Departamento de Tecnologia da Informação – Dacolônia Alimentos

Plano de tratamento de incidentes de segurança da informação

Arlei Vladmir de Souza

Especialista em Gestão de Segurança da Informação

Exin Certificate ISMP - Professional 27001

Julho de 2025.

Sumário

1 APRESENTAÇÃO 1

2 RESPONSABILIDADES 2

3 CONFORMIDADE 3

4 OBJETIVO 4

5 DESCRIÇÃO DE TAREFAS..... 5

6 CONSIDERAÇÕES FINAIS 9

ANEXOS 10

ANEXO 1 – Política de Segurança da Informação 11

ANEXO 2 – Documento sobre o escopo do SGSI..... 14

ANEXO 3 – Orientações para a adequação da LGPD..... 16

ANEXO 4 – Modelo de plano de ação para tratamento de incidente..... 18

Histórico de revisões

Data	Versão	Descrição	Autor
03/06/2024	1.0	Plano de tratamento de incidente de segurança da informação.	Arlei Vladmir de Souza
			Revisor
			Heitor Luís Konzen
01/07/2025	2.0	Plano de tratamento de incidente de segurança da informação.	Arlei Vladmir de Souza
			Revisor
			Heitor Luís Konzen

1 APRESENTAÇÃO

O presente documento está em conformidade com a ISO/IEC 27002, controle 6.26 – Resposta a incidente de segurança da informação bem como a política de segurança da informação da organização Dacolônia Alimentos.

O conhecimento dos seguintes termos é necessário para a compreensão deste plano de tratamento de incidentes:

1. Disponibilidade: Toda a informação deve estar disponível para os usuários que dela necessitarem e que tenham autorização para tal acesso;
2. Integridade: Toda a informação deve ter garantias que estejam integras, sem manipulações ou modificações;
3. Confidencialidade: Toda a informação deve estar acessível somente a quem deve ter acesso;
4. Ativo: Qualquer coisa que tenha valor para a organização;
5. Titular dos dados: Pessoa natural a quem se referem os dados pessoais;
6. Controlador: Pessoa natural o ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
7. Operador: Pessoa natural o ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
8. Agentes de tratamento: o controlador e operador;
9. Ataque: Tentativa não autorizada, bem sucedida ou malsucedida de destruir, alterar, desabilitar, obter acesso a um ativo, dados ou informação;
10. Encarregado de dados: Pessoa indicada pelo controlador e operador para atuar com canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
11. Dado pessoal: Qualquer informação que possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou é ou pode ser direta ou indiretamente vinculada a uma pessoa natural;
12. Dado pessoal sensível: Dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
13. Incidente de segurança da informação: Qualquer evento que quebre os pilares de segurança da informação (disponibilidade, integridade e confidencialidade) e que cause a interrupção das operações dos processos de negócio da organização;

14. Evento de segurança a informação: Ocorrência indicando uma possível violação de segurança da informação ou falha de controles;

15. Log: Processo de registro de eventos relevantes num sistema computacional;

16. Tratamento de dados pessoais: Toda operação realizada com dados pessoais.

17. Vazamento de dados: Qualquer quebra de sigilo ou vazamento de dados que possa resultar criminosamente ou não na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizados.

2 RESPONSABILIDADES

Conforme a LGPD, Lei Geral de Proteção de Dados, o controlador é a pessoa natural ou jurídica a quem cabe as decisões referentes ao tratamento de dados pessoais.

Segue abaixo os dados da organização que se intitula controlador:

Dacolônia Alimentos Naturais, pessoa jurídica, inscrita no CPNJ sobe o número 04.330.736/0001-89, com sede na Estrada Antonio Osório dos Santos,402, bairro Costa da Miraguaia, cidade de Santo Antonio da Patrulha no estado do Rio Grande do Sul.

O operador é a pessoa natural ou jurídica que trata dados pessoais em nome do controlador de dados.

A Dacolônia Alimentos utiliza-se de vários operadores de dados que provem serviços de tecnologia da informação. A relação de operadores designados pela Dacolônia Alimentos é encontrada no Relatório de Impacto a proteção de dados pessoais – RIPDP.

Segue abaixo os responsáveis na execução deste plano:

Ator	Papeis	Responsabilidades
Controlador - Diretoria	Alta administração da organização Dacolônia Alimentos.	Deliberações sobre as ações a serem realizadas para a solução de um incidente de segurança.
Encarregado de dados	Responsável por encaminhar comunicações formais em incidentes envolvendo dados pessoais.	Contato com a Autoridade Nacional de proteção de dados. Revisão das normas de segurança da informação. Elaborar relatório formal de incidente de segurança da informação.
Departamento de tecnologia da informação	Equipe interna e empresas terceirizadas responsável pelo gerenciamento dos serviços de tecnologia da	Monitor os sistemas e serviços de tecnologia da informação com o objetivo de identificar possíveis incidentes. Investigar, realizar a análise e propor medidas para solucionar e

