I. Patrocinar a Política de Segurança Cibernética, da Informação e Privacidade, objetivando o envolvimento e o incentivo necessários para manter as boas práticas nos processos de definição, aprovação e execução das diretrizes de gestão;
II. Aprovar a estrutura organizacional para a Política de Segurança Cibernética, da Informação e Privacidade, bem como diretrizes, políticas e estratégias de atuação;
III. Endossar o nível de tolerância ao risco definido, por meio do conhecimento dos riscos a que estão passíveis as linhas de negócios da Instituição;
IV. Garantir o cumprimento das exigências dos órgãos reguladores;
V. Avaliar, no mínimo anualmente, os relatórios que permitam identificar e corrigir tempestivamente as deficiências de controle tecnológicos;
VI. Comprometer-se com a Política de Segurança Cibernética, da Informação e Privacidade, assim como assegurar a alocação dos recursos tecnológicos e humanos necessários para o bom funcionamento de sua estrutura;
VII. Garantir que todos os processos críticos tenham seus riscos cibernéticos identificados, avaliados, monitorados e controlados; e
VIII. Apoiar na implementação da estratégia da Política de Segurança Cibernética, da Informação e Privacidade na organização, com funções específicas, responsabilidades claramente definidas e instrumentos apropriados que possibilitem a identificação, a avaliação, o monitoramento, a comunicação e o controle do risco.

**5.2 ÁREA DE T.I. - SEGURANÇA CIBERNÉTICA DAS INFORMAÇÕES E PRIVACIDADE**

I. Garantir a manutenção adequada do presente documento e todos os seus derivados, em base de periodicidade minimamente anual;
II. Fazer cumprir todas as determinações do presente documento;
III. Responsabilizar formalmente todos aqueles que obstruíram, prejudicarem ou não cooperarem com a plena e integral execução do presente documento, independentemente de cargo formal dentro da organização;
IV. Promover anualmente a devida conscientização de todos os níveis da Ciclic Corretora quanto ao teor integral do presente documento;
V. Atender a auditorias internas e externas no tocante de todos os assuntos tratados no presente documento;
VI. Promover o desenvolvimento, aprovação, publicação e treinamento de todos os documentos e processos necessários para que se façam cumprir todas as determinações do presente documento;
VII. Manter e divulgar ao público um documento contendo, em linhas gerais, as determinações do presente documento;
VIII. Assegurar que a Política de Segurança Cibernética, da Informação e Privacidade seja difundida de forma ampla e completa entre todos os funcionários e prestadores de serviços terceirizados;
IX. Garantir o cumprimento das exigências dos órgãos reguladores; X. Ser responsável pela implementação da estratégia da Política de Segurança Cibernética, da Informação e Privacidade na organização, com funções específicas, responsabilidades claramente definidas e instrumentos apropriados que possibilitem a identificação, a avaliação, o monitoramento, a comunicação e o controle do risco;
X. Estabelecer padrões e procedimentos de Segurança Cibernética e da Informação, em conformidade com as recomendações dos órgãos reguladores; XII. Avaliar, monitorar, documentar e informar à alta administração, ao diretor responsável e às unidades de negócios da organização sobre a Política de Segurança Cibernética, da Informação e Privacidade;
XI. Gerar e enviar tempestivamente relatórios com informações e análises sobre os Incidentes de Segurança Cibernética com conclusões e providências adotadas para a diretoria da Ciclic;
XII. Avaliar a necessidade de obtenção de novas ferramentas condizentes com as análises de riscos;
XIII. Atender às demandas dos órgãos reguladores, bem como em face às auditorias externa e interna assegurando que a estratégia adotada esteja de acordo à conformidade exigida;
XIV. Atuar em conjunto com a área de Controles Internos e Compliance e contar com aconselhamento jurídico, quando necessário; e
XV. Encarregado de cuidar das questões referentes à privacidade e proteção dos dados da organização e de seus clientes. Atuando para: A. Entender o ciclo de vida dos dados pessoais, instruindo o responsável pelo tratamento para que as atividades relacionadas estejam em conformidade; B. Reportar do tratamento e das conclusões e instruções sobre os riscos envolvidos em caso de inadequação. Tanto com a organização, a autoridade nacional responsável e os titulares dos dados, atuando como canal de interlocução com estes entes, devendo zelar para que o acesso a ele seja facilitado, de forma gratuita, clara e pública nos meios de comunicação do agente de tratamento. C. Coordenar a elaboração do relatório de impacto à proteção de dados pessoais.

**5.2 ÁREA DE CONTROLES INTERNOS E COMPLIANCE**

I. Apoio à área de Segurança da Informação e Privacidade na identificação e devida classificação de riscos, de acordo com o apetite de risco da Ciclic;
II. Avaliar o teor integral do presente documento, a fim de validar e auxiliar sua eficácia na tratativa e mitigação de riscos para a Ciclic.
III. Avaliar o teor integral do presente documento, a fim de sinalizar quaisquer inconsistências que representem ou venham a representar
IV. Apoio à área de Segurança da Informação e Privacidade nas questões jurídicas (com auxílio do escritório externo ou interno, a critério e conforme possibilidade e conveniência da ciclic) relativas à privacidade, Compliance, regulamentações e leis.

**5.3 ÁREA DE RECURSOS HUMANOS**

I. Informar aos responsáveis pelo gerenciamento das credenciais sobre as mudanças nos acessos dos colaboradores em caso de alterações de função ou demissão;
II. Indicar necessidade de capacitação em segurança de novos colaboradores; e
III. Comunicar imediatamente qualquer problema ou riscos relacionados à segurança da informação e privacidade para a área de Segurança da Informação e Privacidade da Ciclic.

**5.4 USUÁRIOS**

Os Usuários deverão utilizar os Recursos de T.I. para fins estritamente profissionais, sempre em conformidade com as políticas da Ciclic, com a moral e com a lei. Os Usuários deverão tomar os devidos cuidados para que, as informações que circulam ou que estejam armazenadas no âmbito dos Recursos de T.I, sejam acessadas somente por quem tenha autorização para tanto.

**5.5 PRESTADORES DE SERVIÇOS E FORNECEDORES**

Os prestadores de serviços, fornecedores e qualquer outra parte externa relacionada à organização, sejam das áreas operacionais ou administrativas, devem manter a disponibilidade, confidencialidade e integridade das informações, resguardando-as contra perdas, danos e acessos indevidos, da seguinte forma:

I. Definindo processos que garantam que os acessos lógicos e físicos à todas as informações da empresa sejam realizadas de acordo com os padrões estabelecidos pela Ciclic, que incluem requisição, aprovação, autorização e limitação de acesso aos recursos, de acordo com as necessidades que a função do colaborador determina;
II. Garantindo que todos os sistemas e computadores, serviços, processos e recursos utilizados estão em acordo com as políticas e padrões estabelecidos neste documento, observando as práticas de segurança adotadas pela corporação;
III. Identificando riscos relacionados à segurança das informações tratadas, através da implantação de controles que possam minimizá-los ou eliminá-los;
IV. Permitindo auditorias periódicas conduzidas pela área de Segurança da Informação e Privacidade da Ciclic, com apoio de entidade externa especializada ou não. Estas auditorias podem ou não ocorrer, de acordo com os níveis de risco identificados pela Ciclic e de acordo com requisitos legais;

V. Observando e praticando as atuais políticas e procedimentos de segurança;
VI. Adquirindo somente softwares e hardwares previamente homologados pela área de Tecnologia da Informação, considerando-se aspectos de compatibilidade, padronização, performance, segurança, suporte, entre outros. Além disso, tais tecnologias devem estar de acordo com os requisitos de negócio da corporação;
VII. Respeitando os procedimentos e políticas de acessos físicos e lógicos aos recursos;
VIII. Comunicando imediatamente qualquer problema ou riscos relacionados à segurança da informação e privacidade para a área de Segurança da Informação e Privacidade da Ciclic;
IX. Utilizando encriptação de dados e certificados digitais para transferência de informações, sejam elas internas ou externas, homologados previamente pela área de Segurança da Informação e Privacidade;
X. Acessos de prestadores de serviços devem ser renovados periodicamente, através de solicitação do gestor, o qual deve informar o período a ser mantido o acesso. O período máximo de renovação de acessos para prestadores de serviços é de 90 dias corridos;
XI. Ao término das atividades do prestador de serviços, o gestor é responsável por notificar imediatamente a área responsável pelo controle de acessos, utilizando os recursos adotados formalmente pela corporação (sistema, formulário, e-mail), tornando-se diretamente responsável por qualquer acesso indevido que venha a ocorrer entre o período de desligamento e a solicitação de cancelamento;
XII. Equipamentos não pertencentes a Ciclic, por exemplo, desktops ou notebooks de prestadores de serviços e visitantes, ou qualquer outro equipamento, devem possuir autorização formal prévia do respectivo Gerente ou superior da área em questão, bem como de segurança da informação e privacidade para serem conectados à rede da Ciclic, devendo ser configurados de acordo com os padrões de segurança adotados pela organização; e
XIII. Estando alerta para o fato de que todas as transações, comunicações, software e hardware utilizados na corporação são passíveis de auditorias (internas e externas), as quais visam garantir os níveis de segurança adequados e se estão sendo aplicados ao uso dos recursos.

