POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - (PSI)

Dezembro 2023

Sumário

1. Introdução

A Planmar Indústria e Comério de Plásticos Ltda. (**PLANMAR**) possui o compromisso de resguardar e proteger os dados, sejam eles pessoais ou não, que estão sob sua guarda.

Nesse sentido, a presente *Política de Segurança da Informação Planmar (PSI Planmar)* apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na **PLANMAR** a fim de mitigar eventuais riscos e danos relacionados a **ameaças** externas ou internas, deliberadas ou acidentais, que possam impactar na **autenticidade**, **confidencialidade**, **integridade** e **disponibilidade** das informações de qualquer natureza, objetivando garantir sua preservação.

Amparada nos preceitos das Normas que regem o mercado de atuação da **PLANMAR** no padrão nacional/internacional para processos de gestão da **Segurança da Informação**, a *PSI PLANMAR* define também papéis e responsabilidades para a implantação dos seguintes controles de **segurança da informação,** conforme diagrama abaixo:

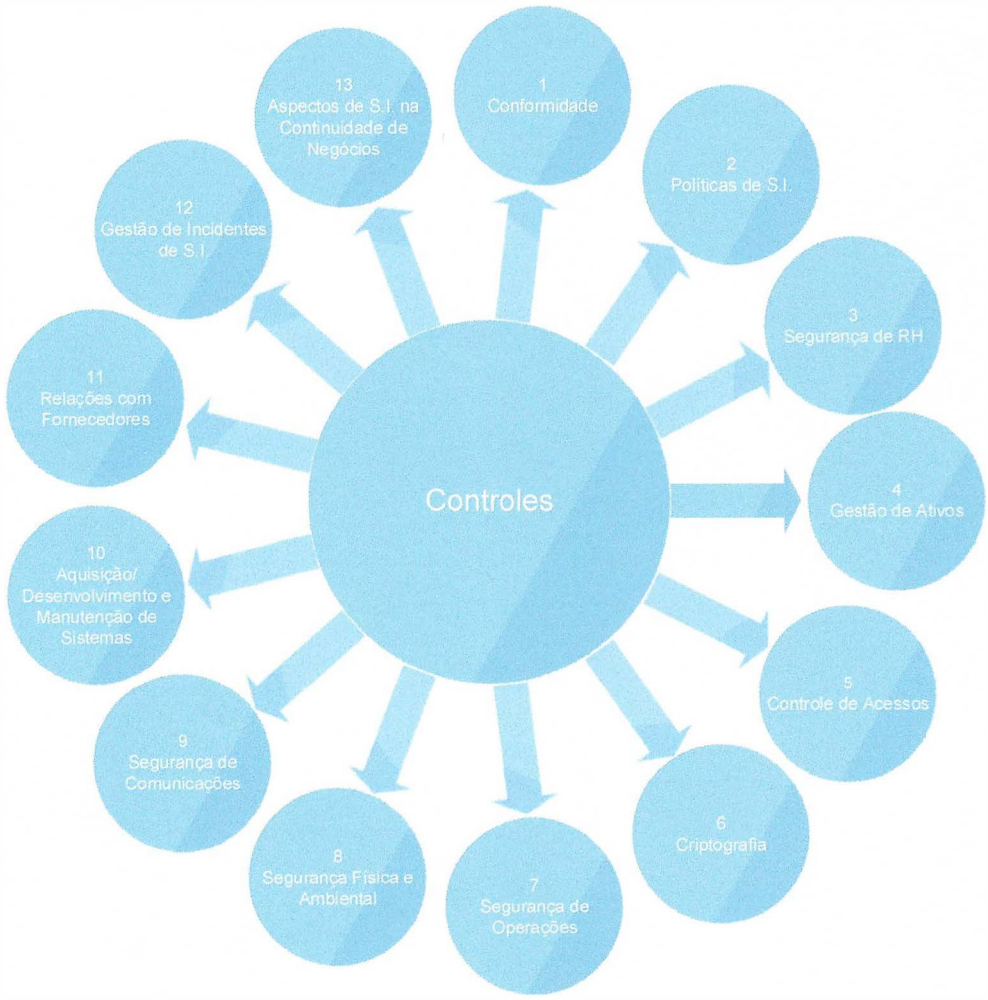

Figura 1 - Controles previstos

2. Definições

- **AMEAÇA:** causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização.
- **RISCO:** efeito da incerteza sobre os objetivos. Nota 1: Um efeito é um desvio do esperado — positivo ou negativo. Nota 2: Incerteza é o estado, mesmo parcial, de deficiência de informação, compreensão ou conhecimento de um evento, sua consequência ou probabilidade. Nota 3: O risco é frequentemente caracterizado por referência a potenciais "eventos" e "consequências", ou uma combinação destes. Nota 4: O risco é frequentemente expresso em termos de uma combinação das consequências de um evento (incluindo mudanças nas circunstâncias e da "probabilidade" associada de ocorrência. Nota 5: No contexto dos sistemas de gestão da segurança da informação, os riscos para a segurança da informação podem ser expressos como efeito da incerteza sobre os objetivos de segurança da informação. Nota 6: O risco de segurança da informação está associado ao potencial de que as ameaças explorem vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causem danos a uma organização.
- **ATIVOS DE INFORMAÇÃO:** são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pela **PLANMAR**.
- **AUTENTICIDADE:** propriedade que uma entidade é o que afirma ser.
- **CLASSIFICAÇÃO DA INFORMAÇÃO:** identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.
- **CONFIDENCIALIDADE:** propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.
- **CONFORMIDADE:** cumprimento de um requisito.
- **CONTROLE:** medida que modifica um risco. Nota 1: Os controles incluem quaisquer processo, política, dispositivo, prática ou outras ações que modifiquem risco. Nota 2: É possível que os controles nem sempre **exerçam o efeito modificativo pretendido ou presumido.**
- **CONTROLE DE ACESSO:** meios para garantir que o acesso aos ativos seja autorizado e restrito com base nos requisitos de negócios e de segurança.