	informação, tratamento e resposta a incidentes.	eliminar incidentes de segurança da informação. Reportar ao encarregado de dados qualquer evento que possibilite a violação de dados pessoais ou outras atividades suspeitas que tiver conhecimento.
Colaboradores dos demais setores	Funcionários da Dacolônia Alimentos	Seguir as normas de segurança da informação da organização e seus procedimentos. Tratar os dados pessoais sob responsabilidade da Dacolônia Alimentos de forma ética e legal, respeitando o direito do titular dos dados pessoais e a legislação vigente. Zelar pela segurança das informações, não utilizando, enviando, transmitindo ou compartilhando indevidamente dados pessoais em qualquer local ou mídia. Reportar ao encarregado de dados qualquer evento que possibilite a violação de dados pessoais ou outras atividades suspeitas que tiver conhecimento.
Operadores: Fornecedores de serviços de tecnologia da informação	Operadores que disponibilizam recursos tais como sistemas, mão-de-obra, infraestrutura, maquinas, equipamentos e demais insumos para o funcionamento dos serviços de tecnologia da informação.	Monitor os sistemas e serviços de tecnologia da informação com o objetivo de identificar possíveis incidentes. Investigar, realizar a análise e propor medidas para solucionar e eliminar incidentes de segurança da informação. Seguir as normas de segurança da informação da organização e seus procedimentos. Reportar ao encarregado de dados qualquer evento que possibilite a violação de dados pessoais ou outras atividades suspeitas que tiver conhecimento.
Departamento jurídico	Corpo jurídico responsável pelas ações no âmbito do direito privada da Dacolônia Alimentos	Apoiar o encarregado na elaboração de respostas à ANPD. Fornecer orientação legal nos casos de ocorrência de incidentes de violação de dados pessoais.

3 CONFORMIDADE

A Dacolônia Alimentos Naturais identificou as seguintes necessidades para elaboração deste relatório:

Em cumprimento a Política de Segurança da informação da organização.

Em cumprimento aos artigos abaixo relacionados, todos da Lei 13.709/2018 (LGPD):

- Artigo, 46, 47,48 e 50. Cabe descrever o artigo 50 abaixo:

> *Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de*

mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - Implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

4 OBJETIVO

O objetivo deste plano é assegurar uma resposta eficiente e eficaz aos incidentes de segurança da informação bem como o cumprimento da Lei 13.709 – LGPD.

O plano de tratamento de incidentes de segurança da informação da Dacolônia Alimentos apresenta os procedimentos a serem seguidos pelos atores nas fases de registro de incidente, investigação do incidente, ações de contenção do incidente, notificação a ANPD, aplicação de medidas de contenção, analise do incidente como um todo, encerramento do incidente e lições apreendias de segurança da informação nos ativos e serviços de tecnologia da informação da organização Dacolônia Alimentos.

Cabe lembra que os serviços de tecnologia da informação utilizados pela Dacolônia Alimentos são suportados por muitos operadores como também alguns deles são suportados pela própria organização

Segue abaixo os serviços de tecnologia da informação que a organização suporta em conjunto com os operadores de dados:

1. Serviço de Internet;
2. serviços de Telefonia fixa e móvel;
3. Serviços Energia elétrica/ Nobreaks e contingência, Gerador de energia;
4. Serviço de Autenticação de usuários e Armazenamento de arquivos;
5. Serviços de Impressão;
6. Serviços de Logs e contabilidade dos sistemas;
7. Serviços Home page da empresa e commerce;
8. Serviço de Sistema ERP (Sistemas Neo, WMW, RH, Linkros etc.);
9. Serviços web de terceiros (Financeiros, bancos, Vales transportes, refeição);
10. Serviços de Backup e Restore;
11. Serviços de E-mail;
12. Serviços de Rede de Wifi;
13. Serviços de Rede de Dados/Cabeamento;
14. Serviço de Segurança dos dados e informações (antivirus, proxy,firewall, criptografia, VPN etc.);
15. Serviço de Suporte de Usuário.

5 DESCRIÇÃO DAS TAREFAS

A Dacolônia Alimentos utiliza-se do sistema SATIWEB para o gerenciamento do seu departamento de tecnologia da informação sendo que dentro deste escopo está disponibilizado a Central de Serviços onde cada usuário tem seu devido acesso para abrir e relatar seus chamados, incidentes e eventos sejam eles relacionados à segurança da informação ou não. O sistema SATIWEB utiliza-se das seguintes situações para determinar a situação atual do chamado:

1. **Pendente:** Chamado ainda não foi atendido pela equipe da central de serviços e ainda não possui pareceres técnicos;
2. **Em atendimento:** Chamado está sendo atendido pela equipe da central de serviços e já possui pareceres técnicos
3. **Em atendimento com peças:** Chamado está sendo atendido pela equipe da central de serviços, possui pareceres técnicos e necessita ou está necessitando de peças;

4. **Aguardando decisão:** Chamado foi atendido pela equipe da central de serviços, já possui pareceres técnicos e está aguardando decisão de um superior/direção;
5. **Entregue:** Chamado foi atendido pela equipe da central de serviços, possui pareceres técnicos e foi concluído, não aparecendo mais na tela da central de serviços.

Segue abaixo as tarefas que devem ser executadas com o apoio do sistema SATIWEB para execução deste plano de tratamento de incidentes.

Tarefa 01 - Registro de Incidente de Segurança da informação	
Orientações	Detectada a suspeita ou ocorrência de incidente de segurança da informação, deve-se proceder com o registro do incidente junto a central de serviços da organização Dacolônia Alimentos através do endereço **https://arleiti.com.br/sctd/**.
Fontes de registro	As fontes de registro são os próprios colaboradores da organização que ao desempenhar seu trabalho identifica uma ou mais anomalias nos sistemas e serviços de tecnologia da informação, bem como a equipe interna de TI, operadores de dados e softwares de monitoramento de ativos e serviços de TI.
Entradas	Registro do incidente na central de serviços com data, hora, serviço de TI afetado e usuário afetado.
Saídas	Registro de incidente computado, status pendente de verificação e lista de operadores responsáveis pelo serviço afetado.

