Sistema de Gestão de Segurança da Informação (SGSI)

Planejamento do SGSI

Rev.	Data	Descrição da revisão	Elaborado por	Aprovado por
6	17/08/2018	Revisão da descrição das necessidades das partes internas interessadas	Logicalis	AWD
5	08/08/2018	Atualizado estrutura de conteúdo (Objetivos de SI, Partes Interessadas e Fatores Internos e Externos)	Logicalis	AWD
4	06/08/2018	Inclusão de conteúdo referente ao item de "entradas da análise crítica". Adição de conteúdo relacionado as partes interessadas e seus requisitos, objetivos de segurança da informação e planos para alcança-los, bem como a respeito das questões internas e externas relacionadas ao SGSI e sintetização do código de conduta e ética do escritório relacionado ao sistema.	Logicalis	AWD
3	04/08/2018	Remoção da duplicidade do campo de revisão, e exclusão do campo "autorizado" da capa deste documento	Logicalis	AWD
2	18/06/2018	Revisão do documento	Logicalis	MTI
1	19/12/2017	Emissão inicial	Logicalis	

Cabe aos integrantes a responsabilidade em utilizar e controlar a revisão deste documento em papel.

Sumário

1. GLOSSÁRIO

Ameaça: Possibilidade de um agente, interno ou externo, explorar acidentalmente ou propositalmente uma vulnerabilidade específica.

Ativos de Informação: Nomenclatura utilizada para determinar os ativos pertinentes ao SGSI. Os ativos de informação são divididos em 7 categorias: Processo de Negócio, Informações, Recurso Lógico, Recurso Físico, Organização, Mídia e Espaço Físico.

Ciclo PDCA: Refere-se a *Plan*, *Do*, *Check* e *Act*. Método para melhorar/otimizar a gestão através de controles/processos eficientes.

Confidencialidade: Propriedade da informação que visa garantir que apenas pessoas ou grupos autorizados possuam acesso.

Disponibilidade: Refere-se à disponibilidade da informação para qualquer parte envolvida e no momento que for necessário o acesso a mesma.

Integridade: Propriedade da informação que visa garantir que o conteúdo da informação está completo em sua totalidade, ou seja, independente da pessoa que possua acesso à informação, o conteúdo será o mesmo.

Risco: Expectativa de perda expressada como a probabilidade de que uma ameaça possa explorar uma vulnerabilidade em particular com um resultado danoso, para o escritório.

Vulnerabilidade: Propriedade de um ativo que visa a identificação de fraquezas, as quais podem ser exploradas pelas ameaças.

2. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A **Gestão de Segurança da informação** de **Pinheiro Neto Advogados** contempla os fatores **internos e externos**, considerando as necessidades das **partes interessadas**, permeando todo o escritório, incluindo as bases estruturadas e definidas no **Código de Ética e Conduta**, na **Cultura Organizacional** e na **Proposta de Valor da Empresa**, tendo como principal responsável e patrocinador o **Sócio Gestor**, **Comitê Diretivo** e **Comissão de TI**, cabendo a cada Sócio do escritório, Gestor dos Ativos de Informação e Gestor de Segurança da Informação **estabelecer, implementar, manter e melhorar continuamente** a Gestão da **Segurança da Informação** no escritório PNA, em conjunto com todos os seus integrantes.

Para atender os seus objetivos, o escritório PNA conta com o **Sistema de Gestão de Segurança da Informação (SGSI)** e toda uma estrutura envolvendo a força de trabalho que visam oferecer a **excelência na prestação de serviço**, **a melhoria contínua da satisfação** e a **manutenção da credibilidade do escritório** perante a todos. Dessa forma, os integrantes atuam de forma rigorosa quanto à **conformidade** com os requisitos técnicos, legais e estatutários, na busca **contínua** da **melhoria** e **desempenho** do escritório.

3. ESCOPO

O **Sistema de Gestão de Segurança da Informação** do escritório **Pinheiro Neto Advogados** engloba os **ativos de informação sensíveis associados aos clientes** do escritório, armazenados na **infraestrutura e sistemas de tecnologia da informação** que suportam os processos **Jurídicos** do escritório. O mesmo está em **conformidade** com a norma **NBR ISO 27001:2013 – Sistema de Gestão de Segurança da Informação**.