- **CRIPTOGRAFIA:** método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.
- **CUSTODIANTE DO ATIVO DE INFORMAÇÃO:** é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.
- **DADOS PESSOAIS:** todo e qualquer dado relacionado a pessoa natural identificada ou identificável (conforme definição trazida no art. 5°, I, da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais),

inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2°, LGPD).

- **DISPONIBILIDADE:** propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.
- **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO (ETRISI):** grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações relacionadas a incidentes com ativos de informação da PLANMAR.
- **EVENTO DE SEGURANÇA DA INFORMAÇÃO:** ocorrência identificada de um estado do sistema, serviço ou rede indicando uma possível violação da política de segurança da informação ou falha nos controles, ou uma situação anteriormente desconhecida que pode ser relevante para a segurança.
- **FORNECEDORES:** no contexto da PLANMAR são considerados fornecedores os outros terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais.
- **GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO - GRSI:** atividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco.
- **PROCESSO DE GESTÃO DE RISCOS:** aplicação sistemática das políticas de gestão, procedimentos e práticas às atividades de comunicação, consulta, estabelecimento do contexto e identificação, análise, avaliação, tratamento, monitoramento e revisão do risco.
- **GESTOR DOS ATIVOS DE INFORMAÇÃO:** unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados.
- **PROPRIETÁRIO DO RISCO:** pessoa ou entidade com responsabilidade e autoridade para gerir um risco.
- **GESTOR DE SEGURANÇA DA INFORMAÇÃO:** funcionário responsável pela operação da Segurança da Informação na Corporação.
- **GDPR:** General Data Protection Regulation: conjunto de regras sobre tratamento de dados aprovado em 2016 válido para a União Europeia (EU). Regulamenta também a exportação de dados pessoais para fora da EU.
- **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** um ou uma série de eventos de segurança da informação não desejados ou inesperados que tenham uma probabilidade significativa de comprometer as operações de negócio e ameaçar a segurança da informação.
- **INFORMAÇÃO:** conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.
- **INFORMAÇÃO DOCUMENTADA:** informações requeridas a serem controladas e mantidas por uma organização e o meio em que estão contidas. Nota 1: As informações documentadas podem estar em qualquer formato e mídia e de qualquer fonte. Nota 2: Informações documentadas podem referir-se a: sistema de gestão, incluindo os processos relacionados; informações criadas para que a organização opere

(documentação); evidência dos resultados alcançados (registros).