**5.6 DAS VEDAÇÕES**

É vedado a todos que tenham acesso aos Recursos de Tecnologia da Informação da Ciclic, sem exceção, utilizar-se dos Recursos de T.I. para o acesso, a visualização, a divulgação, a transmissão ou o armazenamento de qualquer tipo de conteúdo ou informação que possa se enquadrar nas seguintes hipóteses:

I. Conteúdo que possa ser considerado inadequado, imoral ou ilegal;
II. Conteúdo que contenha ou faça referência a qualquer forma de discriminação, ao racismo, à pedofilia, à pornografia, à prática de crimes, à incitação à violência, ou a informações falsas, caluniosas, injuriosas ou difamatórias;
III. Conteúdo que viole a propriedade intelectual de terceiros, notadamente direitos de patentes ou marcas, segredos industriais, regras de licenciamento de softwares ou direitos autorais, ou ainda que configurem concorrência desleal ou outros crimes tipificados na Lei de Propriedade Industrial e na Lei de Direito Autoral;
IV. Conteúdo que caracterize a produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador que tenham como objetivo invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter,

adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita;

V. Conteúdo que caracterize a produção, oferta, distribuição, venda ou difusão de códigos ou programas de computador que tenham como objetivo interromper serviço telemático ou de informação de utilidade pública, ou impedir e dificultar seu restabelecimento (vírus, worms, cavalos de tróia, malware , etc.);

VI. Qualquer outro tipo de conteúdo de caráter malicioso que possa ser caracterizado como vírus, worms, cavalos de tróia ou programa que permitam o controle de outros computadores;

VII. Conteúdo que caracterize spam de propagandas de quaisquer produtos ou assemelhados;

VIII. Conteúdo que desmereça as opiniões e os posicionamentos oficiais adotados pela Ciclic.

Caso o Usuário se depare com qualquer dos conteúdos supramencionados, deverá imediatamente, notificar a instituição através de e-mail ou pelo canal de denúncias disponível no site da CICLIC. Ato contínuo, o usuário não poderá, em nenhuma hipótese, adotar condutas que pretendam burlar os mecanismos de segurança adotados no âmbito dos Recursos de T.I.

**6. MONITORAMENTO E CONTROLE**

A Ciclic reserva para si o direito de monitorar e de interferir no uso dos Recursos de T.I., com o propósito de verificar o cumprimento dos padrões de segurança estabelecidos pela Política de Segurança Cibernética, da Informação e Privacidade, sempre que julgar necessário. Ainda, sempre que possível, a Ciclic armazenará os dados e os registros relativos a todas as atividades realizadas por cada Conta de Usuário, dentro dos Recursos de T.I. As trilhas de auditoria implementadas nas aplicações desenvolvidas ou utilizadas no âmbito da Ciclic, conterá os seguintes dados, sempre que possível:

i. Sistema ou aplicação utilizada pelo Usuário;

ii. Dados da Conta de Usuário utilizada para acesso;

iii. Data e hora de acesso ao sistema ou aplicação;

iv. Especificação da operação realizada pelo usuário. As trilhas de auditoria, permitirá a completa rastreabilidade do processo de tratamento de dados, na infraestrutura de Tecnologia da Informação da Ciclic, feito por qualquer um de seus usuários.

**7. CULTURA, TREINAMENTO E CONSCIENTIZAÇÃO**

Todos os colaboradores, sejam eles contratados ou temporários, que sejam novos na Ciclic ou que tenham passado por uma mudança significativa em suas responsabilidades de trabalho, deverão receber dentro do prazo de 30 (trinta) dias corridos, treinamento acerca dos aspectos da segurança da informação e privacidade relativas às suas funções, a ser realizado pela área de Segurança da Informação, com base na presente Política e nos demais documentos de suporte, que se aplicável. Ainda, todos colaboradores serão submetidos anualmente a um programa de treinamento em segurança da informação e privacidade, com base no inteiro teor desta Política e em todos os demais normativos da instituição, que se façam necessários. Todo treinamento relacionado a segurança da informação e privacidade deve contemplar todos os pontos necessários para as atividades de cada participante. Na dúvida, a presente Política deve ser utilizada como base.

## 8. GESTÃO DA CONTINUIDADE DE NEGÓCIOS

Os processos críticos de negócio da Ciclic deverão ser cobertos por um Plano de Continuidade de Negócios, o qual contempla os cenários de incidente, identificados por todas as áreas da Ciclic, em especial pela área de Tecnologia e informação e privacidade (segurança cibernética), o qual deverá ser aprovado pela Diretoria. O Plano de Continuidade de Negócios é submetido a testes de eficiência e eficácia, no mínimo, uma vez ao ano, e seus resultados são armazenados e utilizados para o aperfeiçoamento dos processos. Cenários de incidentes relacionados à indisponibilidade de sistemas de informação, que suportam os processos críticos de negócio, são registrados e gerenciados de acordo com o Plano de Ação e Resposta aos Incidentes, como o descrito no Anexo I, assim como em outros processos e documentos que se façam necessários.

A Ciclic deverá consolidar todas as informações necessárias de todos os ativos de informação, para o atendimento às práticas de Continuidade de Negócios. Os processos críticos da organização possuem redundância off-site, sujeita a testes parciais semestrais, e testes integrais anuais. Todas as informações críticas do negócio estão sujeitas a cópias de segurança diárias, armazenadas em ambientes que atendem a todos os requisitos de segurança do presente documento.

A Ciclic mantém um plano de backup (cópia de segurança), revisado e atualizado anualmente, contemplando requisitos específicos para cada tipo de informação.

## 9. GESTÃO DE RISCOS CIBERNÉTICOS

A identificação, o registro e a notificação quanto à suspeita e confirmação de riscos cibernéticos, são feitas diretamente à área de Segurança da Informação e Privacidade, que consolida, trata, comunica e acompanha todos os riscos, com as demais áreas da instituição.

O registro de riscos contém, minimamente, as informações quanto à descrição do risco, sua origem, natureza, possíveis impactos correntes e residuais, tratamento utilizado, resultado da aplicação do tratamento, responsável pela identificação e datação, responsável pela revisão e atuação no tratamento. A Ciclic implanta internamente mecanismos, serviços e ferramentas para identificação de vulnerabilidades em seus sistemas de informação e todos os demais meios utilizados para utilizar, transferir e armazenar dados e informações da organização, de seus clientes, fornecedores e parceiros.

Todo os meios de uso, tráfego e armazenamento de dados e informações possui mecanismos de monitoramento e rastreamento, garantindo a visibilidade necessária para identificação de riscos em curso ou em vias de, assim como para proporcionar o nível de granularidade de informações necessário para medidas posteriores a um possível incidente. Os riscos cibernéticos são classificados e tratados de acordo com as diretrizes e especificações dos demais documentos de suporte derivados e/ou suportados pelo presente documento.

Todo profissional com acesso, físico ou não, às informações e dados da Ciclic ou que estejam sob custódia deste, devem assinar, obrigatoriamente, o Termo de Responsabilidade e Confidencialidade (NDA) para resguardar a organização de eventuais riscos relacionados.

Todo ativo de informação da Ciclic deve, obrigatoriamente, possuir rótulo de classificação de informação. Em caso de ocorrência ou suspeita de incidente envolvendo segurança da informação e/ou dados pessoais, ele deverá ser imediatamente reportado, nos termos da presente Política.

## 10. GESTÃO DE ACESSOS

### 10.1 DISPOSIÇÕES GERAIS

Os acessos ao ambiente e às informações da Ciclic são previamente autorizados e segregados de acordo com a necessidade de cada profissional, para a execução das atividades, sob sua responsabilidade. A área de T.I. e S.I. atribui a cada um dos Usuários, uma Conta de Usuário, no qual, deverá ser utilizada exclusivamente para fins profissionais. Para cada usuário, devidamente identificado e individualizado, poderá, somente ser atribuída uma única Conta para acesso aos Sistemas Corporativos. Em caráter excepcional, a T.I. e S.I. poderá criar contas de aplicações ou sistemas, isto é, que podem ser acessadas por aplicações ou sistemas diferentes. Cada uma dessas contas ficará sob a responsabilidade do gestor da área ou do gestor da informação que a utilizar. As credenciais de acesso, tanto físicas quanto digitais, são de uso pessoal e intransferível, e sua divulgação e compartilhamento são considerados violação direta das políticas da Ciclic.

