1. OBJETIVO

Este documento é a Política de Segurança da Informação da Frigol S.A. e tem como finalidade estabelecer as diretrizes, princípios e responsabilidades, além de informar e orientar a todos os envolvidos nos tratamentos de dados da empresa (sejam estes colaboradores, estagiários, terceiros, fornecedores, parceiros e outras partes interessadas nos negócios), como realizar tais tratamentos de forma adequada as diretrizes institucionais.

Esta política foi escrita norteando-se nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida em todo o mundo como um código de prática para a gestão da Segurança da Informação, assim como acorda com as leis vigentes em nosso país.

O objetivo deste documento é assegurar o compromisso de todos envolvidos no tratamento de dados, para que estes sigam as normas seja na manipulação direta destes, em seu armazenamento digital e ou físico, nos controles de acesso a estes, nas ferramentas de monitoramento, podendo estes envolvidos sofrerem medidas punitivas adequadas no caso de não cumprimento destas normas.

1.1 DIRETRIZ DE SEGURANÇA DA INFORMAÇÃO

As informações envolvendo clientes, fornecedores e colaboradores são ativos de suma importância para a Frigol S.A. Por esta razão, desenvolvemos processos sólidos apoiados por tecnologias para assegurar sua confidencialidade, integridade e disponibilidade.

1.2 APLICAÇÃO

Esta política aplica-se a todos os colaboradores e parceiros da Frigol S.A.

1.3 VIGÊNCIA

Esta política tem vigência por tempo indeterminado, até ser revisada pelo Comitê de Privacidade e Segurança da Informação da Frigol S.A. e do departamento de controladoria, com aprovação da diretoria.

1.4 PRAZO DE REVISÃO

A política passará por revisões periódicas a cada 2 anos, ou quando houver quaisquer necessidades de alteração por questões institucionais ou por questões legais.

2. DEFINIÇÕES

2.1 INFORMAÇÃO

Conjunto de dados, que após processamento, manipulação e/ou organização dentro de um contexto, realiza uma modificação quantitativa ou qualitativa no conhecimento do sistema (humano ou máquina) que a recebe.

2.2 SEGURANÇA DA INFORMAÇÃO

Ações e controles realizados com o objetivo de preservar os aspectos de confidencialidade, integridade e disponibilidade das informações dentro das instituições e de seus processos, mantendo assim a autenticidade e conformidade destas informações e de tais processos.

2.3 CONFIDENCIALIDADE

As informações estarão ao acesso dos indivíduos, entidades e ou processos autorizados.

2.4 INTEGRIDADE

As informações devem permanecer integras durante todo seu ciclo de vida, sem que sofram interferências não autorizadas que possam alterá-la, corrompê-las ou danificá-las.

2.5 DISPONIBILIDADE

As pessoas autorizadas deverão acessar à informação e aos ativos correspondentes sempre que necessário.

2.6 CONFORMIDADE

Prática do cumprimento de requisitos, normas e ou diretrizes institucionais e ou legais, adotados pela empresa e que devem ser seguidas por todos os colaboradores e parceiros, ao realizar quaisquer tarefas, processos e ou procedimentos pertinentes a seu trabalho.

2.7 RISCOS DE SEGURANÇA DA INFORMAÇÃO

Vulnerabilidades e ou ameaças que podem possibilitar a ocorrência de uma ação que possa então violar os preceitos da confidencialidade, integridade e disponibilidade das informações.

2.8 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afetem algum dos princípios da tríade da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade das informações).

2.9 ESTRUTURA

Conjunto de ferramentas, bibliotecas, processos e ou conceitos usados como solução de diversas tarefas seja de âmbito técnico e ou gerencial. Traz consigo vários modelos, orientações e guias de como realizar a tarefa em si ou a gestão do processo.

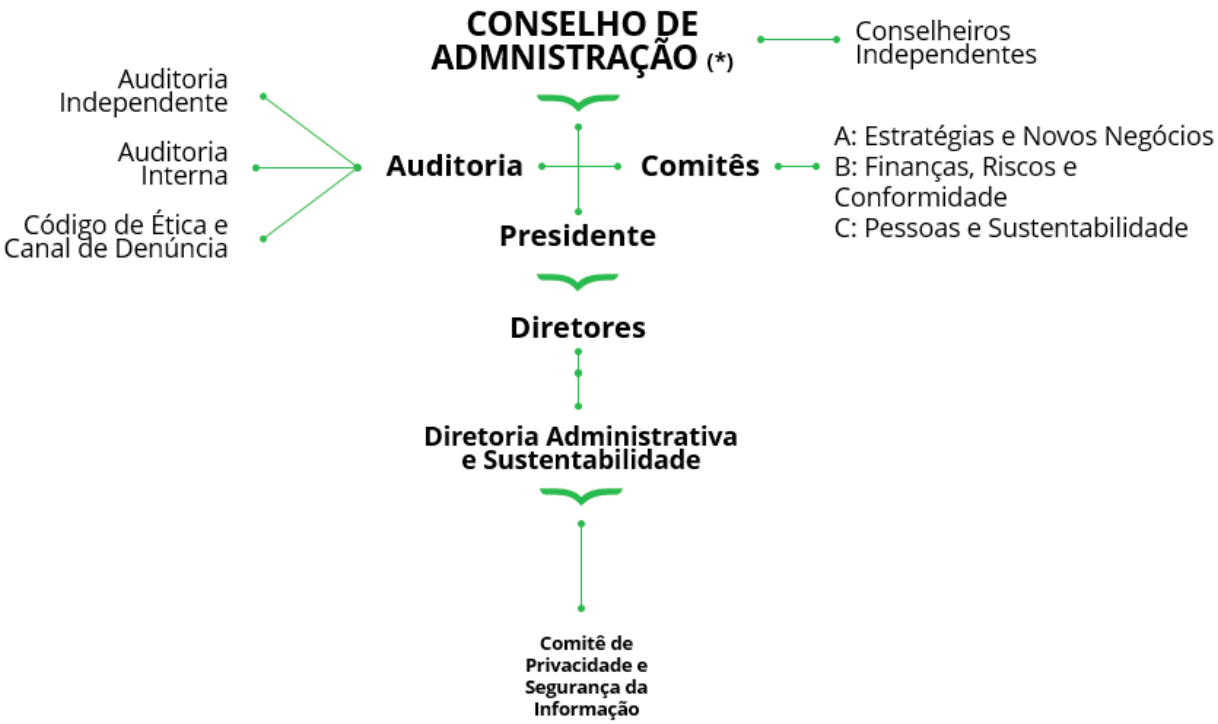
2.10 Comitê de Privacidade e Segurança da Informação da Frigol S.A.