- **INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO:** instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica.
- **INTEGRIDADE:** propriedade de precisão e completude.
- **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD):** Lei nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei (arts. 1° e 17, LGPD).
- **PARCEIROS COMERCIAIS:** no contexto da PLANMAR são considerados parceiros comerciais os terceiros contratados, pessoa física ou jurídica, que atuam em seu nome: Consultores, Conveniados e Agentes Comerciais (aqueles que indicam atividades onde a PLANMAR pode atuar como contratada).
- **POLÍTICA:** intenções e direção de uma organização, conforme formalmente expresso por sua alta direção.
- **QUEBRA DE SEGURANÇA:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.
- **SEGURANÇA DA INFORMAÇÃO:** preservação da confidencialidade, integridade e disponibilidade das informações. Nota 1: Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidos.
- **SEGURANÇA DE COMUNICAÇÕES:** processo de proteção de dados digitais em trânsito.
- **SISTEMA ESTRUTURANTE:** conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.
- **TERCEIROS:** São os parceiros comerciais e os fornecedores da PLANMAR.
- **TRATAMENTO DA INFORMAÇÃO:** conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.
- **TRATAMENTO DE RISCO:** processo para modificar o risco. Nota 1: O tratamento dos riscos pode envolver: evitar o risco, decidindo não iniciar ou continuar com a atividade que dá origem ao risco; assumir ou aumentar o risco para buscar uma oportunidade; remoção da fonte de risco; alteração da probabilidade; alteração das consequências; compartilhar o risco com outra parte ou partes (incluindo contratos e financiamento de risco); reter o risco por escolha informada. Nota 2: Os tratamentos de risco que tratam com consequências negativas são por vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos". Nota 3: O tratamento de riscos pode criar novos riscos ou modificar os riscos existentes.

- **VULNERABILIDADE:** fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

3. Política de Segurança da Informação Planmar (Controle ISO 27001 A.5.1.1, A.5.1.2)

Estabelece o compromisso da Planmar Indústria e Comércio de Plásticos Ltda. em resguardar e proteger as **informações**, sejam elas pessoais ou não, que estão sob sua guarda além de definir a governança de segurança da **informação** na PLANMAR.

Esta *Política de Segurança da Informação (PSI)* exige o cumprimento do *Código de Conduta PLANMAR*, Sistema de Controles Internos e de Conformidade, e de todas as leis e regulamentações aplicáveis em vigor relacionadas a proteção de dados incluindo, sem limitação, a **Lei Geral de Proteção de Dados Pessoais (LGPD)** e a **General Data Protection Regulation (GDPR)**, quando em transações comerciais com a EU (União Europeia) e demais países que a utilizem como lei regulamentadora.

Esta *Política* se insere no *Sistema de Controles Internos e de Conformidade PLANMAR* como sendo o documento que estabelece as diretrizes do ***Programa de Conformidade*** para com a **Lei Geral de Proteção de Dados Pessoais (LGPD).**

4. Destinatários

A presente *Política* se aplica a todos os membros do Conselho Administrativo, CEO, Gerentes, Coordenadores, colaboradores próprios e terceirizados, estagiários, menores aprendizes, parceiros comerciais (consultores, agentes comerciais) que atuam em nome da **PLANMAR** e fornecedores (outros contratados e subcontratados pela **PLANMAR**) e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, **informações,** arquivos, redes e dados de titularidade ou propriedade da **PLANMAR**.

Desta forma:

Todos os ***destinatários*** deverão observar as presentes regras e recomendações em quaisquer operações que possam impactar na **segurança das informações** na **PLANMAR**. O não cumprimento das disposições ora previstas sujeitará o infrator às sanções previstas fixadas pelo *Comitê de Segurança de Informação (CSI)* previsto nesta *Política,* sem prejuízo das medidas previstas em lei, caso se aplique.

5. Aplicabilidade

Esta *Política* estabelece as diretrizes para garantir que seus ***destinatários*** entendam a *Política de Segurança da Informação (PSI)* bem como a *Lei Geral de Proteção de Dados Pessoais (LGPD)*, garantindo os padrões e medidas técnicas visando a **segurança da informação** na **PLANMAR**.

