POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA (PSIC)

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes, princípios e conceitos a serem seguidos pela Indústria Química Del Monte Ltda para assegurar que a segurança da informação, bem como a segurança cibernética, estejam integradas a todas as atividades e processos da Del Monte Química, implementando tecnologias que permitam à Del Monte Química identificar, prevenir, detectar e reduzir o risco cibernético, baseado nos quatro pilares de **confidencialidade**, **integridade**, **disponibilidade** e **autenticidade**, atendendo aos requisitos de negócios e exigências regulatórias e legais.

2. ABRANGÊNCIA

Esta política aplica-se à toda empresa, em todos os seus níveis hierárquicos, bem como terceiros contratados que estejam ligados, direta ou indiretamente, a obtenção e/ou tratamento de dados.

3. REFERÊNCIAS

- Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
- Decreto no 11.856/2023 - Política Nacional de Cibersegurança (PNCiber), que estabelece objetivos, instrumentos e um comitê para a cibersegurança nacional, afetando a forma como as organizações devem gerenciar e proteger as informações.
- Resolução CD/ANPD Nº 18, de 16 de julho de 2024.
- Portaria nº 93, de 18 de outubro de 2021: Glossário de Segurança da Informação.
- CIS – Center for Internet Security – Os 18 Controles de Segurança Críticos do CIS
- POL-DM-LGPD – Rev0

4. TERMOS E DEFINIÇÕES

ATIVO: Qualquer coisa que tenha valor para uma organização, incluindo, mas não se limitando a, outra organização, pessoa, dispositivo de computação, sistema de tecnologia da informação (TI), rede de TI, circuito de TI, software (uma instância instalada e uma instância física), plataforma de computação virtual (comum em computação em nuvem e virtualizada) e hardware relacionado (por exemplo, fechaduras, armários, teclados).

AMBIENTE DE NUVEM: Um ambiente virtualizado que fornece acesso de rede conveniente e sob demanda a um conjunto compartilhado de recursos configuráveis, como rede, computação, armazenamento, aplicativos e serviços. Há cinco características essenciais para um ambiente de nuvem: autoatendimento sob demanda, amplo acesso à rede, pooling de recursos, elasticidade rápida e serviço mensurável. Alguns serviços oferecidos por meio de ambientes de nuvem incluem Softwares como Serviço (SaaS), Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS).

AMBIENTE FÍSICO: Componentes físicos de hardware que compõem uma rede, incluindo cabos e roteadores. O hardware é necessário para a comunicação e interação entre dispositivos em uma rede.

AMBIENTE VIRTUAL: Simula hardware para permitir que um ambiente de software funcione sem a necessidade de usar muito hardware real. Ambientes virtualizados são usados para fazer com que um pequeno número de recursos atue como muitos, com bastante processamento, memória, armazenamento e capacidade de rede. A virtualização é uma tecnologia fundamental que permite o funcionamento da computação em nuvem.

ATIVOS EMPRESARIAIS: Ativos com potencial para armazenar ou processar dados. Para os fins deste documento, ativos corporativos incluem dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores em ambientes virtuais, baseados em nuvem e físicos.

DISPOSITIVOS DE REDE: Dispositivos eletrônicos necessários para comunicação e interação entre dispositivos em uma rede de computadores. Dispositivos de rede incluem pontos de acesso sem fio, firewalls, gateways físicos/virtuais, roteadores e switches. Esses dispositivos consistem em hardware físico, bem como dispositivos virtuais e baseados em nuvem. Para os fins deste documento, dispositivos de rede são um subconjunto dos ativos corporativos.

DISPOSITIVOS DE USUÁRIO FINAL: Ativos de tecnologia da informação (TI) utilizados pelos membros de uma empresa durante o trabalho, fora do horário comercial ou para qualquer outra finalidade. Dispositivos de usuário final incluem dispositivos móveis e portáteis, como laptops, smartphones e tablets, bem como desktops e estações de trabalho. Para os fins deste documento, os dispositivos de usuário final são um subconjunto dos ativos corporativos.

DISPOSITIVOS MÓVEIS PARA USUÁRIOS FINAIS: Pequenos dispositivos de usuário final fornecidos por empresas com capacidade sem fio intrínseca, como smartphones e tablets. Dispositivos móveis de usuário final são um subconjunto de dispositivos portáteis de usuário final, incluindo laptops, que podem exigir hardware externo para conectividade. Para os fins deste documento, dispositivos móveis de usuário final são um subconjunto de dispositivos de usuário final.

DISPOSITIVOS NÃO COMPUTACIONAIS/INTERNET DAS COISAS (do inglês, IoT – Internet of Things): Dispositivos com sensores, software e outras tecnologias incorporados para conectar, armazenar e trocar dados com outros dispositivos e sistemas pela internet. Embora esses dispositivos não sejam usados para processos computacionais, eles apoiam a capacidade de uma empresa de conduzir processos de negócios. Exemplos desses dispositivos incluem impressoras, telas inteligentes, sensores de segurança física, sistemas de controle industrial e sensores de tecnologia da informação. Para os fins deste documento, dispositivos não computacionais/IoT são um subconjunto de ativos corporativos.