**Cada usuário é responsável pela correta utilização dos acessos concedidos, bem como zelar por eles, a fim de não causar impactos negativos ao negócio da instituição. Todo acesso, antes de ser concedido, deve ser formalmente solicitado e aprovado pelo gestor do usuário solicitante, e, pelo proprietário da informação, à qual o acesso foi solicitado**. Devendo ser restrito, ao estritamente necessário para o atendimento às responsabilidades do beneficiado. A aprovação do acesso à informação, dado ou sistema de informação gera evidência do ato e deve atender a todos os requisitos deste e dos demais documentos em vigor na Ciclic. Na hipótese, de ocorrer transferência de colaboradores entre áreas distintas, todos os acessos devem ser revisados, para refletir a nova realidade de responsabilidade, bem como, a autorização de acesso à informação e aos dados da organização.

O ambiente possui controles que garantem, que todos os acessos de colaboradores desligados, bem como, quaisquer acessos de prestadores de serviços, sejam bloqueados imediatamente, após o encerramento do vínculo com a Ciclic. Todo o ambiente tecnológico (lógico e físico) da Ciclic possui mecanismos de controle de proteção de perímetro para impedir acesso não autorizado. Estes mecanismos de controle proporcionam rastreabilidade e lastro entre os eventos de acesso.

O uso de credenciais privilegiadas (acesso administrativo) deve ser restrito a situações em que, se faça indispensável, o seu uso para a continuidade das operações da Ciclic. Estas credenciais não devem ser de uso comum diário, tampouco de conhecimento de um colaborador. Elas são mantidas em local seguro (atendendo a todas as definições da presente Política), de acesso restrito, tratadas com a classificação “confidencial”.

### 10.2 SENHAS E MÚLTIPLO FATOR DE AUTENTICAÇÃO (MFA)

A senha de acesso ou MFA vinculada à Conta de Usuário tem caráter pessoal e intransferível, sendo vedado ao Usuário revelá-la a quem quer que seja, bem como solicitar a senha ou MFA de outros usuários.

Os Usuários deverão criar senhas que:
I. Sejam fáceis de lembrar e difíceis de serem descobertas por terceiros;
II. Não contenham caracteres idênticos consecutivos ou grupo de caracteres somente numéricos ou alfabéticos;
III. Não sejam baseadas em dados de fácil adivinhação ou obtenção a partir de informações pessoais, tais como nome, sobrenome, datas importantes, placas de carros, números de documentos, entre outras.

São exemplos de senhas seguras aquelas que não contenham mais de 2 (dois) caracteres consecutivos do nome completo do titular da Conta de Usuário e que contenham caracteres das quatro categorias seguintes: I. Caracteres maiúsculos (de “A” a “Z”); II. Caracteres minúsculos (de “a” a “z”); III. Base 10 dígitos (0 a 9); IV. Caracteres não alfabéticos (ex: !, $, #, %).

As senhas criadas para acesso aos sistemas corporativos deverão ser utilizadas exclusivamente para este fim, e nunca em sistemas de outras empresas ou serviços, como e-mails pessoais, redes sociais, internet banking, entre outros. O Usuário deverá se atentar para os locais de guarda das senhas criadas para acesso aos sistemas corporativos, evitando anotá-las e deixá-las expostas a terceiros, assumindo a responsabilidade sobre as mesmas. Sempre que possível deve-se utilizar o múltiplo fator de autenticação (MFA) em todos os recursos tecnológicos e sistemas corporativos que for tecnicamente viável.

### 10.3 BLOQUEIO E DESATIVAÇÃO DE CONTAS DE USUÁRIO

As contas de usuários relativas a usuários que não mantenham mais vínculo com a Ciclic serão desativadas na data e hora do término do vínculo, cabendo à liderança do setor em que ocorreu o desligamento notificar o setor de Recursos Humanos da Ciclic previamente sobre o desligamento se possível para que seja programada o bloqueio dos acessos, caso não seja possível deverá ser notificado imediatamente.

Em caso de desligamento da liderança do setor, caberá ao diretor responsável pela área notificar. Ainda que, por algum motivo, a conta de usuário não tenha sido desativada na data do término do vínculo entre o usuário e a Ciclic, o usuário não poderá utilizá-la para acessar os sistemas corporativos. Em caso de necessidade de bloqueios emergenciais, deverá ser feita a solicitação diretamente ao Setor de S.I.

## 11. CANAIS OFICIAIS DE COMUNICAÇÃO

### 11.1 DISPOSIÇÕES GERAIS

Constituem canais oficiais de comunicação da Ciclic todas as funcionalidades disponibilizadas pelo Slack, bem como o e-mail corporativo. Os Usuários devem fazer uso dos canais oficiais de comunicação sempre que for necessária a transmissão de quaisquer informações relativas às atividades da Ciclic, sendo expressamente vedado o envio por canais alternativos de:

i. Dados pessoais
ii. Informações estratégicas da Ciclic, tais como, mas não limitadas a: informações financeiras, contratuais com terceiros e planos de ação. O Usuário assume a responsabilidade pelas informações por ele compartilhadas ou trafegadas por meio de canais não oficiais de comunicação, por exemplo: e-mail particular e aplicativos de mensagens instantâneas (como o Whatsapp ou Telegram).

**11.2 USO DE CORREIO ELETRÔNICO CORPORATIVO (E-MAIL CORPORATIVO)**

O acesso ao e-mail corporativo é concedido a colaboradores e, ocasionalmente, empresas prestadoras de serviço, como ferramenta de trabalho, sendo proibido o seu uso para outros fins. Todas as mensagens eletrônicas enviadas, recebidas ou armazenadas, através de qualquer meio corporativo da Ciclic, são de propriedade da empresa. E-mails com informações classificadas como CONFIDENCIAIS ou SECRETAS, incluindo seus anexos, devem ser protegidos através de criptografia previamente avaliada pela área de Segurança da Informação e Privacidade. O envio e recebimento de e-mails com conteúdo interno ou confidenciais entre a Ciclic e prestadores de serviços devem observar o processo de criptografia de dados, evitando exposição indevida de informações. É dever do usuário fazer uso adequado da conta de e-mail corporativo que lhe for atribuída, sendo vedado:

i. O envio de mensagens com informações particulares, ou seja, que digam respeito à esfera íntima do Usuário;
ii. O envio de mensagens que contenham arquivos anexados cujo conteúdo não possua relação com as atividades desempenhadas pela Ciclic; que veiculam propagandas, boatos, ou que se enquadrem nas hipóteses previstas nesta Política;
iii. O cadastramento da conta de e-mail corporativo em sites com finalidades particulares (como sites de mídias sociais ou de compra e venda online);
iv. Cabe ao Usuário realizar verificações frequentes em sua conta de e-mail, eliminando arquivos e mensagens desnecessárias à execução das atividades da Ciclic. São de responsabilidade do usuário as mensagens transitadas em sua conta de e-mail corporativo e, no caso de contas genéricas, do Gestor da área.

**12. USO DA INTERNET**

**12.1 DISPOSIÇÕES GERAIS**

O serviço de internet é disponibilizado pela Ciclic exclusivamente para atividades relacionadas aos seus negócios ou ao desenvolvimento profissional de seus colaboradores e prestadores de serviços. O acesso para fins pessoais é tolerado, de forma moderada, sem infringir os interesses da Ciclic, sua Política de Segurança Cibernética, da Informação e Privacidade e a legislação em vigor. A disponibilização do serviço de internet pela Ciclic poderá ser condicionada ao aceite, pelo usuário, dos termos de uso, variantes conforme o público. Os perfis de acesso à Internet são administrados pela área de Segurança da Informação e Privacidade e definidos pelos gestores de cada área, de acordo com as necessidades de negócios. O acesso à Internet a partir de qualquer sistema da Ciclic é validado por filtros de controle de conteúdo, previamente homologados pela área de Segurança da Informação e Privacidade. Poderá ser restringido ou bloqueado o acesso a sites que:

i. Veiculem qualquer tipo de conteúdo ilícito ou imoral;
ii. Apresentem risco de comprometimento da produtividade, tais como sites que demandam alto consumo de banda (streaming, vídeo, peer-to-peer e outros);
iii. Apresentem risco à segurança das informações e privacidade ou dados da Ciclic, possuindo alto índice de disseminação de pragas virtuais;
iv. Permitam a realização de publicações em blogs e mídias sociais pelos Usuários. A Ciclic reserva para si o direito de monitorar o uso de qualquer dado ou informação que trafegue na infraestrutura de Tecnologia da Informação.