Tarefa 02 - Investigação de Incidente de Segurança da informação	
Orientações	A equipe de TI deverá prestar o suporte a solicitação registrada e caso se confirme, deverá também investigar as possíveis causas, gravidade e o impacto do incidente com base no registro feito junto a central de serviços. Este primeiro contato com o possível incidente é feito através dos técnicos nível 1 da Dacolônia Alimentos.
Fontes de registro	Técnicos nível 1 e ferramentas de apoio utilizadas na investigação do incidente.
Atividades que devem ser avaliadas nesta etapa:	Identificar todos os sistemas e serviços afetados relacionados com o incidente. Identificar a existência de outros eventos e alertas relacionados com o incidente em questão. Identificar que tipo de informação e processos podem ter sido afetados.
Entradas	Testes feitos, possíveis causas, logs e análise técnica e contato com os operadores de dados responsáveis pelo serviço de TI afetado.
Saídas	Parecer técnico sobre o incidente em aberto dos técnicos nível 1, resposta dos operadores de dados.

Tarefa 03 – Ações de Contenção	
Orientações	Uma vez investigadas as causas do incidente, a equipe de TI deverá propor as medidas para conter ou solucionar o incidente o mais breve o possível, quando estiver ao seu alcance. Caso contrário deverá propor as medias cabíveis. Quando a medida de contenção depender de um operador deve-se documentar tá decisão. Caso as ações aplicadas pelo técnico nível 1 não sejam satisfatórias, o mesmo deve documentar seu parecer técnico junto ao registro do incidente na central de serviços e solicitar o apoio técnico nível 2. Caso o nível 2 também não conseguir resolver o incidente, deve-se adicionar um especialista no incidente que irá propor uma solução do incidente através de um plano de ação conforme consta em anexo a este plano de tratamento de incidente.
Fontes de registro	Técnicos nível 1, 2, operadores de dados e especialista.
Atividades que devem ser analisadas nesta etapa	Desconectar o sistema comprometido ou isolar a rede afetada. Desativar o sistema para evitar maiores perdas, quando há perda ou roubo de informação. Bloquear padrões de tráfego de rede interrompendo o fluxo de ataque, alterar regras de roteamento dos equipamentos de rede. Desabilitar serviços de rede afetados ou vulneráveis, inibindo o comprometimento dos sistemas.
Entradas	Solução encontrada.
Saídas	Parecer técnico sobre o incidente em aberto dos técnicos nível 1 ou 2 ou especialista com a resolução do incidente ou não.

Tarefa 04 – Notificação a ANPD e ao titular dos dados	
Orientações	Caso o incidente de segurança da informação envolver dados pessoais, a equipe de TI deve relatar em seu parecer junto ao registro do incidente na central de serviços e solicitar o apoio do encarregado de dados para que efetue uma análise de impacto aos dados pessoais e a necessidade de notificação formal a ANPD e a titular dos dados.
Considerações	Somente o encarregado de dados poderá gerar a notificação formal a ANPD.
Fontes de registro	Evidencias, logs do vazamento de dados pessoais.
Entradas	Análise de registro do incidente através dos pareceres técnicos cadastrados e o uso do Relatório de impacto a proteção de dados pessoais.
Saídas	Notificação formal a ANPD e ao titular dos dados.

Tarefa 05 – Aplicar as medidas de contenção	
Orientações	Executar as medidas propostas no plano de ação na tarefa Nº 03 – Ações de contenção e analisar se o resultado é o esperado ou não. Documentar as ações no registro do incidente na central de serviços. Informar aos envolvidos neste incidente se o mesmo foi contido. Em caso negativo, novas medidas devem ser tomadas como novo plano de ação sugerido.
Fontes de registro	Análise do incidente, análise feita pelo usuário afetado, plano de ação.
Atividades que devem ser analisadas nesta etapa	Garantir que as causas do incidente foram removidas como também as atividades e arquivos a ele associados. Assegurar a remoção de todos os métodos e acessos utilizados pelo atacante ou ameaça.

Entradas	Medidas propostas para resolver o incidente.
Saídas	Relatório de incidente com as medidas aplicadas

Tarefa 06 – Analisar o incidente como um todo	
Orientações	Após a contenção do incidente de segurança da informação, o mesmo deve ser analisado pela equipe de TI para entender o que levou ao incidente.
Considerações	Verificar quais controles de segurança da informação falharam ou que não estão implantados e propor isso a gerencia da tecnologia da informação. Verificar os logs dos ativos de tecnologia da informação envolvidos afins de encontrar indícios do incidente.
Fontes de registro	Dados, conhecimento e sabedoria da equipe técnica e controles da ISO/EIC 27001:2023, Anexo A.
Entradas	Relatório de incidente de segurança da informação
Saídas	Parecer técnico contendo os controles que falharam, controles a serem implantados ou atualizados.

Tarefa 07 – Encerrar o incidente	
Orientações	O incidente de segurança da informação deve ser encerrado e sua documentação dever ser armazenada para possível consulta.
Entradas	Relatório de incidente de segurança da informação.
Saídas	Relatório de incidente de segurança da informação com os relatórios em anexo (tais como print de telas, logs, fotos, etc.), planos de ações executados.