O Comitê de Privacidade e Segurança da Informação da Frigol S.A. é formado por colaboradores que atuam em diversas áreas da empresa e tem a função cada qual de olhar tais áreas ao olhar LGPD (Lei Geral de Proteção de Dados). Estes colaboradores conhecendo e atuando cada qual em seu devido raio de atuação, tendo como objetivo fomentar, implementar e monitorar o cumprimento da LGPD nos mais diversos processos a qual cada uma destas áreas atua.

A formação atual do Comitê de Privacidade e Segurança da Informação da Frigol S.A. é a seguinte:

Camila Lopes: RH
Fernanda Bonanati: Jurídico
Fernando Alberto Topa: TI
Lucas Stradioto: Controladoria
Rafaela Cristina de Sene: Marketing
Tiago de Barros Martins Costa: TI
Wellington Silva: Financeiro
Fabio Telles: Comercial
Ulisses Oliveira: Industria

Este comitê responderá a organização segundo o organograma abaixo:



Para maiores detalhes, os colaboradores devem ler o documento “Política de Privacidade e Proteção de Dados”.

2.11 VISITANTE

Todos os indivíduos que acessem a empresa com intuito de visitação, e que não tenham nenhum tipo de vínculo contratual com a empresa.

2.12 NORMAS DE SEGURANÇA DA INFORMAÇÃO DA FRIGOL S.A.

São as regras, diretrizes e regulamentos da empresa que devem ser seguidos para garantir que as informações estejam protegidas de riscos e ameaças a sua confidencialidade, integridade e disponibilidade. O não cumprimento destas por parte de colaboradores e terceiros pode acarretar punições proporcionais conforme descrito no capítulo oito deste documento.

2.13 PRESTADORES DE SERVIÇOS

Pessoa física ou jurídica que mantenha vínculos com a empresa, seja através de contratos ou parcerias e que participem de um ou mais processos internos ou externos junto as dependências desta.

3. CONTEÚDO

3.1 FUNDAMENTOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1.1 Informação é patrimônio

Todos os dados ou informações elaboradas, adquiridas, manuseadas, armazenadas, transportada e ou descartada nas dependências e ou em ativos das empresas pertencentes da Frigol S.A, é considerada patrimônio desta e deve ser utilizada exclusivamente para os interesses corporativos, respeitando as normas de Segurança e privacidade da Informação.

3.1.2 As informações devem ser classificadas:

Todas as informações que circulam dentro e fora da empresa, carregam dados importantes sobre esta e o uso, alteração ou perda destas podem acarretar perdas consideráveis e até mesmo irreversíveis.

Para manipulação das informações respeitando sua classificação, colaboradores e parceiros devem seguir a política interna devidamente explanada no documento “Política de Classificação de Informações”.

3.1.3 A Responsabilidade e o comprometimento devem ser de todos

Todos os colaboradores, estagiários, e parceiros da empresa, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e manipulação dos ativos e informações de que sejam usuários ou com os quais tenham contato, assim como dos ambientes físicos e computacionais a que tenham acesso.

3.1.4 O acesso à informação deve ser gerenciado

Os acessos físicos ou lógicos das informações devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas.

A privacidade e segurança das informações são de máxima importância para a Frigol S.A. Por isso, a fim de cuidar para que nenhum dado seja acessado sem a devida liberação e para que não haja vazamentos destes da empresa, todos os colaboradores e parceiros devem seguir as políticas de privacidade e segurança, conforme documento “Política de Controles de acesso” e “Política de Privacidade e Proteção de dados”.

3.1.5 O correto uso de e-mails corporativos

Diferentes dos e-mails que utilizamos no dia a dia, o e-mail corporativo leva a imagem da empresa a cada mensagem enviada, por isso devemos utilizá-lo como uma ferramenta de trabalho, com ética, responsabilidade e profissionalismo.