O acesso à Internet é de total responsabilidade do colaborador ou empresa prestadora de serviço, sendo estes responsáveis pelas consequências do uso indevido. O Usuário deve conduzir adequadamente o uso da internet, sempre em conformidade com as Políticas da Ciclic e com a legislação vigente.

Os usuários, ao utilizarem a rede de internet da Ciclic, não poderão:

i. Acessar, visualizar, armazenar, divulgar ou repassar qualquer site, portal, página da internet ou material com conteúdo inadequado ou ilegal, tais como aquele que contenha ou faça referência a qualquer forma de discriminação, ao racismo, à pedofilia, à pornografia, à prática de crimes, à incitação à violência, à intelorância religiosa, à posicionamento político, a fatos que não sejam verdadeiros, a fatos ou informações caluniosas, a fatos ou informações injuriosas, a fatos ou informações difamatórias, a fatos ou informações que contrariem a moral e os bons costumes, a fatos ou informações que violem direitos autorais, regras de licenciamento de softwares e direitos relativos à propriedade, à privacidade e à proteção da propriedade industrial;
ii. Armazenar ou trocar dados de conteúdos autorais não autorizados;
iii. Fazer download ou distribuição de quaisquer softwares sem autorização prévia e formal do Setor de T.I.;
iv. Efetuar upload de qualquer software licenciado da Ciclic sem a expressa autorização do Setor de T.I.;
v. Acessar e propagar deliberadamente qualquer tipo de conteúdo malicioso, como vírus, worms, cavalos de tróia ou programas que permitam o controle de outros computadores, bem como spam de propagandas de quaisquer produtos ou assemelhados;
vi. Utilizar ferramentas e/ou serviços de troca de mensagens não autorizadas pelo Setor de T.I.;
vii. Utilizar qualquer ferramenta com o intuito de burlar a segurança dos Recursos de T.I., visando o acesso a sites bloqueados ou o acesso não autorizado à internet;
viii. Publicar, em nome da Ciclic, comentários em mídias sociais, sites, blogs ou qualquer outra rede de relacionamento ou colaboração;
ix. Publicar comentários em mídias sociais, sites, blogs ou qualquer outra rede de relacionamento ou colaboração que relacione a Ciclic a assuntos não condizentes com suas atividades. Aplicações que utilizam comunicação via Internet por outro meio que não seja através do browser homologado pela Ciclic, devem ter análise e aprovação prévia da área de Segurança da Informação e Privacidade. Todas as concessões de acesso devem considerar a imagem e a reputação da organização, interna e externamente.

**13. USO E ADMINISTRAÇÃO DA REDE CORPORATIVA**

As informações corporativas, confidenciais ou não, não podem ser armazenadas em estações de trabalho. Essas informações devem estar armazenadas em diretórios de rede para que tenha acesso controlado e que sejam realizadas cópias de segurança, garantindo confidencialidade e evitando indisponibilidade da informação. Existe processo definido para realização de cópias de segurança (backup) do ambiente tecnológico da Ciclic. O procedimento define como as cópias devem ser realizadas bem como seguir corretamente os procedimentos de backup de dados definidos pela área de Segurança da Informação e Privacidade, procedendo a testes minimamente anuais de recuperação dos dados, todo o armazenado deve ser realizado no formato digital. Somente recursos tecnológicos fornecidos e gerenciados pela Ciclic devem ser utilizados para o armazenamento de

informações corporativas. O uso de dispositivos pessoais (notebooks, smartphones e outros) para a manipulação de informações da empresa poderá ser aprovado em caráter de exceção e mediante aprovação formal do gestor, estando o colaborador ciente de que tal equipamento estará sujeito à monitoração e auditorias a critério da Ciclic., sem prévio aviso.

A Rede Corporativa somente deverá ser utilizada pelos Usuários que tiverem permissão para acessá-la, que estiverem devidamente autenticados em suas respectivas contas de usuário, a partir de aparelhos também autorizados, e para fins estritamente profissionais. O Usuário somente poderá acessar as informações e os arquivos cujo acesso lhe for permitido pelo próprio sistema, por orientações de seu Gestor ou por força das disposições do contrato que o vincula a Ciclic. O Usuário deve usar adequadamente a Rede Corporativa, utilizando-a exclusivamente para a consulta de dados e informações relacionados às atividades da Ciclic, sendo vedada sua utilização para o armazenamento de qualquer conteúdo ilícito, imoral. Qualquer acesso à Rede Corporativa e qualquer atividade nela realizada pelo Usuário poderão ser rastreados pela Ciclic. O acesso remoto à Rede Corporativa somente poderá ocorrer mediante VPN, cujo o acesso deve ser via usuário e senha, além de autenticação em de dois fatores, cuja liberação será realizada pela área de S.I. com a assinatura de termo de responsabilidade pelo Usuário.

## 14. USO E MANUSEIO DE ESTAÇÕES DE TRABALHO, EQUIPAMENTOS E PROGRAMA

### 14.1 DISPOSIÇÕES GERAIS

As normas previstas nesta seção regulam a utilização de todos os equipamentos de informática e softwares integrantes dos Recursos de T.I. não tratados especificamente em outras seções deste documento. A utilização de estações de trabalho ou de equipamentos da Ciclic, conectados ou não à rede de internet ou à rede de dados do mesmo, por qualquer meio, somente deve ser possibilitada ao Usuário devidamente autenticado em sua Conta de Usuário. Os usuários devem fazer uso adequado dos equipamentos de informática (hardware) e programas de computador (software) da Ciclic conforme as seguintes orientações:

I. Para conectar qualquer equipamento de informática (computadores, notebooks, switches, hubs, etc.) na rede de dados ou na rede de internet da Ciclic, o Usuário deverá consultar previamente o Setor de T.I., via solicitação prévia, com a aprovação do Gestor, que autorizará ou não a solicitação, a seu exclusivo critério;
II. O Usuário não poderá alterar as configurações-padrão de hardware e software dos equipamentos;
III. O Usuário não poderá violar os lacres dos computadores e demais equipamentos eletrônicos da Ciclic, a fim de não comprometer a segurança e a garantia destes recursos;
IV. O Usuário não poderá compartilhar pastas ou arquivos dos computadores e demais equipamentos eletrônicos que permitam o armazenamento de informações sem a utilização de senhas de proteção e a definição dos demais Usuários autorizados a acessá-los;
V. O Usuário não poderá utilizar nem instalar softwares não autorizados ou sem licença de uso nas estações de trabalho ou nos equipamentos eletrônicos da Ciclic, tais como: a) Jogos ou softwares de entretenimento; b) Softwares gratuitos, temporários ou compartilhados (freewares ou sharewares) que não se relacionam às atividades da Ciclic e que não sejam autorizados pelo Setor de T.I.; c) Softwares desenvolvidos particularmente por um Usuário e não autorizados pelo Setor de T.I.; d) Softwares distribuídos por meio de revistas ou obtidos (download) via internet; e) Cópias sem

licença de softwares autorizados;

VI. Fica vedado o acesso, o armazenamento ou a troca de dados, por qualquer modalidade, de conteúdo que possa ser enquadrado nas hipóteses do art. 9º deste documento;

VII. Os Usuários não poderão utilizar os equipamentos de informática da Ciclic para fazer envio e/ou armazenamento de arquivos de músicas, filmes e outros tipos de documentos não relacionado com as atividades da Ciclic, salvo mediante expressa autorização prévia;

VIII. Os equipamentos de informática da Ciclic não devem ser utilizados para efetuar envio (upload) de dados e documentos do banco que sejam confidenciais ou reservados, sem a autorização prévia e formal do Gestor ou da pessoa responsável. O Usuário deverá realizar o encerramento da sessão sempre que houver a necessidade de se ausentar de sua estação de trabalho, de forma a evitar acessos indevidos. O Usuário deverá tomar todos os cuidados necessários para a preservação dos Recursos de T.I. que lhe foram confiados, sempre em observância às normas de guarda de patrimônio da Ciclic.