Tarefa 08 – Lições apreendidas	
Orientações	Todo o incidente de segurança da informação gera documentação que deve ser aprimorada criando novos ou atualizando procedimentos que estão disponíveis na central de serviços no menu Políticas e procedimentos.
Considerações	O processo de tratamento de incidente também deve ser avaliado para verificar-se a sua eficácia junto as soluções aplicadas a cada incidente de segurança da informação.
Atividades que devem ser analisadas nesta etapa	Verificar o conjunto de lições apreendidas a fim de aprimorar os procedimentos e processos existentes. Identificar os incidentes e suas características em comum para treinar novos membro da equipe. Prover estatísticas e métricas relativas ao processo de resposta a incidentes. Obter informações que possam ser utilizadas em processos legais.
Entradas	Análise crítica do incidente de segurança da informação e do processo de tratamento de incidentes de segurança da informação.
Saídas	Procedimentos novos ou atualizados.

Os seguintes procedimentos em anexo fazem parte deste plano de ação:

1. Política de segurança da informação;
2. Documento sobre o escopo do SGSI – Sistema de Gestão de Segurança da Informação;
3. Orientações para a adequação a Lei Geral de Proteção de Dados – LGPD
4. Modelo para o Plano de ação;

6 CONSIDERAÇÕES FINAIS

Este documento é parte integrando do SGSI, sistema de gestão de segurança da informação da organização Dacolônia Alimentos, onde é demonstrado de que forma a organização trata e responde aos incidentes de segurança da informação atendendo as exigências da legislação vigente e também a gestão correta dos ativos e incidentes de segurança da informação.

Este plano deve ser revisado periodicamente com a finalidade de manter o processo de tratamento de incidentes o mais eficaz possível dentro da realidade da organização, sua cultura e processos de negócio.

Todas as melhorias identificadas neste plano são bem vidas e serão analisadas dentro do contexto da segurança da informação em especial ao escopo do SGSI.

Este plano de tratamento de incidentes de segurança da informação deve ser incorporado as atividades diárias e divulgado amplamente entre todos os envolvidos relacionados no item 2, responsabilidades, da organização Dacolônia Alimentos.

Responsável pela elaboração deste relatório

_____

Arlei Vladmir de Souza
Santo Antônio da Patrulha, 01/07/2025

ANEXOS

www.dacolonia.com.br

dacolonia@dacolonia.com.br

Data:
CNPJ: 04.330.736/0001-89
Inscrição Estadual:
1140064905

ESTRADA ANTONIO OSÓRIO DOS SANTOS, 402 COSTA DA MIRAGUAIA SANTO ANTONIO DA PATRULHA - RS
Fone/fax:51.3409.1041 - Cel.:51.3409.1041

Oracles - políticas, processos e procedimentos

Cliente: **DACOLONIA ALIMENTOS NATURAIS**

Política de Segurança da Informação

Número/Código:	**7**
Data da Inclusão:	**22/06/2023**
Data da Revisão:	**11/08/2023**
Autor do documento:	**Arlei Vladmir de Souza**
Aprovador por:	**Willian Freitas**
Nível de Confidencialidade:	**Interno**

1. Finalidade, escopo e usuários

O objetivo desta política de alto nível é definir a finalidade, a direção e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de Gestão de Segurança da informação SGSI, como definido no documento de escopo do SGSI.

Os usuários deste documento são funcionários, colaboradores e fornecedores da empresa Dacolonia Alimentos assim como as partes externas relevantes.

2.Documentos de referência

A. Norma ISO/IEC 27001;
B. Documento sobre o escopo do SGSI;
C. Metodologia de avaliação e tratamento de riscos;
D. Declaração de aplicabilidade;
E. Lista de obrigações legais, regulamentares e contratuais;
F. Política de Incidentes, Eventos e problemas;
G. Política de Continuidade de negócios;
H. Business Impact Analyse (Análise de Impacto de negócio);
I. Plano de Tratamento de Incidentes de Segurança da Informação;
J. Política de Gerenciamento de Mudanças;
L. Plano de Continuidade de negócios.

3.Terminologia básica de segurança da informação

Toda a informação tem valor para a organização Dacolonia Alimentos, independente da forma como ela está disposta, e sabemos que as informações estão sujeitas há uma série de ameaças que se forem exploradas podem causar sérios danos financeiros ao negócio da organização e até mesmo a sua reputação no mercado e perante a sociedade.

Para proteger as informações da organização Dacolonia Alimentos, a direção da mesma instituiu a Política de Segurança da Informação que está fundamentada nas seguintes diretrizes conforme os pilares da segurança que são:

A.Confidencialidade: toda a informação deve estar acessível somente a quem deve ter acesso;
B.Integridade: toda a informação deve ter garantias que estejam integras, sem manipulações ou modificações;
C.Disponibilidade: toda a informação deve estar disponível para os usuários que dela necessitarem e que tenham autorização para tal acesso;
D.Autenticidade: toda a informação seja proveniente de uma fonte confiável, ou seja, confirma que os dados possuem legitimidade, não havendo manipulação ou intervenções externas, como terceiros se passando por colaboradores;
E.Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;
F.Não repudio: visa garantir que o autor não negue ter criado e assinado o documento;
G.Irretroatividade: visa garantir que o sistema não permita a geração de documentos de forma retroativa no tempo.