Essencial no dia a dia de muitos setores em praticamente todas as áreas de negócio da empresa, faz-se necessário a criação de diretrizes e procedimentos padronizadas de uso, e tais diretrizes encontram-se no documento “Política de uso de e-mail corporativo”. Esta política deve ser do conhecimento de todos que fazem uso da ferramenta, e deve ser seguida rigorosamente, podendo seu descumprimento acarretar punições conforme capítulo oito.

3.1.6 O correto uso da internet corporativa

Uma das ferramentas mais importantes hoje em todo o mundo é a internet, interligando computadores, pessoas, empresas este recurso trouxe produtos e serviços a todos na porta de suas casas, porém tal conectividade trouxe também muitos riscos. Sendo, no entanto, uma ferramenta indispensável, faz-se necessário realizar o uso desta com todo o cuidado necessário para que seus benefícios não se tornem grandes problemas, ainda mais em empresas.

Por isso, a Frigol S.A. traz no documento “Política de uso de Internet corporativa”, diretrizes, processos e procedimentos padronizados no uso desta ferramenta entre seus colaboradores e parceiros, valendo-se de seus benefícios, mas com os cuidados que esse ambiente exige.

3.1.7 Incidentes de Segurança precisam ser tratados

Os incidentes de segurança devem ser identificados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupções das atividades e não afetando as metas e objetivos estratégicos da empresa.

Na Frigol S.A. temos um plano de resposta a incidentes, times de resposta, ferramentas de monitoramento, Comitê de Privacidade e Segurança da Informação da Frigol S.A. para realizar a avaliação e direcionar a resposta a cada ocorrência. Estes recursos permitirão uma melhor avaliação, rápida erradicação e recuperação dos incidentes, bem como a construção da documentação que será utilizada para as medidas preventivas, aprendendo a cada ocorrência e melhorando continuamente todo o processo.

Para maiores detalhes de como funciona todo o processo de tratativas a incidentes, todos os colaboradores devem consultar o documento “Política de Resposta a Incidentes”, e em caso de problemas e ou dúvidas, todos os colaboradores poderão consultar o time de resposta a incidentes e o Comitê de Privacidade e Segurança da Informação da Frigol S.A. conforme política.

3.1.8 Os ativos devem ser gerenciados

Os ativos de TI são de máxima importância para a Frigol S.A. e para suas estratégias de negócio, sendo essenciais para o cumprimento de nossa missão, visão e valores estratégicos.

Para isso, é imprescindível a todos colaboradores e parceiros o devido entendimento de como utilizar estes da melhor forma, seguindo as melhores práticas de mercado e assim, extrair destes o máximo em qualidade e eficiência, tornando-os facilitadores no cumprimento dos objetivos acima descritos.

Esta política trata os assuntos sobre o planejamento, a aquisição, implantação e gerenciamento de ativos da empresa. Além disso, trataremos o ciclo de vida deste ativo, as diretrizes de uso e conservação, os compromissos de todos no seu uso, principalmente de ativos móveis e removíveis quanto a questão de vazamento, furto e perda de informações contidas nestes.

A disposição dos ativos é estruturada da seguinte forma:

- Ciclo de vida
  - Planejamento
  - Aquisição
  - Implantação
  - Gerenciamento de ativos da empresa
  - Descarte
- Diretrizes de uso
- Diretrizes de conservação

O ciclo de vida é compreendido pela criação do ativo junto a empresa iniciando no planejamento respondendo o porquê adquirir tal ativo, a aquisição em si, sua implantação no local de uso (instalações, treinamentos etc.), seu gerenciamento pela equipe responsável, e ao final de sua vida útil, gerenciar seu correto descarte.

Todos os colaboradores e parceiros devem seguir à risca tais diretrizes que constam em detalhes no documento “Políticas de Ativos de TI”.

3.1.9 As mudanças devem ser gerenciadas

Continuamente ocorrem mudanças nos negócios e procedimentos nas empresas de todo o mundo, estas mudanças são necessárias para sua evolução e crescimento e não as acompanhar pode resultar em perdas irreversíveis. Sendo estas então inevitáveis, é indispensável tomar as devidas precauções e cuidados para que ocorram com o mínimo de impacto possível nos processos e negócios da corporação.

Por isso, todos colaboradores e parceiros devem seguir a política de gerenciamento de mudanças conforme documento “Política de Gestão de Mudanças”.

3.1.10 Procedimentos de Resposta a Incidentes - Frigol S.A.

Por mais cuidados que as empresas tenham, as ameaças cibernéticas atualizam-se em uma velocidade maior que as respostas a estes. Com computadores, laptops, tablets, celulares e tantos outros dispositivos acessando a internet, a exposição de redes internas de uma residência ou de empresas são agravantes. Soma-se a isso, o uso de tantos sistemas diferentes utilizados por estes aparelhos, aplicativos e programas, o que deixa claro que muitas vulnerabilidades não pensadas em seus desenvolvimentos serão exploradas uma hora ou outra.

Parte-se do princípio então que não devemos mais pensar se um ataque irá ocorrer, e sim, quando irá ocorrer. Baseando-se nisso e na importância que a Frigol S.A. tem por seus ativos de informação, criamos o documento “Política de Resposta a Incidentes”, o qual traz as diretrizes, processos e procedimentos padronizados a fim de responder aos incidentes, quando estes ocorrerem, de maneira rápida, ordenada e eficiente, fazendo assim com que os recursos atacados voltem a operar o mais breve possível, vulnerabilidades exploradas sejam extintas, ameaças sejam anuladas e que preventivamente seja mitigado tais ocorrência em nosso ambiente.