**14.2 USO DOS COMPUTADORES MÓVEIS DISPONIBILIZADOS**

Somente computadores móveis de propriedade da Ciclic e os utilizados por terceiros, nos casos previstos em contrato, que estejam em conformidade com o padrão estipulado pelo Setor de T.I., devem ser utilizados para acesso à rede de dados ou à rede de internet da Ciclic. Os computadores móveis somente devem acessar a rede de dados ou a rede de internet após as devidas validações realizadas pelo Setor de T.I. Os computadores móveis são disponibilizados aos Usuários como uma ferramenta de apoio às atividades profissionais e seu uso deve ser restrito às atividades realizadas no âmbito da Ciclic. O uso dos computadores móveis somente será permitido a Usuários autorizados e autenticados em suas respectivas Contas de Usuário, e se disponível utilizando perfil corporativo no aparelho, e a sua retirada da unidade da Ciclic deverá ser autorizada pelo Setor de T.I. O Usuário que utiliza computadores móveis disponibilizados pela Ciclic deve observar as instruções dos fabricantes para sua proteção e seu manuseio, além das diretrizes, políticas e normativos da Ciclic. Somente poderão ser instalados, nos computadores móveis, softwares, aplicações e plugins que atendam às seguintes regras:

i. Nos notebooks, notebooks e laptops, somente os softwares homologados pelo Setor de T.I

ii. Nos tablets, palmtops e smartphones, softwares do fabricante necessários para o funcionamento do equipamento e seus periféricos e softwares homologados pelo Setor de T.I. Em viagem ou fora do espaço físico da Ciclic, o Usuário deve tomar todos os cuidados para proteger o computador móvel e os dados nele contidos, como não deixá-lo sozinho ou permitir a visualização do seu conteúdo por terceiros. As informações da Ciclic armazenadas nos computadores móveis devem ser protegidas pelo Usuário contra vazamento e alterações não autorizadas. A área de S.I. deve efetuar a configuração do antivírus, quando disponível para o computador móvel, celulares corporativos, ou qualquer outro dispositivo informático, de modo a realizar a atualização automática via internet, quando o Usuário estiver fora do local onde exerce suas atividades profissionais. O uso externo em computador móvel de qualquer mídia removível, tais como cartões de memória, CDs, DVDs, pen drives e HD externo, entre outros, deve ter sua utilização limitada a: I. Cópia de Segurança (backup) de trabalho. II. Transferência de dados vindos de uma fonte externa confiável. É vedado ao Usuário alterar as configurações de rede sem fio. Quando da devolução do computador móvel, o

Usuário deverá entregar todos os acessórios recebidos (fonte de alimentação externa, mouse sem fio, HD externo, etc.).

Quando não estiver em uso, o computador móvel deve ficar armazenado em local seguro. No caso do notebook, o Usuário deve realizar logout com Ctrl + Alt + Delete quando não estiver em uso, e o tablet deve ser protegido obrigatoriamente com senha de acesso.

**14.3 MANUTENÇÃO E MOVIMENTAÇÃO DE EQUIPAMENTOS**

Os serviços de manutenção de equipamentos e acessórios da Ciclic, bem como de softwares, devem ser executados somente pelo Setor de T.I. e prestadores de serviço autorizados. Similarmente, os serviços de movimentação de equipamentos e acessórios da Ciclic devem ser executados somente pelo Setor de T.I. e fornecedores autorizados. Caso, durante a manutenção, seja identificada a existência de softwares não autorizados, o Setor de T.I. comunicará via canais oficiais o fato ao Gestor ao qual o Usuário se vincula, que tomará as medidas cabíveis, conforme disposto neste documento. O Usuário deve acompanhar a realização da manutenção preventiva ou corretiva de uma estação de trabalho sob sua responsabilidade, quando esta for realizada no seu ambiente de trabalho. Antes do descarte de estações de trabalho, de computadores móveis danificados que demandarem substituição definitiva, ou de equipamentos alugados serem devolvidos, o Setor de T.I. deve providenciar a exclusão definitiva das informações neles contidas, tornando impossível sua recuperação.

**14.4 PROIBIÇÕES**

Ficam vedadas aos Usuários que utilizam computadores móveis da Ciclic as seguintes condutas:

I. Emprestar os computadores móveis sem autorização da pessoa competente; II. Deixar o computador móvel desprotegido em local público, no local de trabalho ou em locais de alto risco de furto ou roubo, tais como: carros ou outros meios de transporte, quartos de hotéis, centros de convenção, salas de reunião, rodoviárias, aeroportos, etc;
II. Conectar qualquer recurso ou mídia removível não autorizada pelo Setor de T.I. nas estações de trabalho e computadores móveis;
III. Conectar qualquer estação de trabalho na rede de internet ou na rede de dados da Ciclic sem autorização do Setor de T.I.;
IV. Compartilhar diretórios (pastas) das estações de trabalho com terceiros;
V. Violar os lacres dos equipamentos que integram os Recursos de T.I. da Ciclic;
VI. Acessar, armazenar ou trocar dados que possam se enquadrar nas definições deste documento;
VII. Alterar a configuração padrão de hardware ou software dos equipamentos que estiverem sob seu controle;
VIII. Baixar arquivos não relacionados às atividades desenvolvidas pela Ciclic.

## 15. USO DE MÍDIAS SOCIAIS

### 15.1 DISPOSIÇÕES GERAIS

A Diretoria e o setor de Relacionamento com o Cliente é responsável pela administração dos perfis oficiais da Ciclic, reservando-se o direito de avaliar e responder a todo e qualquer comentário publicado nestes perfis. Se, a qualquer tempo, algum Usuário publicar ou postar conteúdo que envolva o nome ou a imagem da Ciclic, deverá, primeiramente, deixar claro que o conteúdo publicado contém apenas sua opinião pessoal, desvinculada à da Ciclic; e que assume toda a responsabilidade perante à publicação. Recomenda-se que, na situação descrita no artigo anterior, o Usuário inclua em sua postagem ou publicação a seguinte nota: "As ideias contidas nesta publicação são de cunho pessoal e não refletem a opinião da Ciclic". Os Usuários não devem fazer uso das mídias sociais de maneira que comprometa a confidencialidade de dados, imagens, informações sigilosas, segredos comerciais, reputacionais ou de quaisquer ativos de titularidade da Ciclic, sob pena de tal conduta ser considerada prática de concorrência desleal, nos termos do artigo 195 da Lei nº 9.279/96 ("Lei de Propriedade Industrial"), de constituir crime de calúnia, difamação ou injúria, conforme os artigos 138, 139 e 140 do Código Penal, ou de ensejar responsabilização civil, conforme os artigos 186, 187 e 927 do Código Civil. Fica proibida a publicação, a qualquer tempo, de qualquer comunicação envolvendo assuntos internos da Ciclic, tais como informações estratégicas, financeiras, técnicas, administrativas, sem prejuízo de outras, nas Mídias Sociais e outras formas de divulgação pública na internet.

É vedado ao Usuário divulgar informações acerca do trabalho desenvolvido no âmbito da Ciclic ou do seu ambiente de trabalho, além de projetos, resultados e outras informações que tenha acesso em razão do cargo ou função desempenhada. Caso o Usuário tenha interesse em divulgar informações que sejam de potencial interesse do público-alvo da Ciclic, inclusive seus clientes, deverá realizar solicitação de divulgação para análise do Setor de Relacionamento com o Cliente e Comunicação, indicando o conteúdo que deseja ver publicado nos canais oficiais.

Somente é permitida a publicação de imagens ou informações de clientes, colaboradores, prestadores de serviços, fornecedores e visitantes da Ciclic caso haja a autorização prévia e por escrito do mesmo para tanto. É vedado o uso do endereço de e-mail corporativo da Ciclic para fins de cadastramento em Mídias Sociais, websites, fóruns de discussão, sites de ecommerce e serviços de computação em nuvem, salvo quando utilizados pela Ciclic.

### 15.2 MONITORAMENTO DE CONTEÚDOS PUBLICADOS NAS MÍDIAS SOCIAIS

A Ciclic monitora, em tempo real, todos os conteúdos e comentários publicados e compartilhados nas Mídias Sociais que envolvam o seu nome ou sua marca. O resultado do monitoramento permitirá a Ciclic impor sanções, tomando as medidas cabíveis quando necessário, conforme a presente Política de Segurança Cibernética, da Informação e Privacidade e demais normas internas existentes. Não serão toleradas publicações que veiculam o nome da Ciclic a qualquer tipo de conteúdo mencionado da presente Política de Segurança Cibernética, da Informação e Privacidade; que veiculem dados pessoais, sobretudo de clientes, sem a autorização prévia e formal do titular; ou que digam respeito a informações estratégicas e temas sensíveis como racismo, homofobia, intolerância religiosa e qualquer posicionamento político.

## 16. ACESSO REMOTO EXTERNO

### 16.1 DISPOSIÇÕES GERAIS

As normas deste capítulo são aplicáveis aos Usuários que acessem remotamente os Recursos de T.I. da Ciclic. O acesso remoto somente poderá ser concedido aos Usuários nos casos em que o exercício pleno de suas funções assim o exigirem, mediante assinatura de termo de acesso. Perfis de acesso específicos são criados para empresas prestadoras de serviço para que o acesso remoto seja restrito aos ativos essenciais para realização de suas atividades. A solicitação de acesso remoto para uso corporativo requer aprovação prévia do gestor do solicitante, do proprietário da informação envolvida no acesso, e da área de Segurança da Informação e Privacidade.

