POLÍTICA DE SEGURANÇA

1. Propósito

A Política de Segurança da Informação e Comunicações da Cilia tem como objetivo principal definir as diretrizes estratégicas para as ações relativas à Segurança da Informação e Comunicações, com o intuito de preservar a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações produzidos, adquiridos, armazenados, em trânsito, descartados, de propriedade ou sob controle ou operação da Cilia.

O objetivo das regras sobre Segurança da Informação da Cilia Tecnologia Ltda. é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Esta Política procura estabelecer uma cultura corporativa em Segurança, compatível com o uso aceitável das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades da Empresa.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política está de acordo com as leis, regulamentação e autorregulação aplicáveis e adicionalmente se norteia na resolução do BACEN 4658/18 e as Melhores Práticas de mercado.

Os processos de segurança de dados e da informação devem assegurar:

- A integridade (garantia de que a informação seja mantida em seu estado original, visando protege-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- A disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- A confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas).

2. Escopo

A Política de Segurança da Informação e Comunicações da Cilia aplica-se a:

- Todos os ambientes físicos, incluindo-se a sede, filiais, unidades regionais, unidades de desenvolvimento, centros de processamento e quaisquer outros pertencentes ao patrimônio ou sob a custódia da Cilia.
- Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela Cilia;
- Todos os empregados, estagiários, jovens aprendizes e colaboradores de qualquer natureza jurídica da Cilia.

2.1. Referências Normativas

São referências legais e normativas desta Política:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27005: 2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;

- ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação;
- Resolução do BACEN 4658/18
- ABNT NBR ISO/IEC 31000: 2018 - Gerenciamento de Riscos

3. Princípios

São princípios básicos desta Política:

- A preservação da imagem da empresa e de seus empregados;
- A criação, desenvolvimento e manutenção de cultura de segurança da informação e comunicações;
- Que o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações sejam apropriados e adequados ao valor dos ativos da Cilia, considerando os impactos e a probabilidade de ocorrência de incidentes.
- A preservação da responsabilidade solidária para dados de outras empresas que trafeguem nos ativos da Cilia Tecnologia.

4. Diretrizes Gerais

São diretrizes da Política de Segurança da Informação e Comunicações da Cilia:

4.1 Responsabilidade e Comprometimento

Empregados, estagiários, jovens aprendizes e colaboradores, em qualquer função ou nível hierárquico, são corresponsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários e dos ambientes a que tenham acesso, independente das medidas de segurança implementadas pelos responsáveis da gestão de segurança.

4.2 Gestão de Riscos

A Cilia deve desenvolver um processo de análise, avaliação e tratamento de riscos de segurança, visando a adequada proteção das informações.

4.3 Gestão de Continuidade

A Cilia deve manter um processo abrangente de gestão para identificar ameaças potenciais à Empresa e os possíveis impactos em suas operações, caso estas ameaças se concretizem, sendo capaz de responder estratégica e taticamente a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos e serviços das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

4.4 Tratamento da informação

Informações produzidas, adquiridas, em trânsito, armazenadas, descartadas, de propriedade ou sob custódia da Cilia devem receber o devido tratamento para assegurar a proteção durante todo o seu ciclo de vida.

4.5 Controle de Acesso

O acesso aos ambientes físicos e computacionais da Cilia é controlado e concedido apenas a empregados, colaboradores e visitantes autorizados. As autorizações de acesso devem ser concedidas com base nos princípios da necessidade de conhecer e privilégio mínimo para o desempenho das atividades profissionais.

O acesso pode ser monitorado, registrado ou bloqueado sem prévio aviso.

4.6 Recursos Tecnológicos

A instalação de equipamentos, recursos computacionais, sistemas e serviços para uso na rede ou nas dependências da Cilia é controlada e permitida mediante autorização formal.

4.7 Internet, Intranet e Mensageria

As comunicações por meio eletrônico, o armazenamento de mensagens ou qualquer outra informação produzida no ambiente corporativo são de propriedade da Cilia e, seu conteúdo deve ter tratamento adequado à preservação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade das informações.

Os serviços corporativos de correio eletrônico, mensagens instantâneas, Intranet e Internet devem ter seu uso orientado para as atividades de interesse da Cilia.

O uso do serviço de Internet deve estar em conformidade com perfis pré-definidos.