4. PÚBLICO-ALVO

Este Sistema de Gestão é aplicável a todos integrantes do escritório, bem como aos parceiros, fornecedores, prestadores de serviço e aos clientes de Pinheiro Neto Advogados.

Para fins de esclarecimento, o termo “Integrantes” abrange todos Sócios, Diretores, Gerentes, Coordenadores, Consultores, Associados, Analistas, Técnicos, Secretárias, Assistentes, Auxiliares, Estagiários, Menores Aprendizes e demais cargos que possam surgir

5. ESTRUTURA DO SGSI

A estrutura do **SGSI** de Pinheiro Neto Advogados está dividida em quatro etapas que formam o **ciclo PDCA**. A ilustração abaixo representa a **Arquitetura do SGSI de PNA**.

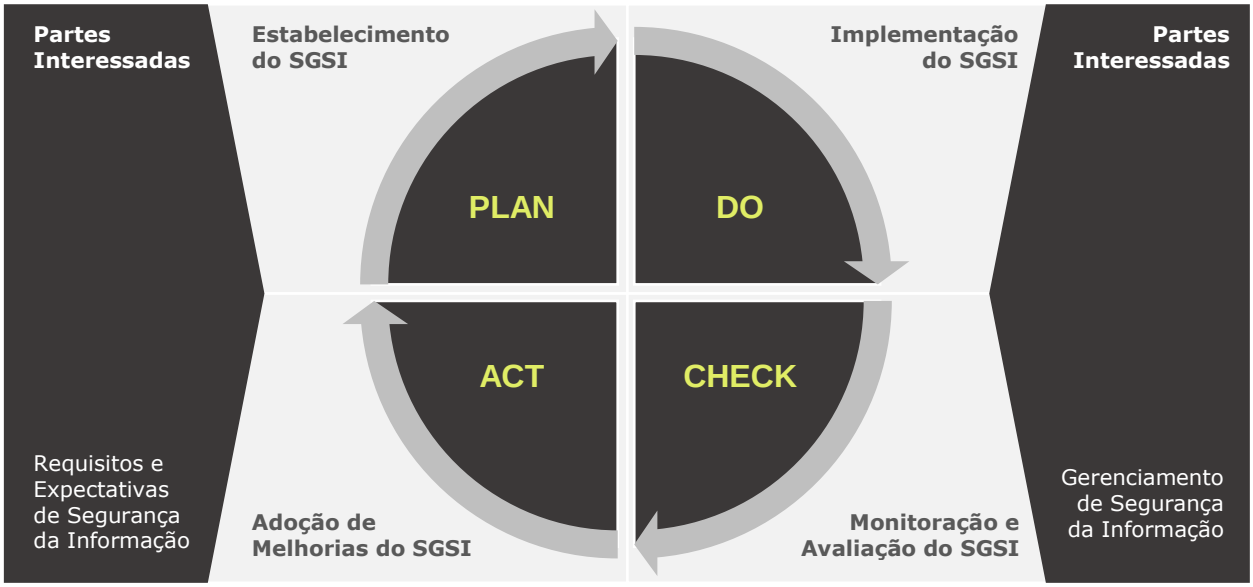

Figura 1 – Arquitetura do SGSI PNA

5.1. Planejamento (*Plan*)

5.1.1 Planejamento da Segurança da Informação

A estrutura do SGSI inicia-se com a fase Planejamento, que visa:

(a) Avaliar e documentar os fatores externos e internos relacionados ao contexto do escritório e do SGSI;
(b) Avaliar e registrar as partes interessadas e suas necessidades;
(c) Avaliar e estabelecer os objetivos de Segurança da Informação;
(d) Documentar a Política de Segurança da Informação, descrevendo a sistemática para sua comunicação, entendimento e avaliação periódica para manutenção da sua adequação;
(e) Definir a Estrutura Organizacional, descrevendo as atribuições e responsabilidades para a gestão e garantia da Segurança, bem como o processo de Comunicação que garanta a divulgação da mesma;
(f) Assegurar que o planejamento da Segurança da Informação seja realizado de forma a garantir o atendimento aos objetivos de Segurança da Informação.