A Ciclic reserva para si o direito de monitorar e interferir no acesso remoto, com os fins de verificar e de garantir o cumprimento dos padrões mínimos de segurança estabelecidos nesta Política de Segurança Cibernética, da Informação e Privacidade. O acesso remoto somente será permitido se realizado em conformidade com as orientações da área de S.I., que terão como objetivo garantir maior integridade no processo de autenticação do Usuário e proteção ao sistema contra acessos não autorizados.

O direito ao acesso remoto será revogado permanentemente ou temporariamente nas seguintes situações:

I. Desligamento do colaborador;
II. Detecção da não necessidade do acesso remoto;
III. Não observância das regras de acesso remoto;
IV. Inatividade por mais de 180 (cento e oitenta) dias. Caso o usuário necessite novamente do acesso, novo processo de solicitação e aprovação é requerido.

## 17. PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO

### 17.1 DISPOSIÇÕES GERAIS

As normas previstas neste capítulo regulamentam o uso e a proteção dos Recursos de T.I., visando resguardar os equipamentos de acesso físico não autorizado, da ação de vírus, de erros, de omissões e de uso indevido, bem como promover o descarte seguro de dados. Os Recursos de T.I. são de propriedade da Ciclic, não podendo ser extraviados, copiados, pirateados ou armazenados em dispositivos que não sejam de propriedade e utilização da Ciclic. Todo uso e acesso a sistemas críticos devem ser monitorados com o objetivo de detectar atividades não autorizadas.

### 17.2 DESCARTE SEGURO DE MÍDIAS DE ARMAZENAMENTO

As Mídias de Armazenamento devem ser descartadas nos seguintes casos por cada um dos usuários e, nos casos técnicos específicos, pela área de T.I. e Segurança da Informação:

I. Mídias que passaram do prazo de validade ou tornaram-se inutilizáveis por alguma outra razão;
II. Devoluções de dispositivos defeituosos que estejam no prazo de garantia;
III. Discos ópticos com informações que deixaram de ser necessárias;

IV. Papéis com dados obsoletos para a Ciclic, que já não precisam estar impressos ou que são redundantes (ou seja, que estão presentes em outras Mídias de Armazenamento). Os papéis que contenham dados pessoais ou quaisquer outras informações estratégicas da Ciclic deverão ser fragmentados antes de serem descartados, e não poderão ser utilizados como rascunho.

**17.3 SEGURANÇA FÍSICA DAS PORTARIAS**

A concessão de acesso aos prédios das unidades da Ciclic está sujeita a controle. O acesso de colaboradores será permitido através da utilização de crachás. O acesso de Prestadores de Serviços, Fornecedores e Visitantes será permitido somente após cadastro nas portarias, sendo necessário o fornecimento de documento pessoal e de informações sobre o motivo da visita, local de destino e a pessoa responsável por acompanhá-lo no período de permanência nos prédios.

**17.4 ANTIVÍRUS, ANTIMALWARE E PROTEÇÃO DE ENDPOINT**

O Setor de T.I. é responsável por instalar a solução de antivírus, antimalware e proteção de endpoint nos equipamentos móveis, estações de trabalho e servidores da Ciclic, com configuração que permita sua atualização recorrentemente. É de responsabilidade da área de S.I. manter a solução atualizada e as correções de segurança do sistema operacional e equipamentos móveis atualizados. É de responsabilidade da área de S.I. monitorar a existência de softwares não autorizados nas estações de trabalho e equipamentos móveis da Ciclic, removendo-os se identificados.

**18. PROTEÇÃO DOS ATIVOS INTANGÍVEIS**

**18.1 DISPOSIÇÕES GERAIS**

As normas constantes desta seção disciplinam o regime aplicável à propriedade dos Ativos Intangíveis criados pela Ciclic ou pelos colaboradores, fornecedores ou prestadores de serviços enquanto vigentes seus vínculos contratuais com a empresa. Os Ativos Intangíveis resultantes de trabalhos realizados em favor da Ciclic, regulados por acordo ou contrato firmado com colaboradores, fornecedores ou prestadores de serviços, serão de titularidade da Ciclic, exceto se disposto em contrário nos exatos termos do contrato celebrado entre as partes. Ressalvado ajuste em contrário, os Ativos Intangíveis desenvolvidos por colaboradores, fornecedores ou prestadores de serviços da Ciclic, de forma colaborativa ou individual, no decorrer do contrato de trabalho ou vínculo contratual aplicável, e com a utilização de recursos, informações, segredos industriais e de negócios, materiais, instalações ou equipamentos, serão de titularidade e propriedade exclusiva da Ciclic.

**18.2 MEDIDAS PROTETIVAS DOS ATIVOS INTANGÍVEIS**

Estão vedadas as seguintes condutas que são consideradas como potenciais riscos à segurança quanto ao uso de ativos intangíveis da Ciclic:

I. Obter e compartilhar, sem a devida autorização ou necessidade, por meio de canais

não oficiais de comunicação, dados pessoais dos clientes, colaboradores, fornecedores, ou prestadores de serviços da Ciclic, caso não sejam expressamente considerados como de acesso público;

II. Publicar ou divulgar a terceiros informações ainda não confirmadas oficialmente pela Ciclic sobre suas atividades;

III. Publicar, sem a devida autorização prévia e formal, imagens ou vídeos que retratam o ambiente interno da instituição.

IV. Divulgar, por qualquer motivo, informações confidenciais, tais como fórmulas, práticas, processos, designs, instrumentos, padrões ou uma compilação de informações ou dados utilizados por um negócio ou código fonte de aplicativos da Ciclic, projetos, segredos industriais e de negócio ou imagens do circuito interno de monitoramento;

V. Utilizar de maneira não autorizada os Ativos Intangíveis da Ciclic, sem que antecipadamente tenha sido requisitada a devida permissão do setor competente, notadamente quanto a eventuais derivações, adaptações, reproduções ou compartilhamentos em qualquer meio;

VI. Criar páginas, perfis ou qualquer outro tipo de presença online relacionada às marcas da Ciclic, a suas atividades;

VII. Responder em nome da empresa qualquer discussão relacionada às atividades da Ciclic na internet, sem devida autorização.

VIII. Fica vedada a divulgação ou compartilhamento de qualquer informação contida na íntegra da política dos contratos com prestadores de serviços, fornecedores. Caso seja identificado qualquer incidente que possa ser enquadrado nas disposições deste artigo, recomenda-se que seja efetuada imediata comunicação do fato ao Setor de Relacionamento com o Cliente, que tomará as ações necessárias para prosseguir o assunto.

**18.3 CRIPTOGRAFIA**

Informações classificadas como CONFIDENCIAIS devem ser protegidas através de criptografia sempre que forem armazenadas ou transmitidas através de qualquer ambiente onde não houver níveis de segurança adequados. O algoritmo criptográfico utilizado pela Ciclic deve ser aprovado pela área de Segurança da Informação e Privacidade e deve ser mundialmente reconhecido como seguro no mercado. As áreas da Ciclic são responsáveis por buscar orientação da área de Segurança da Informação e Privacidade com relação a qualquer processo de transferência de arquivos (através de e-mail, Internet ou outros meios eletrônicos) para que possam ser orientadas adequadamente quanto ao uso, ou não, de criptografia. Todos os ativos de uso, armazenamento e tráfego de informações e dados, incluindo, dispositivos corporativos móveis, como notebooks, laptops e smartphones, devem utilizar criptografia assimétrica.

**18.4 MEDIDAS PROTETIVAS DOS DADOS PESSOAIS**

No que diz respeito ao tratamento de dados pessoais no âmbito da Ciclic, é proibido:

I. O compartilhamento com pessoas não autorizadas, sobretudo que não integrem a Ciclic;

II. A criação de cópias ou duplicatas de documentos com dados pessoais sem que haja necessidade para tanto, ou sem a autorização do gestor ou pessoa por eles responsável;

III. A utilização para finalidade diversa daquela que justificou a sua coleta;

IV. A divulgação sem autorização expressa do titular;
V. O armazenamento em mídias pessoais, como celulares e tablets de uso particular. O compartilhamento de dados pessoais deve ser realizado através dos canais oficiais de comunicação disponibilizados pela Ciclic. Quando do tratamento de dados pessoais, os Usuários deverão sempre observar os seguintes princípios previstos em lei;
   A. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
   B. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
   C. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; Cabe ao Usuário zelar pela segurança e pelo sigilo dos dados pessoais que lhes são confiados, podendo o mesmo ser responsabilizado por quaisquer danos que venham a ser causados em caso de descumprimento das normas aqui previstas.