DISPOSITIVOS PORTÁTEIS PARA USUÁRIOS FINAIS: Dispositivos portáteis para o usuário final que têm a capacidade de se conectar sem fio a uma rede. Para os fins deste documento, dispositivos portáteis para o usuário final podem incluir laptops e dispositivos móveis, como smartphones e tablets, todos eles um subconjunto de ativos corporativos.

DISPOSITIVOS REMOTOS: Qualquer ativo empresarial capaz de se conectar a uma rede remotamente, geralmente via internet pública. Isso pode incluir ativos empresariais, como dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores.

IDENTIFICADOR DE ATIVOS CORPORATIVOS: Geralmente, um adesivo ou etiqueta com um número exclusivo ou sequência alfanumérica que pode ser rastreada dentro de um inventário de ativos corporativos.

INVENTÁRIO DE ATIVOS: Um inventário de ativos é um registro, repositório ou lista abrangente dos ativos de uma empresa e informações específicas sobre esses ativos.

PROPRIETÁRIO DO ATIVO: O departamento, unidade de negócios ou indivíduo responsável por um ativo empresarial.

SERVIDORES: Um dispositivo ou sistema que fornece recursos, dados, serviços ou programas para outros dispositivos em uma rede local ou de longa distância. Os servidores podem fornecer recursos e usá-los de outro sistema simultaneamente. Exemplos incluem servidores web, servidores de aplicativos, servidores de e-mail e servidores de arquivos.

USUÁRIO: Funcionários (tanto no local quanto remotos), fornecedores terceirizados, contratados, prestadores de serviços, consultores ou qualquer outro usuário que opere um ativo empresarial.

5. DECLARAÇÕES DA POLÍTICA

Fica instituída a Política de Proteção de Dados Pessoais da Indústria Química Del Monte Ltda, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção e segurança de informações e cibernética.

Esta Política de Proteção de Segurança das Informações e Cibernética (PSIC) aplica-se a toda unidade organizacional da Indústria Química Del Monte Ltda, e deverá ser observada por todos os usuários de dados e/ou informação em dispositivos ativos da empresa (tecnologia da informação, rede, dispositivos de usuário final, sejam fixos ou móveis, portáteis ou remotos, não computacionais, servidores), em ambiente físico, virtual ou em nuvem, seja colaborador, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade e do Código de Conduta e Ética de Parceiros de Negócios, para acessar ou guardar os ativos de dados e informação sob responsabilidade da Del Monte.

A aplicação desta Política também complementa a Política POL-DM-LGPD.

5.1 – PRINCÍPIOS

Todas as proteções de segurança cibernética implementadas devem possuir a premissa de segurança operacional, salvaguardando dados e informações de pessoas físicas e jurídicas, garantindo que um incidente de segurança cibernética ou da segurança da informação não se torne um acidente que possa causar danos à integridade física de pessoas, uso indevido que impacte imagem, seja da corporação como de qualquer pessoa com ela envolvida, bem como dos negócios por nós realizados, incluindo informações confidenciais.

5.1.1 – Confidencialidade: as proteções implementadas devem ter como premissa a garantia de que a informação estará acessível apenas a pessoas autorizadas, bem como monitoramento e registro de quem realizou eventuais alterações.

5.1.2 – Integridade: as proteções implementadas devem garantir a manutenção das condições iniciais das informações,
de acordo com a forma com que foram produzidas e armazenadas; os controles implementados devem possuir rastreabilidade, com registros de ações realizadas, permitindo que seja possível identificar os responsáveis por elas, bem como o exato momento em que ocorreram.

5.1.3 – Disponibilidade: as proteções implementadas devem considerar todos os requisitos e/ou protocolos que mantenham a disponibilidade de sistemas de informação adotadas e necessárias para o nosso negócio, sem comprometer o seu desempenho; os controles de segurança implementados devem ser monitorados e capazes de notificar qualquer evento que possa a vir impactar o bom funcionamento ou a proteção dos sistemas de informação.

5.1.4 – Autenticidade: Os controles implementados devem possuir recursos para confirmar a identidade dos usuários, sistemas ou dispositivos, impedindo que invasores acessem os sistemas e dados.