6. Objetivos

Esta *Política de Segurança da Informação (PSI)* tem como objetivos:

- Estabelecer as diretrizes que assegurem e reforcem o compromisso da Empresa com as práticas e medidas preventivas garantidoras de **segurança da informação;**
- Definir o referencial para a normatização das questões de **segurança da informação** na **PLANMAR**;
- Criar condições para que a **PLANMAR** eleve continuamente a sua maturidade em **segurança da informação** por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os **ativos de informação** da **PLANMAR** visando a promoção da **Integridade, Confidencialidade, Disponibilidade e Autenticidade** dos **ativos de informação** da **PLANMAR**;
- Prover a **PLANMAR** de mecanismos de atendimento e **conformidade** às leis de **segurança da informação**, nacionais e internacionais;
- Descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela **PLANMAR** que garantam a prevenção de incidentes de **segurança da informação** e a proteção de **dados pessoais.**

Os demais documentos da **PLANMAR** que se relacionam com esta *Política* são:

- *Código de Conduta*
- *Manual do Colaborador*
- *Política de Controles Internos e de Conformidade*
- *Guia de Políticas, Normas e Procedimentos da Segurança da Informação Planmar*

Cada um desses documentos tem objetivos específicos, mas em todos está reforçado o compromisso da **PLANMAR** com a **segurança da informação**.

7. Princípios

O compromisso da **PLANMAR** com o tratamento adequado das **informações** se baseia nos seguintes princípios:

- **Autenticidade** - todos os esforços serão feitos para que as **informações** sejam confiáveis e corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida;
- **Confidencialidade** - o acesso à **informação** é permitido somente para pessoas autorizadas e quando ele for de fato necessário;
- **Disponibilidade** - somente as pessoas autorizadas têm acesso à **informação** sempre que necessário;
- **Integridade** – todos os esforços serão feitos para que as **informações** sejam exatas e completas bem como seu processamento.

8. Diretrizes

8.1. Diretrizes Gerais

- A gestão da **segurança da informação** na **PLANMAR** é de responsabilidade do *Comitê de Segurança da Informação (CSI)* cujos membros são indicados pelo CEO da **PLANMAR**;
- O cumprimento desta *Política* e de suas *normas de procedimentos complementares* deve ser avaliado periodicamente por meio de verificações de **conformidade,** realizadas por um grupo de trabalho designado pelo *Comitê de Segurança da Informação (CSI)*.
- A **PLANMAR**, além das diretrizes estabelecidas nesta *PSI*, deve também se orientar pelas melhores práticas e procedimentos de **segurança da informação,** conforme relacionados nos documentos elencados no item 6 (Objetivos) desta *PSI*.

8.2. Diretrizes e Normas Complementares específicas

Para cada um dos controles complementares propostos pela ISO 27001 o *Comitê de Segurança da Informação (CSI)* deve elaborar estratégias, diretrizes e *normas de procedimentos complementares* (Políticas de SI – controle ISO 27001 #2), assim como manuais, procedimentos de conduta e avaliações periódicas de **conformidade.**

A *PSI PLANMAR* preconiza a implantação priorizada das seguintes *normas de procedimentos* com as seguintes diretrizes:

8.3. Gestão de Ativos de Informação (Controle ISO 27001 #4)

Os **ativos de informação** devem:

Ser inventariados e protegidos;

a) Ter identificados os seus proprietários e **custodiantes;**

b) Ter mapeadas as suas **ameaças, vulnerabilidades** e interdependências;

c) Ter a sua a entrada e saída nas dependências da **PLANMAR** autorizadas e registradas por autoridade competente;

d) Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de **quebra de segurança,** por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

e) Ser regulamentados por *norma de procedimentos específica* quanto a sua utilização; e

f) Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de **terceiros,** entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

E, além disso:

i. A **PLANMAR** deve criar, gerir e avaliar critérios de tratamento e classificação da **informação** de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a

legislação em vigor.

ii. Os recursos tecnológicos e as instalações de **infraestrutura** devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

iii. Os sistemas de informação e as aplicações da **PLANMAR** devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

iv. O acesso dos usuários aos **ativos de informação** e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

v. Os **ativos de informação** devem possuir mecanismos que permitam a auditoria dos eventos de acesso e alteração dos registros. Esta auditoria deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período mínimo de um ano.

8.3.1. Gestão de Riscos e Incidentes (Controle ISO 27001 #12)

I. O **gestor dos ativos de informação** deve estabelecer processos de **Gestão de Riscos de Segurança da Informação – GRSI** que possibilitem identificar **ameaças** e reduzir **vulnerabilidades** dos **ativos de informação,** assim como reduzir os impactos de eventuais incidentes com os mesmos.

II. A GRSI é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da SI na **PLANMAR**.

8.3.2. Segurança em Recursos Humanos (Controle ISO 27001 #3)

I. Os destinatários devem ter ciência:

a) Das **ameaças** e preocupações relativas à **segurança da informação** e;

b) De suas responsabilidades e obrigações no âmbito desta *PSI*.