**18.5 ARMAZENAMENTO EM NUVEM**

Toda e qualquer informação e dado da Ciclic ou sob sua custódia, que sejam armazenadas na nuvem (cloud), deve atender a todas as diretrizes constantes no presente documento. A seleção do provedor de serviço na nuvem (cloud) deve passar por aprovação obrigatória da área de Segurança da Informação e Privacidade e Diretoria para garantir a aderência do provedor a todas as políticas e normas da Ciclic, assim como ao apetite de risco da organização. O provedor selecionado deve ser submetido a uma auditoria mínima, a ser realizada pela área de Segurança da Informação, antes do início da prestação do serviço, com foco no nível de maturidade e de conformidade do ambiente com as práticas da Ciclic. O acesso a todas as informações e dados da Ciclic dentro do ambiente de nuvem (cloud) contratado deve ser, obrigatoriamente, garantido integralmente e a qualquer momento que a organização julgue necessário. O provedor selecionado tem a obrigação de notificar a Ciclic imediatamente sob quaisquer suspeitas ou confirmações de não-conformidade com as práticas da organização, assim como de possíveis incidentes de segurança cibernética e/ou vazamento de dados pessoais. O provedor selecionado também deve conferir acesso integral por parte da Ciclic a relatórios elaborados por empresas especializadas no tocante dos recursos, controles e procedimentos utilizados na prestação do serviço de nuvem (cloud). Todas as validações, análises, e relatórios devem ser devidamente documentados pela Ciclic e armazenados pelo período mínimo de 5 (cinco) anos.

**19. DESENVOLVIMENTO E AQUISIÇÃO DE SISTEMAS DE INFORMAÇÃO**

Todos os sistemas adquiridos ou desenvolvidos para a Ciclic, seja interna ou externamente, e que suportam ou se relacionam com outras tecnologias que suportam direta ou indiretamente processos críticos de negócio da organização, devem atender às seguintes determinações:

I. Atender a todos os requisitos de segurança determinados no presente documento, assim como em seus documentos e processos derivados.
II. Devem passar por análise de segurança da informação e privacidade, que irá gerar relatório com parecer quanto aos possíveis riscos identificados.

III. A Ciclic deve aprovar formalmente a aceitação ou não dos riscos identificados. Esta aprovação deve ser armazenada pelo período integral de uso do sistema em questão.
IV. Devem ser submetidos, no mínimo, anualmente a avaliações de vulnerabilidades conduzidas por especialistas, com base nas melhores práticas mundiais, com apoio especializado externo, se necessário.
V. Todos os processos e documentos derivados desta política devem ser atualizados para refletir o necessário sobre o sistema em questão.
VI. É obrigatória a manutenção de segregação entre os ambientes de desenvolvimento, produção e homologação, garantindo todos os requisitos desta Política de Segurança.
VII. É de responsabilidade do Setor de T.I. manter sempre exposto de forma fácil o acesso ao relatório de vulnerabilidades e riscos das aplicações.

## 20. NORMA DE GERAÇÃO E PRESERVAÇÃO DE EVIDÊNCIAS

### 20.1 DISPOSIÇÕES GERAIS

Esta seção estabelece procedimentos que regulamentam a notificação, o registro e o tratamento de incidentes cibernéticos e de segurança da informação e privacidade e de fragilidades em sistemas ou serviços identificadas pelos Usuários e que possam ter impactos na segurança dos Recursos de T.I. ou dos Ativos Intangíveis da Ciclic, visando a permitir o controle e a adoção de medidas corretivas em tempo hábil. Todos os Usuários devem, obrigatoriamente, notificar, conforme definido nesta seção, qualquer incidente cibernético e de segurança da informação e privacidade ou fragilidades em sistemas ou serviços da Ciclic, imediatamente após sua identificação ou suspeita de sua identificação.

### 20.2 INCIDENTES CIBERNÉTICO, DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

São considerados exemplos de incidentes cibernéticos, de segurança da informação e privacidade ou fragilidades em sistemas ou serviços que devem ser notificados:

I. Falhas de sistema de informação ou perda de serviços;
II. Código malicioso;
III. DoS (Negação de serviço);
IV. Erros resultantes de dados incompletos ou inconsistentes;
V. Violações de confidencialidade e integridade das informações;
VI. Indisponibilidade das informações;
VII. Uso impróprio de sistemas de informação;
VIII. Perda de serviço, equipamento ou recursos;
IX. Erros humanos;
X. Violações da Política de Segurança da Informação;
XI. Violações de procedimentos de segurança física;
XII. Mudanças não controladas ou não previstas de sistemas;
XIII. Mau funcionamento de software ou hardware;
XIV. Violações de acesso;
XV. Tentativas de invasão física ou lógica;
XVI. Tentativas de fraude;
XVII. Sinistros envolvendo ativos de informação;
XVIII. Vulnerabilidades em softwares ou aplicativos.

Os incidentes de Segurança da Informação deverão ser comunicados ao Gestor da área de sua ocorrência e ao Gestor do Setor de T.I., da maneira mais rápida possível. Ao reportar o incidente de Segurança da Informação, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações das políticas da Ciclic. O Usuário não deve tomar nenhuma ação própria para solucionar o Incidente de Segurança da Informação, mas reportá-lo imediatamente conforme disposto no caput. Os Usuários não devem testar Fragilidades em Sistemas ou Serviços, mas reportar sua suspeita ao Setor de T.I. imediatamente, pois esse teste pode causar danos e ser interpretado como uso impróprio desses sistemas ou serviços. Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser comunicado sobre as medidas tomadas para a solução do incidente. Após a notificação, o Incidente de Segurança da Informação será categorizado (hardware/software), priorizado (urgência/impacto), e investigado pela Gerência do Setor de T.I. Sempre que tomar conhecimento de algum Incidente de Segurança da Informação, o setor ou a pessoa responsável pela informação ou pelo equipamento deverá preservar as informações relacionadas ao incidente, bem como informar a Gerência do Setor de T.I. para que esta tome as providências cabíveis.

### 20.3 INCIDENTES ENVOLVENDO O TRATAMENTO DE DADOS PESSOAIS

São considerados exemplos de Incidentes envolvendo o tratamento de dados pessoais que devem ser notificados:

I. O vazamento de dados pessoais;
II. A suspeita de vazamento de dados pessoais;
III. A invasão ou tentativa de invasão do banco de dados pessoais;
IV. O compartilhamento ou cópia indevidos de dados pessoais;
V. Violações da Política de Segurança da Informação envolvendo dados pessoais. Qualquer incidente envolvendo o tratamento de dados pessoais deverá ser comunicado imediatamente ao Gestor do setor em que ocorreu, e ao Encarregado pelo tratamento de dados pessoais. Ao reportar o incidente envolvendo o tratamento de dados pessoais, o Usuário deve relacionar todos os detalhes, tais como mensagens da tela, comportamento estranho, não conformidade ou violações das políticas da Ciclic. O Usuário não deve tomar nenhuma ação própria para solucionar o Incidente envolvendo o tratamento de dados pessoais, mas reportá-lo imediatamente conforme disposto no caput. Dependendo do grau de confidencialidade e sigilo requerido, o Usuário que enviou a notificação via e-mail pode não ser comunicado sobre as medidas tomadas para a solução do incidente. Em caso de incidentes envolvendo o tratamento de dados pessoais, deverá ser observado o processo de contingenciamento disposto no Anexo I desta Política.

## 21. INFRAÇÕES E PENALIDADES

Na confirmação de não-conformidade com as definições do presente documento, o(s) envolvido(s) deve(m) ser devidamente identificados e todos os detalhes com relação à não-conformidade devem ser imediatamente formalizados e transmitidos através do canal de denúncias da Ciclic. O canal de denúncia deve notificar de imediato o responsável pela Segurança da Informação e a Diretoria, que devem tomar as devidas medidas para apurar o caso e evitar reincidências. Na eventualidade de uma exceção às diretrizes deste documento, necessária para o cumprimento legal das responsabilidades da organização, assim como para a continuidade da entrega dos serviços por ela prestados, caracterizando

um desvio de procedimento. Este anexo deve ser devidamente preenchido e armazenado até o fim do desvio de procedimento ou por 5 (cinco) anos, o que ocorrer primeiro.

A ação, omissão ou conivência de colaboradores, prestadores de serviço, fornecedores ou terceiros que impliquem desobediência ou inobservância das disposições desta Política de Segurança Cibernética, da Informação e Privacidade sujeita o infrator às sanções abaixo descritas:

I. Advertência por escrito;
II. Suspensão não-remunerada, conforme a legislação trabalhista, em se tratando de colaborador;
III. Demissão por justa causa, em se tratando de colaborador;
IV. Rescisão do contrato e aplicação de multas cabíveis, em se tratando de prestadores de serviços e fornecedores. O disposto neste capítulo não substitui a aplicação de sanções cíveis ou penais definidas na legislação pertinente.

## 22. VIGÊNCIA E APROVAÇÃO

A partir de 26 abril de 2024, devendo ser atualizada quando necessário ou a cada 02 (dois)anos.