3.1.11 A Frigol S.A. audita a conformidade com as práticas de SI e LGPD

A Frigol S.A. audita periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus colaboradores e parceiros em relação ao estabelecido nesta Política e na legislação aplicável.

3.2 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

São os fundamentos que norteiam as ações de implantação e gestão desta política.

3.2.1 Estabelecer a Segurança da Informação em toda a empresa

A Segurança da Informação está presente em nível organizacional em todos os processos da empresa, incluindo os de caráter críticos aos negócios em que está envolvida.

3.2.2 Gestão baseada em riscos

A gestão da Segurança da Informação da Frigol S.A. é baseada e fundamentada em riscos, entendendo que em sua falta ou em caso de falhas, poderá haver perda de vantagem competitiva e de conformidade, falhas com suas responsabilidades civis, interrupções operacionais, danos à reputação e perdas financeiras.

3.2.3 Promover um ambiente positivo de segurança

A Frigol S.A estrutura sua gestão em Segurança da Informação com base na análise e no comportamento humano, treinando, orientando e conscientizando colaboradores e parceiros da

importância do trabalho contínuo de segurança e privacidade das informações, objetivando manter o nível adequando no trato destas.

3.3. ATRIBUIÇÕES E RESPONSABILIDADES

A Frigol, seus Colaboradores e Terceiros devem zelar pela manutenção da segurança das informações, aderindo aos cuidados na manutenção das mesas limpas e no tratamento das informações, independentemente da forma ou meio utilizado, inclusive oralmente.

São permitidos usos de dispositivos móveis como celulares, tablets (dentre outros), para o uso das informações internas, e-mails e WhatsApp, somente após avaliação e aprovação por parte do departamento de Controladoria Corporativa, Tecnologia da Informação, e diretoria. A liberação também somente será realizada após assinatura do Termo de Responsabilidade ao qual será arquivado junto a ficha do colaborador no RH.

Deve notar-se o extremo cuidado e respeito às leis de proteção de dados e a respeito dos comprometimentos de todos colaboradores e parceiros quanto as regras de sigilo sobre as informações transitadas por estes dispositivos, conforme contratos firmados. Além disso, todo o conteúdo presente nos dispositivos pertencentes ou não a Frigol S.A, mas de uso na execução de tarefas relacionadas a empresa como: Aplicações de mensageria (e-mail, WhatsApp, etc.), aplicações de vendas de mercadorias ou de sistemas pertencentes a esta, e devem ser apresentados a empresa sempre que solicitado.

3.3.1 Compete a TI

I. Controlar o acesso à internet em conformidade com Política de Uso de Internet Corporativa;

II. Construir e manter as políticas de segurança da informação e privacidade de dados;

III. Manter a integridade, disponibilidade e confidencialidade dos ativos tecnológicos da Frigol S.A.;

IV. Manter o controle efetivo e validado sobre as permissões de acesso concedidas a Colaboradores e terceiros;

V. Assegurar que as soluções de segurança, tais como proxy, criptografia, backup, antivírus, AntiSpam, estejam operacionais e aderentes aos procedimentos internos, assim como suportando as diretrizes e objetivos listados nesta política;

VI. Controlar o acesso à internet em conformidade com as regras e procedimentos internos de uso da internet;

VII. Manter registros das atividades feitas dentro da organização por meio de: circuito fechado de televisão (CFTV), log de e-mail, acesso físico e lógico, ligações telefônicas de ramais e outras tecnologias que sejam implantadas para a coleta de registros de atividades.

VIII. Planejar, criar, disponibilizar e monitorar ambiente controlado por onde as informações possam ser tratadas, de maneira que garanta a Lei Privacidade da Política de Segurança da Informação em todo o ambiente digital corporativo. O monitoramento irá abranger:
    a. Uso da capacidade instalada da rede e dos equipamentos;
    b. Tempo de resposta no acesso à internet e aos sistemas críticos;
    c. Períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
    d. Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
    e. Atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

f. Atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

IX. Garantir que este ambiente esteja seguro contra ataques e ameaças digitais que possam ferir as normas de privacidade e ou a Política de Segurança da Informação;

X. Organizar controles de segurança no ambiente digital para que apenas as pessoas autorizadas tenham acesso ao conteúdo que necessitam e assim, garantir a disponibilidade, confidencialidade, privacidade e integridade das informações;

XI. Realizar backups do ambiente garantindo a disponibilidade destes em caso de incidentes;

XII. Realizar contramedidas em caso de incidentes que possam comprometer o acesso às informações (Plano de Recuperação de Desastres);

3.3.2 Compete ao Colaborador

I. Cumprir as regras estabelecidas nesta política, assim como as normas e procedimentos de Lei Privacidade da Política de Segurança da Informação, bem como as demais leis, regulamentos e normas aplicáveis pelos órgãos reguladores;
II. Proteger as informações sobre seus cuidados contra acessos indevidos, divulgações não autorizadas e descarte de forma segura;

III. Zelar para que os recursos da empresa sejam utilizados de forma eficaz, dentro de suas finalidades e de conhecimento da empresa. O usuário não deve alterar a configuração do equipamento recebido;