II. Todos os destinatários devem difundir e exigir o cumprimento da *PSI*, das normas de segurança e da legislação vigente acerca do tema.

III. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em **segurança da informação**, que alcancem todos os destinatários, de acordo com seu relacionamento e atribuições na **PLANMAR**.

8.3.3. Os usuários devem ser sensibilizados e conscientizados:

I. O controle de usuários de sistemas:

a) É de responsabilidade do titular da unidade da **PLANMAR** juntamente com o RH; e

b) Deve ser implementado controles de perfis, permissões e procedimentos necessários para a salvaguarda dos **ativos de informação** da **PLANMAR**.

8.3.4. Segurança das Operações de TI da Planmar (Controle ISO 27001 #7)

O *Comitê de Segurança da Informação (CSI)* deve estabelecer *norma de procedimentos específica* contendo diretrizes de segurança da **informação** para a disponibilização e execução dos serviços, sistemas e **infraestruturas** de TIC da PLANMAR.

8.3.5. Segurança das Comunicações da Planmar (Controle ISO 27001 #9)

O *Comitê de Segurança da Informação (CSI)* deve estabelecer *norma de procedimentos específica* contendo diretrizes de segurança da **informação** para a disponibilização e utilização de serviços de comunicação relacionados aos **ativos de informação** da **PLANMAR**.

8.3.6. Assinatura Digital e Criptografia (Controle ISO 27001 #6)

O *Comitê de Segurança da Informação (CSI)* deve estabelecer *norma de procedimentos específica* contendo parâmetros para o uso de assinaturas digitais que reflitam as necessidades específicas de garantia de **autenticidade** dos dados **PLANMAR**.

Também deve ser estabelecida norma específica ditando quando e onde recursos criptográficos devem ser utilizados dentro da **PLANMAR** para proteger suas informações, além de estabelecer quais padrões de **criptografia** são aceitáveis.

8.3.7. Controles de Acessos (Controle ISO 27001 #5)

O *Comitê de Segurança da Informação (CSI)* deve estabelecer *norma de procedimentos específica* contendo parâmetros para a gestão de acesso aos dados **PLANMAR**, atendendo os requisitos abaixo:

i. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

ii. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos **ativos de informação**.

iii. Os usuários da **PLANMAR** são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

iv. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

v. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela **informação.**

vi. Todos os sistemas de informação da **PLANMAR**, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às **informações.**

vii. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente,

devendo ser cancelados de imediato em caso de desligamento da **PLANMAR** ou bloqueados em caso de afastamento.

viii. Os **sistemas estruturantes** devem possuir normas específicas, no âmbito de sua atuação, que regrem o **controle de acesso** quanto:

a) Ao acesso às suas bases de dados;

b) À extração, carga e transformação de dados e;

c) Aos serviços acessíveis via linguagem de programação.

ix. Os sistemas estruturantes devem possuir mecanismos para:

d) Revogar as concessões e desativar as contas de acesso do colaborador nos casos de demissão, aposentadoria e falecimento do colaborador;

e) Bloquear as contas de acesso do colaborador nos casos de licença, afastamento, cessão e **disponibilidade** do colaborador e;

f) Tratar os casos de remoção e redistribuição do colaborador, segundo as definições constantes na norma de **controle de acesso** ao sistema.

8.3.8. Aquisição, Desenvolvimento e Manutenção de Sistemas (Controle ISO 27001 #10)

O *Comitê de Segurança da Informação (CSI)* deve editar *norma de procedimentos específica* estabelecendo critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e sustentação de sistemas.

8.3.9. Relação com Fornecedores (Controle ISO 27001 #11)

O *Comitê de Segurança da Informação (CSI)* deve estabelecer *norma de procedimentos específica* que vise o atendimento de demandas em segurança da **informação** para contratos, convênios, acordos e afins, conforme os requisitos abaixo:

a) Os acordos com **terceiros** que possuam algum relacionamento com **ativos de informação** da **PLANMAR** devem observar as disposições e normas desta *PSI*.

b) Os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta *PSI* e de suas normas complementares.

c) O contrato, convênio, acordo ou instrumento congênere devem prever a obrigação da outra parte de divulgar esta *PSI* e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na **PLANMAR**.

d) Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

8.3.10. Gestão de Incidentes (Controle ISO 27001 #12)

O *Comitê de Segurança da Informação (CSI)* deve instituir uma Equipe de Tratamento e Resposta a Incidentes de Segurança.