5.1.2 Fatores Externos e Internos

Pinheiro Neto Advogados é um escritório brasileiro, independente, de atuação diversificada (full service), especializado em operações multidisciplinares e capaz de traduzir o ambiente legal brasileiro em benefício de seus clientes nacionais e internacionais.

Sendo o escritório parte da sociedade legal, é necessário observar quais fatores internos e externos influenciam no contexto da empresa.

Fatores Externos

Fatores Externos Relevantes	Descrição
Cenário Brasileiro	Ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico e econômico
Cenário Competitivo	Escritório com atuação no mesmo ramo ou nicho de mercado
Relações com as Partes Externas Interessadas	Relacionamento com clientes, mídias, seguradoras, fornecedores e parceiros de negócio, órgãos regulatórios e legislativos, governo e entidades do estado

Tabela 1 – Fatores Externos

Requisitos Regulatórios, Estatutários e Contratuais

Como parte complementar da tabela de fatores externos relevantes, foi desenvolvido a tabela abaixo que representa os requisitos regulatórios, estatutários e contratuais.

Categoria	Descrição
Geral / Corporativo	Constituição da República Federativa do Brasil Código Civil Brasileiro (Lei 10.406/2002) que institui a Sociedade Simples Pura (arts. 997 a 1.038) Código Tributário Nacional Marco Civil da Internet (Lei 12.964/2014)
Profissão do Advogado	OAB (Lei do Estatuto da Advocacia 8.906/1994)
Clientes	Constituição da República Federativa do Brasil Lei das licitações Código Civil Brasileiro (Lei 10.406/2002) Código de Defesa do Consumidor (Lei 8.078/1990)

Parceiros e Fornecedores	Constituição da República Federativa do Brasil Contrato de parceria Contrato de prestação de serviços e fornecimento Código Civil Brasileiro (Lei 10.406/2002) Código de Defesa do Consumidor (Lei 8.078/1990)
Integrantes	Constituição da República Federativa do Brasil Código Civil Brasileiro (Lei 10.406/2002) Consolidação das Leis Trabalhistas (CLT) Convenção coletiva de trabalho (Sindicato)

Tabela 2 – Requisitos Regulatórios, Estatutários e Contratuais

Esta tabela é construída a partir do acionamento da equipe de controladoria pelo Gestor de Segurança da Informação (GSI), a fim de identificar e avaliar o impacto dos requisitos regulatórios, estatutários e contratuais aplicáveis ao escritório.

Obs. Esta tabela representa um conjunto mínimo de leis e regulamentos aplicáveis, que podem ser complementados no âmbito das operações e de departamentos, para acomodar necessidades específicas.

Fatores Internos

Fatores Internos Relevantes	Descrição
Estrutura do Escritório	Cultura do escritório (Código de Ética e Conduta, valores, visão, missão, razões para acreditar e crenças), governança, estrutura organizacional, funções e responsabilidades
Governança Corporativa	Políticas, normas, diretrizes e modelos adotados pelo escritório, bem como objetivos e estratégias implementadas para atingi-los
Recursos e Competências	Capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias)
Fluxo das Operações	Sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais)
Relações com as Partes Internas Interessadas	Relacionamento com Alta Direção, Grupo Gestor de Segurança da Informação, Gestor de Segurança da Informação, Gestores dos ativos de informação, Integrantes e contratados