4.Gerenciando a segurança da informação

4.1 Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação, respeitando o escopo definido no Documento sobre o escopo do SGSI, são os seguintes:

a) Proteger os dados da organização Dacolonia Alimentos;

b) Proteger os ativos (pessoas, processos, equipamentos e informação) da organização Dacolonia Alimentos;

c) Garantir a operação diária do negócio da organização Dacolonia Alimentos;

d) Gerenciar e responder aos incidentes, eventos e problemas relacionados a Segurança da informação e tecnologia da informação;

e) Gerenciar, tratar e responder aos riscos de segurança da informação;

f) Gerenciar a continuidade de negócio da organização Dacolonia Alimentos;

g) Instituir políticas e procedimentos adequados para operação aceitável do negócio da organização.

A direção da organização é responsável por rever estes objetivos do SGSI e por definir novos objetivos que devem ser revisados pelo menos 1 vez por ano.

A organização Dacolonia Alimentos irá avaliar o cumprimento de todos os objetivos. O gestor de Segurança da informação é o responsável por medir e reportar para a direção.

4.2 Requisitos de segurança

Esta política e todo o Sistema de Gestão de Segurança da Informação SGSI deve estar em conformidade com os requisitos legais regulamentares e contratuais sendo eles:

a) Constituição federal;

b) Obrigações estatutárias, regulamentares e contratuais;

c) Contratos de trabalho;

d) Lei Geral de Proteção de dados.

4.3 Controles de segurança da informação

Os controles de segurança da informação são definidos na metodologia de Avaliação de Riscos e de Tratamento dos Riscos. Os Controles selecionados e seu status de Implementação estão listados na Declaração de Aplicabilidade.

4.4 Continuidade de negócios

A Política de Continuidade de Negócio deve ser instituída, respeitando a BIA Business Impact Analyse (Análise de Impacto de negócio) realizado em 22/03/2023. Esta política deve ser revisada pelo menos 1 vez por ano ou sempre que houver alterações nos processos de negócio da organização Dacolonia Alimentos.

4.5 Responsabilidades

As responsabilidades básicas para o SGSI são:

a) O diretor da organização Dacolonia Alimentos Willian Freitas é responsável por garantir que o Sistema de Gestão de Segurança da Informação SGSI seja implementado de acordo com esta política;

b) A direção da organização Dacolonia Alimentos deve analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar minutas sobre a reunião. A sua finalidade é elaborar diretrizes para que sejam seguidas pelos fornecedores, funcionários e colaboradores proprietários ou custodiantes de cada ativo de informação;

c) Todos os incidentes, eventos e problemas de segurança da informação devem ser reportados por todos os funcionários e colaboradores conforme a Política Gestão de incidentes, Eventos e Problemas;

d) Funcionários e colaboradores, proprietários ou custodiantes de ativos de informações da organização Dacolonia Alimentos devem ficar cientes, serem treinados e cumprir o Plano de Tratamento de Incidentes de Segurança da Informação;

e) Gerentes e donos de processos de negócio devem ser treinados e estarem apitos a operar o Plano de Continuidade de negócios.

4.6 Comunicação da política

O gestor de segurança da informação juntamente com o departamento de recursos humanos da organização Dacolonia Alimentos deve divulgar esta política a os envolvidos bem como obter o aceite por escrito de cada envolvido.

5.Suporte para a implementação do SGSI

O Diretor da organização Dacolonia Alimentos, Willian Freitas declara estar de acordo com os requisitos identificados nesta política e determina seu cumprimento.

6.Validade e gestão de documentos

Este documento é válido a partir de 22/06/2023.
O proprietário deste documento é o gestor em segurança da informação. Este documento deve ser revisado pelo menos 1 vez por ano.
Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios dever ser considerados:

a) Total de funcionários e colaboradores que desconhecem o sistema de gestão de segurança da informação SGSI e desconhecem este documento;
b) Não conformidade do sistema de gestão de segurança da informação SGSI com as leis e as regulamentações, as obrigações contratuais;
c) Responsabilidades confusas na implementação do SGSI.

_____

Arlei Vladmir de Souza
Gestor de Segurança da Informação da organização Dacolonia Alimentos

_____

Willian Freitas
Diretor da organização Dacolonia Alimentos

Retorna

www.dacolonia.com.br

dacolonia@dacolonia.com.br

Data:
CNPJ: 04.330.736/0001-89
Inscrição Estadual:
1140064905

ESTRADA ANTONIO OSÓRIO DOS SANTOS, 402 COSTA DA MIRAGUAIA SANTO ANTONIO DA PATRULHA - RS
Fone/fax:51.3409.1041 - Cel.:51.3409.1041

Oracles - políticas, processos e procedimentos

Cliente: **DACOLONIA ALIMENTOS NATURAIS**

Documento sobre o escopo do SGSI – Sistema de Gestão de Segurança da Informação

Número/Código:	**6**
Data da Inclusão:	**18/06/2023**
Data da Revisão:	**11/08/2023**
Autor do documento:	**Arlei Vladmir de Souza**
Aprovador por:	**Willian Freitas / Heitor Luis**
Nível de Confidencialidade:	**Interno**

1.Finalidade, escopo e usuários
A finalidade deste documento é definir claramente os limites do Sistema de Gestão da Segurança da informação SGSI na empresa Dacolonia Alimentos.
Este documento aplica-se a toda a documentação e as atividades do SGSI.
Os usuários deste documento são membros da gestão da empresa Dacolonia Alimentos, membro do projeto que está implementando o SGSI fornecedores de tecnologia da informação, prestadores de serviços em tecnologia a informação para a empresa Dacolonia Alimentos.