4.8 Educação e Conscientização

Esta Política e seus documentos agregados devem ser divulgados para criar e manter uma cultura corporativa em Segurança da Informação e Comunicações. De forma a reduzir os riscos à segurança da informação, os empregados e colaboradores devem ser informados quanto ao uso adequado e seguro dos recursos tecnológicos e das informações da Cilia a que tenham acesso.

É responsabilidade dos empregados, estagiários, jovens aprendizes e colaboradores conhecer e cumprir as diretrizes, regras e ações definidas por esta Política, assim como pelas suas normas e procedimentos agregados.

4.9 Aquisição, desenvolvimento e manutenção de sistemas de informação

Os sistemas de informação da Cilia, durante todo o seu ciclo de vida, devem ter sua segurança especificada, analisada e testada, utilizar padrões de interoperabilidade do mercado, e estar em conformidade com os requisitos contratuais e a legislação pertinente em vigor.

4.10 Reporte e Tratamento de Incidentes

Os empregados e colaboradores da Cilia têm a obrigação de reportar imediatamente eventos ou incidentes de segurança que tenham conhecimento ao departamento responsável pelo tratamento e resposta a incidentes de segurança.

Os incidentes de segurança devem ser registrados e receber avaliação e tratamento.

4.11 Auditoria e Conformidade

O cumprimento desta Política e de suas normas e procedimentos agregados devem ser auditados, periodicamente, como forma de identificar, corrigir e/ou prevenir situações inseguras para a Cilia.

As atividades, produtos e serviços desenvolvidos na Cilia devem estar em conformidade com leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

O uso de sistemas, serviços e documentos deve estar em conformidade legal com direitos de propriedade intelectual e, portanto, com termos de licenciamento de instalação e uso.

5. Penalidades

O não cumprimento dos princípios e diretrizes da Política de Segurança da Informação e Comunicações, suas normas e procedimentos agregados, sujeita o infrator às penalidades previstas em lei e nos regulamentos internos da Cilia.

6. Atualização

A Política de Segurança da Informação e Comunicações e o Manual de Segurança da Informação e Comunicações da Cilia devem ser atualizados sempre que necessário ou em um intervalo não superior a 01 (um) ano.

7. Disposições Finais

O detalhamento necessário à implementação desta Política está contido no Manual de Segurança da Informação e Comunicações e da Cilia.

Os casos omissos, as situações especiais e demais diretrizes necessárias à implantação desta Política de Segurança da Informação e Comunicações devem ser analisados e deliberados pelo Coordenador de Segurança da Cilia.

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela Cilia Tecnologia Ltda. pertence à empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. A Cilia Tecnologia Ltda. exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Seguem abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar ao Comitê Gestor da Segurança da Informação (CGSI) os riscos residuais.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, bem como definir e assegurar a segregação das funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Empresa.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Proteger continuamente todos os ativos de informação da Empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Empresa.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Empresa.

- Garantir backup em nuvem, devidamente criptografado com as rotinas de retenção (2 últimas semanas / 1 peça de mês / 1 peça de ano – por 5 anos).
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Empresa, mediante campanhas, treinamentos e outros meios de endomarketing.

8. Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação será composto por ao menos um integrante de cada área da empresa.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que deverá convocar reunião do Comitê Gestor de Segurança da Informação, a qual poderá ser eletrônica, conforme o caso e as circunstâncias do incidente.

O Comitê deverá ser instalado necessariamente com a presença do Responsável pela Segurança da Informação (ou, na sua ausência, seu suplente), a quem caberá a sua coordenação.

As deliberações serão tomadas pelo voto da maioria dos presentes, devendo ser lavrada ata das reuniões, a qual poderá ser sob a forma sumária e arquivada no sistema de gerenciamento de compliance da Empresa.

9. Identificação/avaliação de riscos (risk assessment)

A Empresa periodicamente, no mínimo uma vez ao ano, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pela equipe de TI, o qual deverá ser documentado pelo Responsável pela Segurança da Informação com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Empresa e seus riscos de cibersegurança.

A Empresa poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança da Informação julgue necessário e mediante aprovação do Comitê Gestor de Segurança da Informação. Após a condução do referido processo, o Comitê Gestor de Segurança da Informação deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Empresa, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de Segurança da Informação identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política;
- Vazamento de informações durante tráfego de dados não criptografados.

A Empresa estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade. Todas as informações encontradas nos ambientes da Cilia Tecnologia Ltda. são tratadas como confidenciais e sigilosas.