Tabela 3 – Fatores Internos

5.1.3 Partes Interessadas

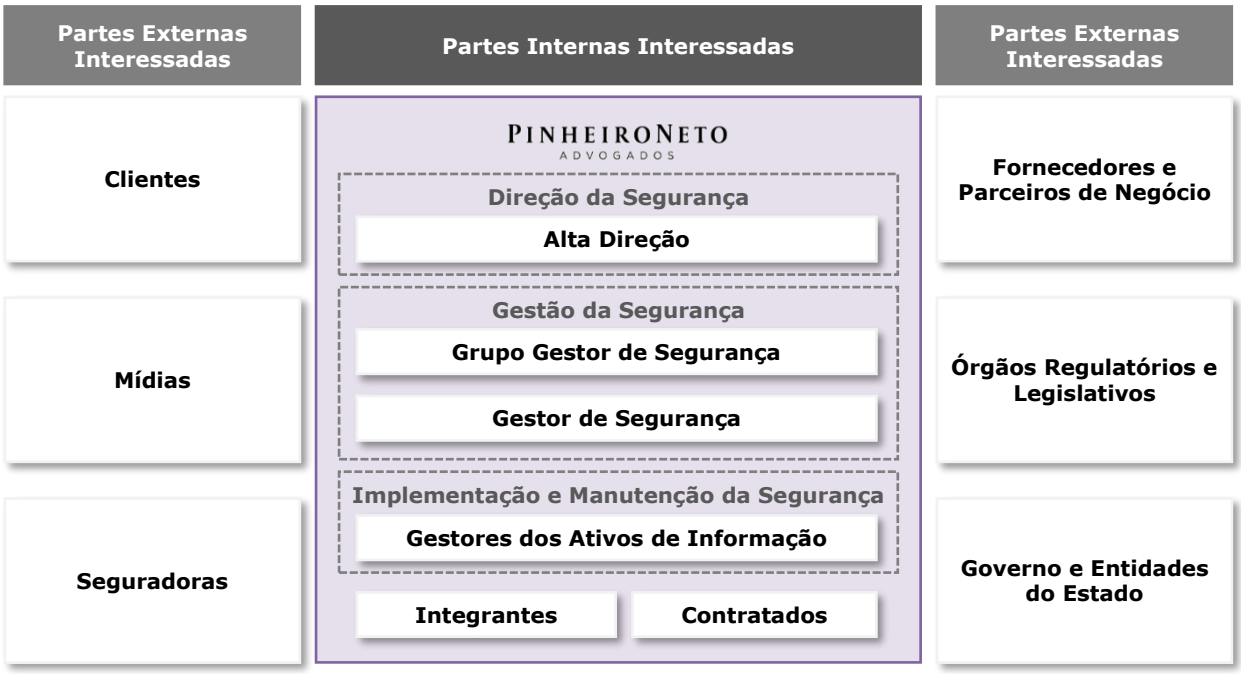

Figura 2 – Partes Interessadas

Necessidades e Requisitos das Partes Interessadas

Partes Interessadas	Necessidades e Requisitos das Partes Interessadas
Clientes	Receber o serviço contratado dentro dos padrões de qualidade e prazos acordados, respeitando a segurança e privacidade das informações compartilhadas
Mídias	Receber informações a respeito de incidentes de segurança de forma precisa
Seguradoras	Identificar controles adequados para gerir riscos e melhor avaliar prêmios de seguro oferecidos
Fornecedores e Parceiros de Negócio	Realizar os negócios em andamento, tanto no âmbito de pré-vendas, entrega e garantia
Órgãos Regulatórios e Legislativos	Fazer com que as leis e regulamentos vigentes sejam cumpridos
Governo e Entidades do Estado	Receber informações solicitadas e tributos de maneira precisa e dentro dos prazos estabelecidos
Alta Direção	Possuir um sistema capaz de manter a reputação do escritório dando respaldo a estratégia geral do negócio

Grupo Gestor de Segurança	Possuir um sistema capaz de estabelecer, implementar, manter e melhorar continuamente o SGSI e a segurança do escritório
Gestor de Segurança	Possuir um sistema capaz de gerenciar e o manter informado a respeito de incidentes e oportunidades de melhorias
Gestores dos Ativos de Informação	Manter os ativos sob sua responsabilidade, protegidos e em conformidade
Integrantes	Ter respaldo para que seu trabalho seja executado em ambiente seguro e adequado, tendo suas informações pessoais protegidas
Contratados	Ter respaldo para que seu trabalho seja adequado, em ambiente seguro, com informações pessoais protegidas e com o contrato de serviço estabelecido