2.Documentos de Referência
a) Norma ISO/IEC 27001.
b) Código de ética Dacolonia Alimentos

3.Definição do escopo do SGSI
Conforme decisão da direção da organização Dacolonia Alimentos e através do processo de BIA - Business Impact Analyse (Análise de impacto de negócio), relizado no dia 22/03/2023, ficou decidido que os limites do SGSI da empresa Dacolonia Alimentos abrange somente a matriz da mesma, com sede em Santo Antônio da Patrulha, Rio Grande do Sul levando em consideração os processos e serviços, unidades de organizacionais, locais, redes de infraestrutura de TI como também itens que serão excluídos deste escopo.

3.1 Processos e serviços
Os seguintes processos de negócios estão incluídas neste escopo:
Comercial, Financeiro, Faturamento, Compra, Tecnologia da informação, Custos, Recursos Humanos, Logística, Produção, Direção, Contas a pagar, Contas a receber.

3.2 Unidades Organizacionais
As macros unidades organizacionais presentes na matriz da empresa são:
Administrativo, Comercial, Recursos Humanos, Produção, Logística, Qualidade.

3.3 Locais
Todas as unidades organizacionais estão dentro da unidade matriz com sede na Estrada Antônio Osório dos Santos, número 402 – Costa da Miraguaia cidade de Santo Antônio da Patrulha – RS.

3.4 Redes e infraestrutura de TI
A infraestrutura de Tecnologia da informação presente na sede da empresa Dacolonia Alimentos é composta da seguinte forma:
03 Links de internet de 300MBs cada fornecidos via fibra ótica pelas empresas VERO e NETCOMMIT, Cabeamento de rede estruturado 10/100/1000 Mbps e links de vibra óptica, Switch fibra e gigabit, Roteador de borda, 06 servidores, 75 estações de trabalho, 10 impressoras, 8 roteadores wifi, 5 coletores utilizados no processo de expedição, Sistema de telefonia, Central telefônica, 3 Sistemas ERP sendo eles 1 desenvolvido internamente para o RH, 1 fornecido pela NEO Sistema e 1 fornecidopela WMW Sistemas

Os seguintes serviços de tecnologia da informação suportam a infraestrutura de tecnologia da informação:

Serviço de Internet Serviço de Sistema ERP (Sistemas Neo, WMW, RH etc) Serviços de Impressão; Serviços de Rede de Dados/Cabeamento; Serviços de Rede de Wifi; Serviços de E-mail; Serviços Home page da empresa e commerce; Serviços de comunicação instantânea Whatsap/Telegram; Serviços Energia elétrica/ Nobreaks e contingência, Gerador de energia; Serviço de Canas de comunicação - Redes sociais; Serviço de Mídias (TV, Som, Data show, DVD, Camerasde monitoamento); Serviços web de terceiros (Financeiros, bancos, Vales transportes, refeição); Serviços de Telefonia fixa e móvel; Serviço de Segurança dos dados e informações (antivirus, proxy,firewall, criptografia, VPN etc); Serviços de Backup e Restore; Serviço de armazenamento de arquivos; Serviço de Manutenção Preventiva;

3.5 Exclusões
Não fazem parte deste escopo as unidades comerciais espalhadas pelo Brasil e fora do país bem como unidades que não estão relacionadas neste escopo e também toda e qualquer unidade organizacional fora do local descrito no item 3.3 deste documento.

4. Validade e gestão de documentos
Este documento é valido a partir de 20/06/2023.
O proprietário do documento é o gestor em Segurança da Informação da empresa Dacolonia Alimentos e deveser revisado uma vez por ano.
Para avaliar a eficácia e a adequação deste documento, os seguintes critérios deve ser considerados:
• Quantidade de incidentes em função da definição confusa do escopo do SGSI.
• Tempo dedicado pelos colaboradores à implementação do SGSI para resolver dilemas internos.

www.dacolonia.com.br

dacolonia@dacolonia.com.br

Data:
CNPJ: 04.330.736/0001-89
Inscrição Estadual:
1140064905

ESTRADA ANTONIO OSÓRIO DOS SANTOS, 402 COSTA DA MIRAGUAIA SANTO ANTONIO DA PATRULHA - RS
Fone/fax:51.3409.1041 - Cel.:51.3409.1041

Oracles - políticas, processos e procedimentos

Cliente: **DACOLONIA ALIMENTOS NATURAIS**

Orientações para a adequação a Lei Geral de Proteção de Dados – LGPD

Número/Código:	**32**
Data da Inclusão:	**26/03/2024**
Data da Revisão:	**02/06/2024**
Autor do documento:	**Arlei Vladmir de Souza**
Aprovador por:	**Heitor Luís Konzen**
Nível de Confidencialidade:	**Interno**

A Dacolonia Alimentos dando continuidade a sua gestão de segurança da informação, vem informar aos seus parceiros de negócio, fornecedores e partes interessadas que está em processo de adequação a Lei Geral de Proteção de Dados - LGPD. Lei 13.709 de 14 de agosto de 2018.

Artigo 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Desta forma informamos que iremos iniciar o processo de verificação do Processamento de Dados pessoais junto aos operadores de dados pessoais aos quais a Dacolônia Alimentos é a controladora.