8.3.11. Aspectos de Segurança da Informação em Continuidade das Atividades (Controle 27001#13)

O *Comitê de Segurança da Informação (CSI)* deve instituir metodologias e *norma de procedimentos específica* que enderecem tratativas de **segurança da informação** relacionadas à **disponibilidade** dos **ativos de informação** da **PLANMAR**.

8.3.12. Gestão de Conformidade (Controle ISO 27001 #1)

Deve ser realizada, com periodicidade mínima anual, verificação de **conformidade** das práticas de **segurança da informação** da **PLANMAR** e de suas unidades administrativas com esta *PSI* e suas *normas de procedimentos complementares*, bem como com a legislação específica de **segurança da informação.**

I. A verificação de **conformidade** deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a **PLANMAR**.

II. O calendário de ações de verificação de **conformidade** é elaborado com base na priorização dos riscos identificados ou percebidos na análise de risco.

III. A **PLANMAR** matriz ou qualquer outra unidade da **PLANMAR** que venha a ser instituída não pode permanecer sem verificação de **conformidade** de suas práticas de **segurança da informação** por período superior a 3 (dois) anos.

IV. É vedado a prestadores de serviços executar a verificação da **conformidade** de **segurança da informação** dos próprios serviços prestados.

V. A verificação de **conformidade** pode combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

VI. Os resultados de cada ação de verificação de **conformidade** são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo **Gestor de segurança da informação** ao Gestor da unidade verificada, quando houver, para ciência e tomada das ações cabíveis.

VII. Para que seja possível efetuar as verificações de **conformidade** a equipe delegada pelo CSI deve possuir acesso aos ambientes computacionais da **PLANMAR**.

8.3.13. Plano de Investimentos em Segurança da Informação da Planmar

I. Os investimentos em **segurança da informação** serão realizados de forma planejada e consolidados em um plano de investimentos plurianual.

II. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, o produtório entre a probabilidade de ocorrência e o impacto do risco no negócio ou na imagem da **PLANMAR**.

III. Os planos de investimento e seus orçamentos, são produzidos, apresentados e geridos pelo *Comitê de Segurança da Informação (CSI)*.

9. Papéis e responsabilidades referentes a segurança da informação

9.1. Comitê de segurança da informação

a) Supervisionar a segurança da informação no âmbito da **PLANMAR**;

b) Constituir a **Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI)**;

c) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre **segurança da informação;**

d) Elaborar normas específicas que complementem esta *Política* em consonância com a *Política da Estrutura Normativa PLANMAR;*

e) Conduzir apurações quando da suspeita de ocorrências e incidentes em **segurança da informação** na **PLANMAR**;

f) Avaliar e aprimorar continuamente a *PSI* e suas normas de procedimentos complementares, visando a sua aderência aos objetivos institucionais da **PLANMAR** e às legislações aplicáveis vigentes;

g) Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à *PSI*;

h) Monitorar e avaliar periodicamente o plano estratégico de **segurança da informação**, assim como determinar os ajustes cabíveis;

i) Apoiar a Alta Administração da **PLANMAR** no planejamento dos investimentos em **segurança da informação** com base nas exigências estratégicas e legais.

j) Ser responsável pela realização da Análise de Risco de Segurança da Informação.

9.2. Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI)

Cabe à **Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação (ETRISI)**:

i. Coordenar as atividades de tratamento e resposta a incidentes de segurança;

ii. Promover a recuperação de sistemas junto a área de TIC responsável;

iii. Agir pro-ativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de **segurança da informação** e avaliando condições de segurança de redes por meio de verificações de **conformidade**;

iv. Realizar ações quando do recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

v. Analisar ataques e intrusões na rede da **PLANMAR**;

vi. Executar as ações necessárias para tratar quebras de segurança;

vii. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

viii. Cooperar com outras equipes de Tratamento e Resposta a Incidentes;

k) Apurar ações que violem esta *PSI* ou quaisquer de suas diretrizes e *normas de procedimentos*. Aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor; e

ix. Participar em fóruns, redes nacionais e internacionais relativas à **segurança da informação**.