IV. Não expor informações confidenciais da empresa em ambientes públicos ou expostos como transportes individuais ou coletivos, elevadores, restaurantes, dentre outros), ou com terceiros não autorizados;

V. Não compartilhar ou divulgar credenciais de acesso, IDs, senhas, crachás, tokens e similares sem a devida autorização. As senhas são de responsabilidade do usuário, sendo individual e intransferível;

VI. Estar atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área responsável sempre que for necessário;

VII. No caso de necessitar de acessos e autorizações, estas devem ser obrigatoriamente documentadas por processos estabelecidos pela empresa;

VIII. Não criar, adquirir ou realizar uso de softwares não homologados e não autorizados pela área de Tecnologia;

IX. Comunicar a área de Segurança da Informação quaisquer riscos, falhas e incidentes relacionados a Lei Privacidade da Política de Segurança da Informação, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, suspeita de intercepção de mensagens eletrônicas, de acesso indevido e desnecessário a diretórios de rede, acesso indevido à Internet e programas eventualmente instalados sem conhecimento da área de TI;

X. Envolver antecipadamente a área de Tecnologia sempre que houver a intenção de aquisição ou desenvolvimento de quaisquer softwares a serem usados na empresa, para a devida análise de riscos;

XI. Toda informação adquirida, criada ou modificada pelos colaboradores em suas ferramentas pertencentes a empresa como: Softwares de comunicação, e-mails, aplicativos de mensageria, e demais aplicativos que manipule informações, são de propriedade da empresa, mesmo que estas estejam sob controle deste colaborador.

XII. A gravação de informação em mídias removíveis (CDs, DVDs, Blue Ray, Pen Drive, celulares etc.) é permitida somente nas condições relacionadas nos Procedimentos de Solicitação e Uso de Dispositivos de TI, e devem ser solicitadas via chamado utilizando o canal respectivo;

XIII. A utilização de armazenamento em nuvem (cloud) é permitida somente para uso corporativo por meio do parceiro credenciado informado no procedimento interno da Frigol S.A., e somente após a devida autorização do gestor responsável, controladoria e TI;

XIV. É vedada a utilização de serviços de nuvem de parceiros não homologados, assim como para fins particulares;

XV. É vedada a instalação de qualquer software/plug-in diretamente pelos Colaboradores, tais como aplicações bancárias, programas gratuitos, aplicativos terceiros de recursos para o office, Internet Explorer, Chrome etc. Qualquer demanda de instalação de softwares deve ser passada para a TI via chamado utilizando o canal respectivo;

XVI. É vedada a utilização de qualquer serviço de armazenamento de dados não homologado nesta política e em seus documentos de referência;

3.3.3 Compete a área de Tecnologia da Informação

I. Estudar, monitorar e propor controles e melhorias relacionados ao tema de privacidade e segurança da informação;

II. Documentar as políticas e procedimentos relacionados a Lei Privacidade da Política de Segurança da Informação;

III. Analisar os alertas e informações relacionados a Lei Privacidade da Política de Segurança da Informação;

IV. Verificar durante processo de aquisição de novos produtos e ou serviços as ameaças e riscos no que tange a privacidade e a Política de Segurança da Informação;

V. Testar a eficácia dos controles utilizados e informar aos gestores as possíveis riscos e ameaças;

VI. Disseminar a cultura de privacidade e segurança da informação junto a todas as áreas da empresa;

VII. Apoiar todas as áreas envolvidas em projetos, tarefas e processos que envolvam a Lei Privacidade da Política de Segurança da Informação;

VIII. Fornecer a todos os colaboradores e parceiros que tratem quaisquer tipos de informações, estes documentos e demais que se façam necessário para que haja completa ciência por todos envolvidos das políticas diretrizes e normas de privacidade e da Política de Segurança da Informação.

3.3.4 Compete ao Comitê de Privacidade e Segurança da Informação da Frigol S.A.

I. Determinar as diretrizes de lei de privacidade e da Política de Segurança da Informação;

II. Aprovar e revisar periodicamente política de Lei Privacidade da Política de Segurança da Informação (periodicidade máxima de 2 anos);

III. Apresentação de assuntos relevantes a Diretoria quando cabível;

IV. Receber e tratar os casos de violação da lei de privacidade ou da Política de Segurança da Informação;

V. Responsabilizar-se pelo uso adequado de dados pessoais em suas atividades;

VI. Promover o conhecimento adequado dos principais stakeholders em relação à importância da proteção de dados pessoais e das atividades internas inerentes as iniciativas de privacidade;

VII. Discutir e tomar decisões técnicas sobre novas atividades de tratamento de dados pessoais, principalmente as avaliações de impacto à proteção de dados pessoais (AIPDs), e auxiliar a Controladoria quanto a revisão de procedimentos após a construção de cada AIPD;

VIII. Decidir sobre as medidas técnicas a serem aplicadas para eventos de alto risco, assim como as medidas disciplinares pertinentes;

IX. Submeter a Diretoria a resolução sobre as medidas técnicas relativas a eventos de alto risco;

3.3.5 Compete ao Encarregado de Proteção de Dados (DPO)

I. Propor ao Comitê de privacidade e segurança da informação da Frigol S.A., a revisão periódica das políticas;

II. Garantir que a Frigol S.A. esteja em conformidade com as leis e regulamentos atuais vigentes relacionados a privacidade e proteção de dados, bem como sobre suas próprias políticas de privacidade, proteção e segurança da informação;