Para que todos possam compreender suas funções junto aos processos de negócios, desenvolvidos pela Dacolônia Alimentos, resumimos as definições da Lei conforme abaixo:

Pedimos a atenção dos gestores dos setores da Dacolônia Alimentos e as empresas terceiras que processam dados para a Dacolonia Alimentos afim de estarem alinhados aos próximos passos para a adequação da lei.

Definições:

Privacidade: A privacidade é definida como o direito a respeitar a vida privada e familiar de uma pessoa, sua casa e correspondência.
Proteção de dados: A LGPD diz respeito à proteção de dados pessoais e não de todos os dados.
Dados Pessoais: Qualquer informação relativa a uma pessoa natural identificada ou identificável (titular dos dados), uma pessoa natural é aquela que pode ser identificada, direta ou indiretamente seja por nome, número de identificação, fisiologia, dados de localização, dados econômicos, cultural ou social.

Para que as informações sejam "dados pessoais" elas não precisam ser verdadeiras.

O conceito de dados pessoais inclui informações disponíveis em qualquer formato: texto, figuras, gráficos, fotografias, vídeos ou qualquer outra forma possível.

Pessoal Natural: é um ser humano, um indivíduo capaz de assumir obrigações e de ter direitos. A LGPD não se aplica a pessoas falecidas.
Processamento: Processamento significa qualquer operação ou conjunto de operações efetuadas em dados pessoais ou em conjunto de dados pessoais por meio automatizados ou não como coleta, registro, organização, estrutura, armazenamento, adaptação ou alteração, recuperação, consulta utilização, divulgação por transmissão, disseminação ou de outra forma tornar disponível, alinhamento ou combinação, restrição, apagamento ou destruição.

A coleta de dados pessoais é processamento.
O armazenamento de dados pessoais é processamento.
Destruir dados pessoais é processamento.
Fazer um backup de um servidor que não seu, mas contém dados pessoais também se inclui na definição de processamento.

Titular: Pessoa natural a quem ser refere os dados pessoais que são objetos de tratamento.
Controlador: Pessoa natural ou jurídica que determina as finalidades e meios do processamento de dados pessoais. Ele é responsável e deve ser capaz de demonstrar que o processamento é executado de acordo com a LGPD.

Operador: Pessoa natural ou jurídica que processa dados pessoais em nome do controlador.
Data Protection Office (DPO): é uma pessoa que tem a tarefa formal de garantir que a organização esteja ciente e cumpra suas responsabilidades e obrigações de proteção de dados de acordo com a LGPD.

Controladores e operadores podem e nos casos abaixo devem nomear um DPO:

1. O tratamento for efetuado por uma autoridade ou organismo público.
2. As atividades principais do controlador ou do operador consistem em operações de tratamento que, devido à sua natureza, âmbito e ou finalidades, exigem monitoramento regular e sistemático em grande escala dos titulares dos dados.
3. As atividades principais do controlador ou do operador consistem no tratamento de uma grande variedade de categorias especiais de dados.

As organizações que não precisam nomear um DPO são livres para fazê-lo por vontade própria.

Destinatário: é uma pessoa natural ou jurídica, uma autoridade pública, uma agência ou outro organismo para o qual os dados pessoais são divulgados, terceiros ou não. O destinatário é uma parte interessada importante sendo que o resultado do processamento de dados pessoais é divulgado.
Terceiro: Terceiro é uma pessoa ou organização sem motivos legítimos específicos para processar dados pessoais. Exemplo: Um contador, que nas atribuições de suas atividades inadvertidamente ver dados pessoais ou um técnico que nas rotinas de backup de dados pessoais vê alguns nomes e outros dados pessoais.

Retorna

ANEXO 4

Modelo de plano de ação para tratamento de incidente

Assunto: **Tratar incidente Nº _____**	**Início:** _____	**Fim:** _____	**Responsáveis:** _____
Objetivo:			
Ativo afeto:	**Serviço de TI afetado:**	**Operador de dados afetado:** **Nenhum**	
Houve vazamento de dados pessoais?	**Requer notificar a ANPD?**	**Observações em relação a este plano:**	

Antes de propor as medidas de contenção para o incidente de segurança, há de se identificar os riscos relacionados a tais medidas e para isso o processo de gestão de risco de segurança da informação abaixo é proposto como forma de mitigar os mesmos.

1.Estabelecimento e manutenção de critérios de risco de segurança da informação

1.1 Geral

A Dacôlonia Alimentos definiu que seus critérios de riscos serão os seguintes:

Nível de risco	Avaliação de riscos	Descrição
Baixo	Aceitável como é apresentado	O Risco pode ser aceito sem mais ações.
Médio	Tolerável sob controle	Convém que um acompanhamento e termo de gestão de riscos seja realizado e que ações sejam criadas no quadro de melhoria contínua a médio e longo prazo.
Alto ou Muito Alto	Inaceitável	Convém que medidas para reduzir o risco sejam tomadas absolutamente no curto prazo. Caso contrário, convém que toda ou parte da atividade seja recusada.

1.2 Critérios de aceitação de riscos

A Dacôlonia Alimentos definiu que seus critérios de aceitação de riscos de risco são os riscos classificados como:

- Baixo
- Médio

1.3 Critérios para a realização de processos de avaliação de riscos de segurança da informação

1.3.1 Geral

A Dacôlonia Alimentos definiu que seus critérios para a realização de processos de avaliação de riscos de segurança da informação é identificar os riscos que tornam os ativos de tecnologia da informação que apoiam os macro processos da empresa, sendo que neste caso específico e tratar o incidente de segurança da informação relacionado acima.