9.3.Gestor do Ativo de Informação

Cabe ao **Gestor do Ativo de Informação:**

a) Seguir as diretrizes desta Política;

b) Garantir a segurança dos **ativos de informação** sob sua responsabilidade;

c) Definir e gerir os requisitos de segurança para os **ativos de informação** sob sua responsabilidade, em **conformidade** com esta *Política;*

d) Conceder e revogar acessos aos **ativos de informação**;

e) Comunicar à **ETRISI** a ocorrência de incidentes de segurança da **informação**;

f) Designar **custodiante** dos **ativos de informação,** quando aplicável.

9.4.Custodiante do Ativo se Informação

O **Custodiante do Ativo de Informação:**

g) Deve proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em **conformidade** com esta *PSI*.

a) Deve ser formalmente designado pelo gestor do **ativo de informação.** A não designação pressupõe que o gestor é o próprio **custodiante.**

9.5.Titular da Unidade Planmar

Cabe ao Titular da Unidade PLANMAR:

a) Conscientizar os usuários sob sua supervisão em relação à **segurança da informação** da **PLANMAR**.

b) Incorporar aos processos de trabalho de sua unidade, ou de sua área, boas práticas em **segurança da informação.**

c) Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da **segurança da informação** por parte dos usuários sob sua supervisão.

d) Garantir a realização do tratamento e a **classificação da informação** definidos nas *Políticas e normas de procedimentos*.

e) Autorizar, de acordo com a legislação vigente e as diretrizes do *Comitê de Segurança da*

Informação (CSI), a divulgação das **informações** produzidas na sua unidade administrativa.

f) Comunicar à **ETRISI** os casos de **quebra de segurança.**

g) Solicitar suporte à **ETRISI** quando perceber riscos ou suspeitas de incidentes em **segurança da informação**;

h) Manter lista atualizada dos **ativos de informação** sob sua responsabilidade com seus respectivos gestores;

i) Informar o Recursos Humanos sobre a movimentação de pessoal de sua Área.

9.6. Terceiros e Parceiros Comerciais da Planmar

Cabe aos **Terceiros e Parceiros Comerciais:**

a) Tomar conhecimento e seguir as diretrizes estabelecidas pela **PLANMAR** em relação a **segurança da informação.**

b) Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos **ativos de informação,** objetos do contrato.

c) Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

10. Compliance

As atividades da **PLANMAR** devem ser realizadas cumprindo-se as normas legais e regulamentares, dos procedimentos e das boas práticas de conduta adequadas. O acompanhamento sistemático das atividades desenvolvidas é realizado de forma a avaliar se os objetivos são alcançados e cumpridos, assegurando que quaisquer desvios possam ser prontamente corrigidos.

11. Penalidades

O evento de não atendimento a esta *PSI* e aos documentos relacionados, sejam eles de forma acidental ou ilícita, deverá ser analisada e o evento ou acidente de segurança resultante, pode acarretar a instauração de procedimento administrativo disciplinar para verificar os atos e as responsabilizações do(s) envolvido(s), podendo ocorrer a aplicação de penalidades administrativas cabíveis prevista em cláusulas contratuais, código de conduta e outros documentos normativos da empresa, incluindo a legislação vigente.

12. Dúvidas e denúncias

As dúvidas e denúncias deverão ser encaminhadas em um ou mais meios de comunicação que se seguem:

- Dúvidas: e-mail csi@planmar.com.br ou formulário disponível na intranet.
- Denúncias: formulário de denúncia anônima disponível na intranet.

13. Controle de Versões/Revisões

Versão	Rev.	Data	Descrição	Autor	Função	Depto.
0	0	15/06/2023	Criação do documento	Gustavo Pilotto Diehl	Gerente de TI	T.I.C.
0	0	15/06/2023	Criação do documento	Marcelo Augusto de Arruda	Coordenador de TI	T.I.C.
0	1	04/12/2023	Revisão do documento	Marcelo Augsuto de Arruda	Coordenador de TI	T.I.C.
0	1	04/12/2023	Revisão do documento	Gustavo Pilotto Diehl	Gerente de TI	T.I.C.

14. Documentos Relacionados

Nº	Descrição	Identificação
1	PSI – Política de Segurança da Informação	TIC.SI.001

15. Identificação do Documento

Identificação: TIC.SI.001

Documento: Política de Segurança da Informação PLANMAR
Tipo de Instrumento Normativo: Política
Categoria do Assunto: Tecnologia da Informação
Assunto: Segurança da Informação
Classificação da Informação: Pública

16. Aprovação

Nome: Celso Siqueira Junior
Posição: CEO
Data: 15/12/2023