III. Liderar, coordenar e supervisionar a estratégia de proteção de Dados Pessoais e orientar na implementação das medidas requeridas para estar em conformidade com os requisitos da legislação e da regulamentação aplicáveis de proteção de Dados Pessoais;

IV. Participar dos projetos corporativos que envolvam tratamento de dados pessoais, atentando-se estão enquadrados nas diretrizes e políticas da Frigol S.A. e os requisitos da legislação e da regulamentação aplicáveis de proteção de dados pessoais;

V. Realizar treinamentos, programas de conscientização e comunicação do tema de privacidade de dados pessoais em toda a empresa;

VI. Elaborar e manter atualizada a documentação orientadora relativa à privacidade que estejam sob sua competência;

VII. Monitorar o cumprimento das regras internas de privacidade;

VIII. Desenvolver junto a área jurídica toda a documentação pertinente a transferência de dados pessoais quando esta for realizada fora do país;

IX. Coordenar a construção e execução da Análise de Impacto à Privacidade de Dados (AIPD), quando esta se fizer necessária;

X. Alinhar periodicamente as definições e critérios junto ao de privacidade e segurança da informação da Frigol S.A;

XI. Definir, revisar e atualizar avisos de privacidade;

XII. Periodicamente analisar a maturidade da empresa em relação as iniciativas de privacidade, identificando correções e melhorias, assim como seu andamento e evolução;

XIII. Acompanhar as medidas corretivas de falhas em processos e procedimentos no que se refere a privacidade e proteção dos dados pessoais;

XIV. Realizar o contato, tratativas e atender as solicitações dos titulares dos dados sempre que necessário de acordo com as legislações de cada país em que o titular residir;

XV. Cooperar e se relacionar com a Autoridade Nacional de Proteção de Dados Pessoais;

XVI. Garantir a manutenção das evidências de execução e implementação das iniciativas de privacidade atendendo ao princípio da responsabilização.

3.3.7 Compete a Diretoria e Presidência

I. Comunicar e reforçar o cumprimento das normas de privacidade e da Política de Segurança da Informação para todos colaboradores e parceiros, bem como ser modelo de conduta e boas práticas;

II. Propor melhorias, ajustes e ferramentas para assegurar o melhoramento contínuo da gestão da política junto à organização;

III. Manter contínua comunicação com os departamentos, atualizando-os sobre quaisquer novos contratos ou encerramentos destes e ou parcerias que possam ter informações da empresa;

IV. Contribuir nos processos de revisão das políticas, diretrizes e normas da lei de Privacidade e da Política de Segurança da Informação;

V. Assegurar que as políticas e diretrizes estejam compatíveis com a estratégia da organização;

VI. Assegurar a integração desta política com os processos da organização;

VII. Assegurar os recursos necessários para a aplicação das normas de privacidade e da Política de Segurança da Informação;

3.3.9 Compete a Controladoria

I. Supervisionar, apoiar e determinar controles para que informações relativas ao negócio da empresa sejam confiáveis e auditáveis, em conformidade com as legislações e regulamentações aplicáveis nas regiões onde existam operações da organização;

II. Assegurar que o controle de acesso aos sistemas e registros da Frigol S.A. atenda às legislações e regulamentações vigentes nos territórios onde existam operações da organização;

III. Apurar os eventos de violação da privacidade ou da Política de Segurança da Informação, seguindo as normas previstas nesta política após deliberação do Comitê de Privacidade e Segurança da Informação da Frigol S.A. e em casos em que necessitem desta ação;

IV. Propor contramedidas no caso de processos ou procedimentos ferirem a lei de privacidade ou a Política de Segurança da Informação;

V. Assegurar a aplicação de procedimentos internos para tratar de casos de vazamento de informações confidenciais, reservadas ou privilegiadas;

VI. Autorizar a consulta de informações aos sistemas de controle de acesso físico ou lógico (unidades e pastas da rede), seja a colaboradores, parceiros ou visitantes;

VII. Autorizarem a escuta de gravações de outro usuário ou a gravação de conversas telefônicas para mídia externa, em atendimento a eventuais solicitações das autoridades competentes e em conformidade com a diretoria e com as leis e regras atuais vigentes no país e onde a empresa atuar;

3.3.10 Compete a área Jurídica

I. Requerer a inserção de cláusulas que obriguem o cumprimento desta política e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços.

4. REQUISITOS

Para a aplicação das normas de privacidade e Política de Segurança da Informação, a empresa se valerá do uso de tecnologias e frameworks tais como documentados os descritos abaixo.

4.1 NORMA ISO 27.000

Trata-se de uma família de certificações internacionais reconhecida mundialmente, e utilizada por empresas para a implantação de Sistemas de Gestão em Segurança da Infamação (SGSI), e subdivide-se em normas com funções distintas para auxiliar as empresas no cumprimento e na comprovação de conformidade em relação a privacidade e segurança da informação.

4.2 PMBOK

Guia utilizado no gerenciamento de projetos, traz consigo as boas práticas e orientações na condução destes, com o objetivo de padronizá-las conforme experiências testadas e avaliadas em projetos em todo o mundo. Traz consigo ao todo dez área de conhecimento, ao qual poderão ser utilizadas segundo a necessidade individual de cada projeto. Ou seja, tendo projetos com necessidade de envolvimento de todas as área e projetos com uma ou duas áreas apenas com referência.