Tabela 4 – Necessidades e Requisitos das Partes Interessadas

5.1.4 Objetivos de Segurança

OBJETIVO	DESCRIÇÃO DO OBJETIVO	MÉTRICAS
SIGILO	Prover o controle sobre a confidencialidade das informações que estão sob a responsabilidade do escritório	INCIDENTES DE SEGURANÇA PLANOS DE AÇÃO RELATIVOS A NÃO CONFORMIDADES, AÇÕES PREVENTIVAS E DE MELHORIA E TRATAMENTO DE RISCOS RELATÓRIOS E TESTES DE DISPONIBILIDADE, DESEMPENHO E DE VULNERABILIDADES E AMEAÇAS TREINAMENTOS E INFORMES DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO CONTROLES IMPLEMENTADOS
REPUTAÇÃO	Manter a credibilidade de PNA intacta através da proteção da informação, e dos recursos na qual as mesmas são processadas e armazenadas	
CONFORMIDADE	Garantir o cumprimento de regulamentações e legislações vigentes	
DISPONIBILIDADE	Prover a continuidade das operações e do negócio	
INTEGRIDADE	Prover a integridade das informações e confiabilidade dos recursos do escritório	
GERENCIAMENTO DO RISCO	Prover controles para administrar e mitigar riscos	
CONSCIENTIZAÇÃO	Melhorar a capacidade dos integrantes e terceiros em prevenir e reagir adequadamente a situações de risco	

Figura 3 – Objetivos de Segurança da Informação

5.1.5 Responsabilidades quanto à Segurança da Informação

É responsabilidade de cada profissional do escritório:

(a) No plano individual, desenvolver seu trabalho em sintonia com a Política de Segurança da Informação de Pinheiro Neto Advogados e com as práticas dela decorrentes;

(b) No plano coletivo, contribuir para a implementação do Sistema de Gestão da Segurança da Informação, garantindo que seus objetivos sejam estabelecidos de modo a obter a redução dos riscos aos quais os ativos de informação estão sujeitos.

Atribuição de Responsabilidades - Gestão da Segurança da Informação

Alta Direção

Formado pelo Sócio Gestor e Comitê Diretivo, tem como principais atribuições:

(a) Aprovar a Política de Segurança da Informação;
(b) Designar o representante da Alta Direção para o tema de Segurança da Informação;
(c) Explicitar seu compromisso e comprometimento com o SGSI em eventos que envolvam a comunidade;
(d) Estabelecer e formalizar as diretrizes gerais relacionadas com o tema Segurança da Informação no âmbito do escritório;
(e) Definir os objetivos estratégicos de Segurança da Informação;
(f) Tornar disponíveis os recursos necessários para a implementação e melhoria do Sistema de Gestão de Segurança da Informação (SGSI) e atingimento dos objetivos;
(g) Monitorar, por meio dos processos de melhoria contínua, o atingimento dos objetivos estratégicos de Segurança da Informação;
(h) Por meio do processo de análise crítica, avaliar a política e eficácia do SGSI;
(i) Manter a política e o SGSI adequados aos negócios do escritório Pinheiro Neto Advogados.

Os seguintes integrantes fazem parte da Alta Direção (Sócio Gestor + Comitê Diretivo) do escritório:

Função	Nome	Cargo
Sócio Gestor	Alexandre Bertoldi - ALE	Diretor Presidente
Membros do Comitê Diretivo	Angela Fan Chi Kung - KNG	Sócio Contencioso
	Antonio José Mattos Morello - MLO	Sócio Empresarial
	Giuliano Colombo - GLO	Sócio Contencioso
	Guilherme F. de Almeida Leite - GRM	Sócio Empresarial
	Marcello Alfredo Bernardes - BER	Sócio Contencioso
	Marcos de Vicq de Cumptich - VIC	Sócio Tributário
	Raphael de Cunto - RAP	Sócio Empresarial
	Renê Guilherme S. Medrado - RNE	Sócio Contencioso
	Ricardo Luiz Becker - KER	Sócio Tributário
	Vicente Coelho Araújo - AJO	Sócio Contencioso

Tabela 5 – Integrantes da Alta Direção

Grupo Gestor de Segurança da Informação

Formado pela Comissão de Tecnologia da Informação, tem como principais atribuições:

(a) Implementar e manter atualizado o SGSI;
(b) Apoiar as operações e unidades do escritório na implementação dos processos operacionais do SGSI;
(c) Canalizar as informações e propostas de melhorias do SGSI, provenientes do escritório;
(d) Implementar os planos de melhoria do SGSI no âmbito do escritório;
(e) Estabelecer e implementar programas de treinamento, comunicação e conscientização sobre o tema de Segurança da Informação;
Conduzir as auditorias internas e externas e avaliar os indicadores no âmbito do SGSI e de segurança da informação, relatando seus resultados para a Alta Direção (Sócio Gestor + Comitê Diretivo);
(f) Implementar os recursos necessários para garantir o cumprimento dos objetivos de segurança da informação;
(g) Contribuir com propostas para inserção do tema Segurança da Informação no Planejamento Estratégico do escritório.

Os seguintes integrantes fazem parte da Comissão de Tecnologia da Informação:

Função	Nome	Cargo
Comissão de Tecnologia da Informação	Alexandre Wada - AWD	Gerente de TI
	Caio Carlos Cruz F. Silva - CRZ	Sócio Empresarial
	Francisco Werneck Maranhão - FWA	Sócio Empresarial
	Ivan Pliopas - IVP	Diretor Adm. E Finanças
	Leonardo Rocha e Silva - LPS	Sócio Contencioso
	Tiago A.D. Themudo Lessa - AGO	Sócio Empresarial

Tabela 6 – Integrantes da Comissão de TI

Gestor de Segurança da Informação

Representado pelo gerente de TI, tem como principal atribuição:

(a) Representar o Grupo Gestor de Segurança (Comissão de TI) e Alta Direção (Sócio Gestor + Comitê Diretivo) em relação ao tema de Segurança da informação.

Integrante responsável pela gestão de segurança da informação:

Função	Nome	Cargo
Gestor de Segurança da Informação	Alexandre Wada - AWD	Gerente de TI

Tabela 7 – Responsável Pela Gestão de Segurança da Informação

Gestores dos Ativos de Informação

Responsáveis pelas unidades administrativas e processos de negócio, formado por integrantes de diferentes áreas, tem como principais atribuições:

(a) Responder pela implantação e manutenção do SGSI no âmbito das unidades de negócios, administrativas ou processos sob sua responsabilidade;
(b) Assegurar a implementação de ações corretivas e a manutenção de registros da Segurança da Informação;
(c) Participar dos processos de auditoria, análise crítica e melhoria do SGSI;
(d) Implementar os processos específicos de Segurança da Informação no âmbito da operação;
(e) Garantir o cumprimento das diretrizes e procedimentos estabelecidos para o SGSI.

Os seguintes integrantes fazem parte do grupo de gestores dos ativos de informação:

Função	NOME	Cargo
Gestores dos Ativos de Informação	Bianca de Cassia M. Espindola - BAS	Analista Aprimoramento
	Francisco Fabio Alves de Araújo - FAL	Supervisor de RH
	Mario Piccin - MTI	Coordenador de Infraestrutura de TI
	Mauro Norio - MNK	Coordenador de HelpDesk/Suporte
	Patricia Zanata - PZT	Coordenadora de Sistemas de TI
	Solange Passos - SGP	Coordenadora Executivo de Adm. Predial

Tabela 8 – Integrantes do Grupo de Gestores dos Ativos de Informação

5.1.6 Recursos para Segurança da Informação

Os recursos utilizados na implementação, operacionalização e melhoria do Sistema de Gestão de Segurança da Informação (SGSI) devem estar previstos no Planejamento Estratégico do

escritório. Cabe à Alta Direção (Sócio Gestor + Comitê Diretivo) definir e aprovar esses recursos.

Treinamentos específicos podem ser ministrados internamente por um profissional qualificado, ou externamente, por empresa especializada, para dar suporte à implementação e manutenção do SGSI.

5.2. Execução (*Do*)

5.2.1 Levantamento e Classificação de Ativos

O levantamento e a classificação de ativos têm como finalidade criar e manter um inventário de ativos de informação do escritório e de seus proprietários, devendo ser realizados de acordo com o escopo definido para o sistema.