5.2 – DIRETRIZES GERAIS

a) Todas as informações do negócio, adquiridas, processadas, armazenadas e transmitidas são consideradas patrimônio da Indústria Química Del Monte Ltda e devem ser utilizadas somente para a finalidade autorizada, bem como adequadamente protegidas de riscos e ameaças que possam comprometer sua confidencialidade, integridade, disponibilidade e autenticidade.
b) Os recursos, sistemas, equipamentos e serviços fornecidos para desenvolvimento das atividades profissionais, mesmo que tenham sido adquiridos por locação, devem ser considerados, para fins desta Política, como propriedade da Indústria Química Del Monte Ltda e devem ser utilizados apenas para a finalidade laboral do negócio. É vedado o uso desses equipamentos para quaisquer fins pessoais ou recreativos.
c) Os acessos aos sistemas informatizados devem utilizar tecnologias por meio de credenciais pessoais e que sejam intransferíveis, devendo seguir os critérios de segurança definidos pela empresa.
d) A Indústria Química Del Monte Ltda poderá monitorar e registrar todas as atividades realizadas, com a finalidade de proteção dos seus ativos, da sua imagem e do seu negócio, que poderão ser usados para fins administrativos e legais, além de subsidiar autoridades em caso de investigações.
e) Os protocolos e atividades com ações de segurança da informação da Indústria Química Del Monte Ltda devem ser avaliadas periodicamente, com base nas melhores práticas divulgadas pelas normas e frameworks, com a finalidade de elevar o nível de maturidade do nosso processo de segurança da informação.

5.3 – DIRETRIZES ESPECÍFICAS

A Indústria Química Del Monte Ltda utiliza os seguintes procedimentos para assegurar que os controles de segurança implementados atendam aos níveis de proteção adequados para as informações e os seus ativos cibernéticos:

a) Inventário e gestão de ativos: classificação dos ativos em Tecnologia da Informação (TI) e Tecnologia da Operação (TO), incluindo hardware, software e licenças.
b) Identificação e gestão de vulnerabilidades: utilização de planos, procedimentos e tecnologias apropriadas para detectar, identificar, analisar, gerenciar e responder a vulnerabilidades e ameaças cibernéticas.
c) Identificação e gestão dos riscos cibernéticos: execução de processos para identificar, analisar e responder aos possíveis riscos cibernéticos nos ambientes de Tecnologia da Informação (TI) e Tecnologia da Operação (TO).
d) Gestão de identidade e acessos: criação e gerenciamento de identidades para controle de acessos para todos os colaboradores e terceiros, caso aplicável, que venham a acessar o ambiente de dados e informações da Indústria Química Del Monte Ltda.

e) Ações de Tratamento e Resposta aos incidentes de segurança: utilização de planos,instruções de trabalho, procedimentos e tecnologias para detectar, analisar, mitigar, responder e recuperar dados e informações de incidentes de segurança cibernética e garantir a continuidade da operação dos serviços e sistemas da Indústria Química Del Monte Ltda.
f) Monitoramento constante: atividades e tecnologias para coletar, monitorar e analisar as comunicações de tecnologia da Informação (TI) e de Tecnologia da Operação (TO) para estabelecer a capacidade de compreensão do ambiente em operação e a habilidade de resposta rápida.
g) Riscos em fornecedores e prestadores de serviços: garantir a responsabilidade, tal qual, de fornecedores e prestadores de serviços para que atendam ao gerenciamento de riscos cibernéticos.
h) Cultura de conscientização: planos, tecnologias e controles utilizados para criar uma cultura de segurança da informação e assegurar que a força de trabalho possa reconhecer situações de risco e agir corretamente.
i) Arquitetura de controles de segurança: gerenciamento dos processos, controles e tecnologias para a identificação de requisitos de segurança para os ativos cibernéticos e o desenho dos controles, inclusive de acessos, apropriados para protegê-los.
j) Gestão do programa de segurança da informação: estabelecimento de programa que apoie na governança, no planejamento e na promoção das atividades de segurança cibernética, alinhando os objetivos de segurança aos objetivos da organização.

6 – RESPONSABILIDADES

A segurança da informação é responsabilidade de todos os colaboradores da Indústria Química Del Monte Ltda, bem como terceiros, fornecedores e consultores, devendo cada um conhecer e compreender as diretrizes e princípios estabelecidos para o cumprimento desta Política, bem como estarem comprometidos com a proteção adequada das informações e sistemas contra ameaças e riscos. Assim espera-se que:

a) Todas as pessoas com acessos ao ambiente da Indústria Química Del Monte Ltda devem participar de atividades de conscientização sobre esta Política, com a finalidade de mitigar possíveis riscos de segurança, compreender as suas responsabilidades e seguir os procedimentos recomendados.
b) Todos os colaboradores devem comunicar à área de Segurança da Informação quaisquer descumprimentos da Política de Segurança da Informação e Cibernética.
c) Cabe às lideranças orientarem todos sob sua coordenação sobre o conteúdo desta Política, instruções e demais diretrizes de segurança e assegurar o seu cumprimento.
d) Cabe ao Comitê de Privacidade, Proteção de Dados e Segurança Cibernética avaliar e monitorar periodicamente as ações de segurança cibernética e segurança da informação, garantir recursos para a execução das atividades e apoiar as ações de promoção dessa Política.
e) Quaisquer dúvidas e/ou informações, podem ser contatados os seguintes responsáveis pelo Comitê: Sandra (sandra@delmontequimica.com.br) ou Adriana (adriana@delmontequimica.com.br).

7. DISPOSIÇÕES FINAIS

A presente Política de Segurança da Informação e Cibernética foi editada e aprovada pelo Conselho Diretor da Indústria Química Del Monte Ltda em 13 de outubro de 2025 com vigência imediata.