4.3 GDPR

Regulamento Geral de Proteção de dados adotada pela União Europeia e Espaço Econômico Europeu, sendo reconhecida em todo o mundo como o mais completo regulamento de proteção as violações de privacidade de dados.

4.4 LGPD

Baseada no regulamento europeu (GDPR), a LGPD ou Lei Geral de Proteção de Dados, é a norma regulamentadora de privacidade de dados criada pelo governo brasileiro, e que deve ser

seguida por todas as pessoas físicas ou jurídicas do país ao realizar quaisquer tratamentos de dados neste território.

5. RECURSOS HUMANOS

A segurança da informação se estende por todas as áreas da empresa que manipulam e tratam dados. Sendo assim, a área de Recursos Humanos não é diferente e alguns cuidados e procedimentos devem ser seguidos quanto a seleção, contratação, promoção e desligamentos.

5.1 SELEÇÃO DE CANDIDATOS

I. Realizar validação e análise das competências acadêmicas e profissionais do currículo certificando sua exatidão e clareza das informações;

II. Verificação independente da identidade do candidato vide documentação pessoal (CPF, RG, certidão de nascimento, passaporte ou similares);

III. Verificação e validação de referência de caráter satisfatórias (indicação pessoal do currículo;

IV. Verificação e validação de registros criminais (certidão de antecedentes criminais);

V. Validação e autorização dos direitos de acessos físicos e lógicos do candidato junto a empresa, compatíveis com as funções que serão desempenhadas por este;

VI. Verificação e validação de diplomas e certificados apresentados pelos candidatos quanto aos cursos por este concluídos, habilitando-os a executar as funções correspondentes a estes documentos, principalmente (mas não se limitando), aos que se referem a trabalhos em ambientes de risco como: altura, eletricidade, confinamento, dentre outros;

5.2 CONTRATAÇÃO DE CANDIDATOS

I. Passar ao conhecimento dos candidatos aprovados, as políticas de segurança da informação e de privacidade de dados da Frigol S.A., bem como o Código de Conduta da empresa para ciência e entendimento destes;

II. Passar as responsabilidades legais e de direitos e deveres para os candidatos, parceiros e quaisquer partes externas que tenham acesso as informações sensíveis associadas a Frigol S.A., sendo obrigatória a assinatura do Termo de Confidencialidade e de não divulgação destas informações e dados, antes da concessão de quaisquer acessos;

III. Passar as responsabilidades legais e de direitos e deveres para os candidatos, parceiros e quaisquer partes externas com relação às leis de direitos autorais e legislações de proteção de dados;

IV. Orientar os candidatos, parceiros e quaisquer partes externas que tenham acesso a documentos, dados e informações associadas a Frigol S.A., sobre as responsabilidades nas conduções dos documentos internos da empresa ou mesmo de outras empresas associadas a

empresa, agindo com ética e responsabilidade quanto a sua classificação, armazenamento, transporte, compartilhamento, divulgação e até mesmo seu descarte;

5.3 RESPONSABILIDADES

5.3.1 Responsabilidades da Diretoria

I. Fomentar e apoiar as áreas no que for necessário quanto a divulgação e aplicação desta política para que esta esteja na ciência de colaboradores e parceiros e que esta seja cumprida conforme descrito;

II. Que as diretrizes sejam periodicamente revisadas, analisadas e aprovadas para que possam ser passadas aos colaboradores antes de iniciarem suas atividades junto a empresa;

5.3.2 Responsabilidades dos agentes de RH

I. Repassar, fomentar, instruir e monitorar o cumprimento das diretrizes básicas da segurança da informação como: segurança com senhas, atenção ao uso do e-mail e internet, política de mesa limpa e tela limpa), a todos os colaboradores, parceiros e partes externas que tenham relação como a Frigol S.A.;

II. Estejam atualizados e em constante desenvolvimento quanto as práticas de segurança da informação, praticando, revisando e procurando novos métodos mais apropriados a execução dos trabalhos referentes a área e para estarem preparados para passar o conhecimento a todos colaboradores recém-contratados em processo de integração;

III. Cumpram e façam cumprir as diretrizes básicas da política de segurança da informação, principalmente as que envolvem colaboradores já contratados do setor e de todos os outros setores, ou durante o treinamento de reciclagem e revisão periódica desta política;

IV. Periodicamente convoquem (mesmo que remotamente), colaboradores para a reciclagem quanto as políticas de segurança da informação e privacidade de dados, bem como sobre o código de conduta da empresa. Estas campanhas devem revisar os papéis, responsabilidades e conscientização destes, mantendo-os alinhados e cumprindo as expectativas da empresa quanto ao tema;

V. Disponibilizem um canal de denúncia, para reportar violações das políticas, normas e procedimentos relacionados à segurança e privacidade da informação;

5.3.3 Promoções e desligamentos

Quanto a ocorrência de promoções e desligamentos, a segurança da informação e privacidade dos dados devem seguir atuantes e presentes durante todos os processos.

Caso a promoção acabe por ceder mais direitos ao colaborador ou parceiro, toda a questão de sigilo, privacidade e segurança da informação também devem ser atualizadas/revisadas, e por um período de transição, podem ser necessárias adaptações, extensões das antigas obrigações e responsabilidades.