Esta Normativa foi revisada pelo e aprovada pela Diretoria responsável e está arquivada na sede da Sociedade

**ANEXO I - PLANO DE RESPOSTA A INCIDENTES ENVOLVENDO SEGURANÇA CIBERNÉTICA E O TRATAMENTO DE DADOS PESSOAIS**

Os incidentes devem ser seguir a norma de Plano de Ação e Resposta a Incidentes de Segurança Cibernética. Todos os colaboradores, prestadores de serviços, parceiros e fornecedores da Ciclic possuem o dever de registrar formalmente quaisquer desvios por falha no esquema de segurança e violações das políticas da organização, imediata e exclusivamente, à área de Segurança da Informação e Privacidade e/ou ao Encarregado pelo Tratamento de Dados Pessoais, a depender do tipo de incidente.

A Ciclic deverá ter seus processos de negócios, primordialmente os críticos, cobertos pelo Plano de Ação e Resposta a Incidentes de Segurança Cibernética. O Plano de Ação e Resposta a Incidentes de Segurança Cibernética contempla os diferentes níveis de incidente, ações a serem tomadas antes, durante e após um incidente, assim como todas as diretrizes de cada etapa. O Plano de Ação e Resposta a Incidentes de Segurança Cibernética deve atender a todos os demais documentos da organização e deve ser revisado minimamente uma vez ao ano. Em geral, uma resposta a um incidente envolvendo o vazamento de dados pessoais e informações deve seguir quatro passos: contenção, avaliação, notificação e revisão. Os três primeiros passos (conter, avaliar e notificar) devem ser executados simultaneamente ou em rápida sucessão.

**PASSO 0: CONFIRMAÇÃO**

Uma vez que o colaborador suspeita que um vazamento de dados e/ou informação confidencial tenha ocorrido, ele deve imediatamente alertar seu Gestor, o chefe da Área de Segurança da Informação e Privacidade ou Encarregado de Proteção de Dados. Estes, então, deverão avaliar a situação e confirmar a existência de um incidente a fim de efetivamente iniciar o plano de contingenciamento. Prazo: Até 24 horas (úteis).

**1º PASSO: CONTENÇÃO**

Tendo certeza de que ocorreu um incidente, o Encarregado deve notificar a diretoria para que, juntamente com ele, tome as medidas cabíveis. No documento de notificação, devem constar:

I. Nome e informação de contato do indivíduo que descobriu o incidente;
II. Data e hora da descoberta do incidente;
III. Data, hora e local do incidente, se conhecidos;
IV. tipo de dados pessoais vazados (dados de colaboradores, dados de clientes, dados de terceiros);
V. Breve descrição do ocorrido;
VI. Formato de armazenamento dos dados (papel, eletrônico, ambos);
VII. Que tipo de registros ou mídia o indivíduo acredita estarem envolvidos no vazamento;
VIII. Se o dispositivo ou informação vazada estavam protegidos por senha; IX. se estava criptografada;
IX. Se suspeita que dados pessoais identificados (nome, CPF, usernames e senhas, etc.) e/ou informação confidencial foram expostas;
X. Se suspeita que dados pessoais identificados (nome, CPF, usernames e senhas, etc.) e/ou informação confidencial foram expostas;
XI. Estimativa do volume de dados e/ou informações envolvidos;
XII. Se já foi interrompido ou esgotado, ou se ainda há possibilidade de mais

vazamentos.

Juntos, então, o Encarregado e a área de Segurança da Informação e Privacidade deverão fazer o possível para interromper, reverter ou limitar o vazamento. Por exemplo, interrompendo a prática não autorizada, recuperando registros ou desligando o sistema que foi vazado. Não sendo prático o desligamento do sistema, ou se resultar em perda de evidência, revogar ou mudar os privilégios de acesso aos computadores ou endereçar vulnerabilidades físicas e eletrônicas.

Nesta fase preliminar é vital, a partir das orientações do Encarregado, com apoio jurídico, preservar as evidências em conformidade legal, de modo a identificar a causa e a autoria do vazamento, e/ou que possam permitir à Ciclic endereçar todos os riscos representados aos titulares de dados envolvidos. Prazo: Até 24 horas (úteis).

**2º PASSO: AVALIAÇÃO**

Após a tentativa preliminar de contenção, o Encarregado deverá avaliar se o incidente representa algum risco de prejuízo grave aos titulares dos dados pessoais e à Ciclic. O indivíduo que descobriu o incidente deve estar pronto para atuar junto ao Encarregado nessa avaliação, caso necessário. Caso se confirme o risco potencial de prejuízo aos titulares de dados e à Ciclic, o Encarregado deverá proceder ao terceiro passo do plano de contingenciamento. Não se confirmando tais suspeitas, é possível pular para o quarto passo. O Encarregado deverá analisar as provas, as medidas extrajudiciais ou judiciais a serem tomadas e remeter o seu parecer para o responsável pelo poder diretivo da empresa para aprovação das medidas de enfrentamento sugeridas. Prazo: Até 48 horas

**3º PASSO: NOTIFICAÇÃO**

Dependendo da abrangência do incidente, deverá ser comunicada à autoridade controladora envolvida - como, por exemplo, Ministério Público, a Autoridade Nacional de Proteção de Dados, a respeito do incidente a fim de estabelecer laços de cooperação que podem mitigar possíveis prejuízos e penalidades. Também deverão ser notificados os titulares de dados afetados com o incidente, para que possam tomar as atitudes necessárias para se resguardar e alertar pessoas próximas a eles de eventuais golpes e fraudes. Prazo: Até 72 horas

**4º PASSO: REVISÃO**

O quarto passo envolve a revisão e a catalogação do relatório do incidente pelo Encarregado, área de Segurança da Informação e Privacidade, suporte jurídico (interno ou externo) e demais envolvidos, para a tomada de decisões para prevenir novos vazamentos da mesma natureza.

**ANEXO II - TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DE ID´S PRIVILEGIADOS**

Todos os colaboradores e prestadores de serviços que requeiram acesso especial devem seguir o procedimento atual de solicitação de acesso da Ciclic, ler e assinar o presente termo.
O acesso especial não será concedido aos que, por qualquer motivo, venham a se recusar a assinar esse documento.

Esse termo define que: O acesso especial é caracterizado pela custódia do login (identificador) e a senha correspondente com acessos privilegiados ou total acesso ao ambiente, como por exemplo, o administrador ou root. Quando ocorrer a solicitação de login em dupla custódia, após a entrega dos envelopes correspondentes ao login solicitado, o solicitante tem a responsabilidade de manutenção do sigilo da senha contida nos envelopes e pelo próprio formulário que contém a senha. Qualquer incidente ou revelação da senha decorrente da utilização desse login no período em que o envelope foi aberto até o processo da inclusão de nova senha é de total responsabilidade do solicitante autorizado que abriu o envelope. Não deve ser compartilhada a senha e/ou escrevê-la e/ou deixá-la disponível e de modo visível em nenhuma hipótese.

Os usuários com acesso especial devem ter o conhecimento apropriado para a utilização do login e o acesso especial deve ser utilizado estritamente quando necessário. O usuário com acesso especial não deve utilizar os privilégios para conseguir ou dar acesso a recursos computacionais, ou ainda prover informações do ambiente computacional sem observar as políticas e padrões estabelecidos pela Política Segurança da Informação. Ao utilizar o login com acesso especial, o usuário não deverá executar jogos, programas, scripts, comandos ou qualquer outro software não homologado pela Segurança da Informação ou que causem impacto ao ambiente computacional da Ciclic.

O usuário de login com acesso especial não pode se utilizar de seus privilégios sobre o sistema para ler arquivos ou e-mail de outros usuários da Ciclic, a não ser em casos específicos, previstos pelo Departamento de Segurança da Informação e estritamente autorizados. Durante a utilização do acesso especial, o usuário não deve alterar nenhuma configuração do ambiente, sistema ou aplicações que não estejam diretamente relacionados à atividade descrita no processo de autorização para uso deste login e autorizadas através do processo de controle de mudanças no ambiente Produtivo.

Eu li o termo acima e utilizarei o login de acesso especial de acordo com os termos dispostos e com as demais políticas e normas de segurança existentes nesta empresa que venham a normalizar a utilização do login de acesso especial. Também estou plenamente ciente de que no caso de constatação de má-utilização de quaisquer privilégios do acesso especial e violação de quaisquer normas decorrentes desta utilização, esse acesso privilegiado será suspenso e estarei sujeito às penalidades acordadas na ocasião entre o proprietário do ambiente de Produção e a área de Capital Humano, baseadas em regulamentações jurídicas vigentes.

Local, data.

_____

NOME LEGÍVEL E ASSINATURA