Para isso será utilizado uma matriz que irá tratar consequências X probabilidade = Riscos.

1.3.2 Critérios de consequências

As consequências definidas pela Dacôlonia Alimentos, conforme o histórico de consequências já observadas e levando em consideração as perdas financeiras, planos e prazos levam em consideração os seguintes níveis:

Consequências	**Descrição**
Catastrófico	Consequências setoriais ou regulatórias além da organização. Consequências que podem ser duradouras. Incapacidade para assegurar uma função regulatória ou missão vital da organização.
Crítica	Consequências desastrosas para a organização. Incapacidade da organização de assegurar toda ou uma parte de sua atividade. A organização provavelmente não superará a situação.
Séria	Consequências substanciais para a organização. Alta degradação no desempenho da atividade. A organização superará a situação com sérias dificuldades.
Significativa	Consequências significativas porem limitadas para a organização. Degradação no desempenho da atividade. A organização vai super a situação apesar se algumas dificuldades.
Menor	Consequências insignificantes para a organização.

1.3.3 Critérios de probabilidade

As probabilidades definidas pela Dacôlonia Alimentos levam em consideração os seguintes níveis:

Probabilidade	**Descrição**
Quase certo	A fonte de risco certamente atingirá seu objetivo usando um dos métodos de ataque. A probabilidade do cenário de risco é muito alta.
Muito provável	A fonte de risco provavelmente atingirá seu objetivo usando métodos de ataque. A probabilidade do cenário de risco é alta.
Provável	A fonte de risco é capaz de atingir seu objetivo usando um dos métodos de ataque. A probabilidade do cenário de risco é significativa.
Bastante improvável	A fonte de risco tem pouca chance de atingir seu objetivo usando um dos métodos de ataque. A probabilidade do cenário de risco é baixa.

Improvável	A fonte de risco tem pouca chance de atingir seu objetivo usando um dos métodos de ataque. A probabilidade do cenário de risco é muito baixa.

1.3.4 Critérios para determinação do nível de risco

Os Critérios para determinação do nível de risco definidas pela Dacôlonia Alimentos levam em consideração a relação em Probabilidade X Consequência como mostra a matriz de risco abaixo:

Probabilidade	**Consequências**				
	Catastrófica	Crítico	Sério	Significativo	Menor
Quase certo	Muito Alto	Muito Alto	Alto	Alto	Médio
Muito Provável	Muito Alto	Alto	Alto	Médio	Baixo
Provável	Alto	Alto	Médio	Baixo	Baixo
Bastante improvável	Médio	Médio	Baixo	Baixo	Muito Baixo
Improvável	Baixo	Baixo	Baixo	Muito Baixo	Muito Baixo

1.3.5 Escolha de um método apropriado para a gestão de riscos

A Dacôlonia Alimentos escolheu o método de gestão e riscos descrito na ISO IEC 27005:2023 como seu padrão para que traga consistência, comparabilidade e validade nos resultados encontrados.

1.3.6 Determinação do rico e seus proprietários:

1.3.7 Lista de riscos identificados e seus proprietários:

ID	**Risco identificado**	**Proprietário do risco**
1		
2		

1.3.8 Lista de possível consequência:

ID	**Risco identificado**	**Fontes de risco**	**Processos de negócios afetados**	**Consequência**
1				
2				

1.3.9 Lista de controles implantados:

ID	**Risco identificado**	**Controles Organizacionais (ver Anexo A ISO/EIC 27001:2023)**	**Implantado**	**Eficaz?**

1.3.10 Lista de possível probabilidade:

ID	**Risco identificado**	**Fontes de risco**	**Processos de negócios afetados**	**Probabilidade**

1.3.11 Determinação do nível de risco residual:

ID	Risco identificado	Consequência	Probabilidade	Nível de risco

2 Processo de tratamento de risco relacionado ao incidente

2.1 Determinação das tarefas para tratamento do incidente

Nª	O que deve ser feito?	Por que fazer?	Onde fazer?	Quem vai fazer?	Quanto vai custar?	Quanto tempo vai levar?	Status: Não iniciado Produção atrasado Concluído
01							
02							
03							

2.1 Lista de riscos residuais identificados e seus proprietários após as tarefas propostas:

ID	Risco residual identificado	Proprietário
1		

2.2 Lista de possível consequência após as tarefas propostas:

ID	Risco residual identificado	Fontes de risco	Processos de negócios afetados	Consequência
1				

3.3 Lista de controles implantados após as tarefas propostas:

ID	Risco residual identificado	Controles Organizacionais (ver Anexo A ISO/EIC 27001:2023)	Implantado	Eficaz?
1				

4.4 Lista de possível probabilidade após as tarefas propostas:

ID	Risco residual identificado	Fontes de risco	Processos de negócios afetados	Probabilidade
1				

5.5 Determinação do nível de risco residual após as tarefas propostas:

ID	Risco residual identificado	Consequência	Probabilidade	Nível de risco
1				

3. Conclusão

Descrever a conclusão com este plano de ação:_____

O nível de risco residual identificado ficou em _____, o que está _____ dos parâmetros definidos pela direção nos critérios de aceitação de riscos. O controle tecnológico implantado _____.