Nos casos de desligamentos, a área de TI deve ser antecipadamente avisada para os devidos bloqueios e dependendo da atividade desempenhada, termos de sigilo e reponsabilidade devem ser estendidos para os resguardos estratégicos das informações.

Sendo assim, podem ocorrer (a depender do cargo/função), que as responsabilidades e obrigações contidas nos contratos de trabalho (seja colaborador ou parceiro), permaneçam validas por um período, mesmo após encerramento das atividades.

O departamento de RH deve estar em total alinhamento com as gerências das áreas quanto a quaisquer mudanças, desligamentos ou contratações, observando atentamente aos processos em si, bem como o cumprimento de todas as normas e políticas da privacidade e da segurança da informação.

6. HOME OFFICE

O conceito do regime de trabalho em “Home Office”, podendo também ser traduzido ou referenciado como “Escritório em casa”, “Teletrabalho” ou “Remoto”, é um regime em que colaboradores atuam exercendo suas funções, porém estas são executadas de casa, não estando fisicamente nas dependências da empresa.

Complementando a definição acima, podemos citar a norma ISO/IEC 27.002 (2013, p. 11) “Trabalho remoto refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: “ambientes de telecommuting”, “local de trabalho flexível”, “trabalho remoto” e “trabalho virtual”.

Em decorrência de quaisquer circunstâncias e ou necessidades, a Frigol S.A. poderá adotar este regime de trabalho para um ou mais colaboradores, cabendo esta decisão aos gestores e podendo ser revogado por estes se necessário.

Todo o conteúdo da política de atuação deste regime e suas responsabilidades estão descritos no documento “Política de Privacidade”, sendo o conhecimento deste obrigatório para todos os colaboradores que estão ou irão trabalhar sob este regime.

7. GESTÃO DE TERCEIROS

As atividades das empresas, por mais simples que estas sejam, podem envolver uma grande variedade de funções internas necessárias para a condução dos negócios. Muitas destas funções são permanentes e necessárias no dia a dia, outras, porém são sazonais ou esporádicas e o custo para manter permanentemente colaboradores nos exercícios destas, acabam tornando-se inviáveis. Mesmo as funções fixas na empresa, necessárias para a realização do negócio fim, mas diferente deste, podem tornar-se onerosas para a instituição.

Para atender a estas demandas, as empresas recorrem a outras empresas ou profissionais, também denominados terceiros, que direcionam os seus negócios e atividades a especialização na prática de um dado nicho de negócio, e supre o mercado que possui a necessidade deste.

Embora seja uma relação mútua de ganhos, por tratar-se de profissionais com relação contratual com uma empresa, porém atuando em outra, ocorre a necessidade de cuidados principalmente no que tange a privacidade e segurança da informação, e por isso se faz necessária normas e diretrizes de gestão destas empresas e profissionais.

Por isso, o Comitê de Privacidade e Segurança da Informação da Frigol S.A. criou um documento que contém todas estas normas, processos e procedimentos padronizados para sua devida gestão, denominado “Política de Gestão de Terceiros”.

8. COMPROMISSOS E PENALIDADES

8.1 COMPROMISSOS

Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os colaboradores da empresa. O descumprimento da Política é considerado uma falta

grave e poderá acarretar aplicação de sanções previstas em lei, assim como advertências conforme este regulamento e nas disposições contratuais.

8.2 PENALIDADES

Para os colaboradores podem acarretar aplicações de advertências, suspensão ou desligamento formal, proporcional a falta cometida.

Para os parceiros e prestadores de serviços, podem acarretar aplicações rescisória imediatas dos respectivos contratos.

8.3 TREINAMENTOS, ATUALIZAÇÕES E DIVULGAÇÕES

Este documento foi elaborado pelo Comitê de Privacidade e Segurança da Informação da Frigol S.A., podendo apenas este realizar alterações ou atualizações em seu conteúdo. O comitê promove periodicamente eventos e treinamentos para que todos os colaboradores e parceiros tenham atualizados o conhecimento das políticas, suas normas e diretrizes institucionais.

Por conta desta e das demais políticas serem de conteúdo amplo, todos os envolvidos devem ser consultados periodicamente, mantendo-se assim cientes e atualizados com as responsabilidades de cada uma frente as normas de privacidade e da política de segurança da informação da Frigol S.A.

9. SUBPOLÍTICAS REFERENCIADAS NESTA POLÍTICA.

- **Política de Ativos de TI**
- **Política de Classificação de Informações**
- **Política de Controles de Acesso**
- **Política de Gestão de Mudanças**
- **Política de Gestão de Terceiros**
- **Política de *Home Office***
- **Política de Privacidade**
- **Política de Privacidade - Site Frigol**
- **Política de Privacidade e Proteção de Dados**
- **Política de Resposta a Incidentes**
- **Política de Uso de E-Mail Corporativo**
- **Política de Uso de Internet Corporativa**

10. ELABORADORES

Revisão	Nome	Área	Relatório	Data
01	Fernando Alberto Topa	TI	Criação da Política	11/08/2021
02	Tiago Costa	TI	Ajustes solicitados pelo CFRC	21/01/2022
03	Fernando Alberto Topa	TI	Atualização do Comitê/Organograma	18/03/2022