A precisão das informações coletadas, durante esse processo, é fundamental para a condução de uma avaliação correta dos riscos a que esses ativos estão sujeitos, bem como para criar programas específicos de controle e acompanhamento dos riscos.

Essa atividade deve ser conduzida pelo Grupo Gestor de Segurança (Comissão de TI) ou por um profissional designado, utilizando os processos formais reconhecidos pelo escritório como referência.

A classificação dos ativos sempre irá considerar que:

(a) O valor do ativo da informação representa a sua importância;
(b) A exposição ao risco é um fator que indica o quanto o ativo está exposto às ameaças;
(c) A gravidade indica o quanto a ocorrência de um evento pode ser crítica;
(d) Probabilidade da ocorrência de ataques às vulnerabilidades;
(e) O dano à confidencialidade é o índice que representa qual o dano possível à confidencialidade do ativo de informação;
(f) O dano à integridade é o índice que representa qual o dano possível à integridade do ativo de informação;
(g) O dano à disponibilidade é o índice que representa qual o dano possível à disponibilidade do ativo de informação.

5.2.2 Gerenciamento de Riscos

Avaliação

A avaliação de risco é realizada nos ativos de informação inventariados no levantamento e classificação de ativos.

A análise de riscos permite identificar quais ativos estão mais suscetíveis a riscos em um processo, norteando a priorizarão de ações com o objetivo de reduzir o nível de risco.

O índice de risco é calculado em função do ativo de informação, observando as seguintes características:

(a) Valor do ativo;
(b) Probabilidade de uma ameaça incidir sobre vulnerabilidades conhecidas do ativo, considerando os controles já existentes.

Os níveis de risco são classificados de acordo com o índice de risco calculado, conforme os critérios descritos no procedimento "**P004 - Procedimento Análise de Riscos de Segurança da Informação**", disponível na intranet de Pinheiro Neto Advogados.

Gerenciamento

Os ativos de informação com classificação de risco de nível baixo estão dispensados de tratamento. A implementação de controles para a redução de risco desses ativos não é obrigatória. Os ativos de informação com maior índice de risco devem ser obrigatoriamente tratados e os de médio risco, opcionalmente tratados. As ações adotadas podem ser do tipo:

(a) Retenção: Aceitação do risco sem implantação de nenhum controle;
(b) Modificação: Não aceitação do risco e tratamento com controles;
(c) Evasão: Não aceitação do risco e eliminação de atividades que originam o mesmo;
(d) Compartilhamento: Transferência do risco para uma outra parte.

Tratamento de riscos

Os riscos sujeitos ao tratamento devem ser mitigados por meio da elaboração de um plano de tratamento de riscos, que deve ter como objetivo reduzi-los para níveis aceitáveis dentro de critérios estabelecidos pelo escritório.

Na medida do possível, os planos devem buscar a causa-raiz do problema identificado, permitindo sua correção. Problemas similares identificados podem ser tratados em um único plano.

Para auxílio na execução deste processo, consultar o procedimento "**P007 - Procedimento de Tratamento de Riscos**", disponível na intranet de PNA.

5.2.3 Gerenciamento de Indicadores

Alinhados aos objetivos estratégicos do escritório e ao escopo do Sistema de Gestão de Segurança da Informação (SGSI), os indicadores permitem avaliar se os objetivos do SGSI, bem como da segurança da informação foram alcançados. Eles se baseiam em:

(a) Incidentes de segurança;
(b) Planos de ação relativos a não conformidades, ações preventivas e de melhoria e tratamento de riscos;
(c) Relatórios e testes de disponibilidade, desempenho e de vulnerabilidades e ameaças;
(d) Treinamentos e informes de conscientização sobre segurança da informação;
(e) Controles implementados.

Os indicadores são avaliados periodicamente por meio de comparações históricas para:

(a) Medir a efetividade do controle a que se refere;
(b) Verificar sua validade;
(c) Identificar necessidades de criação de novos controles e respectivos indicadores.

5.2.4 Campanhas de Conscientização sobre Segurança da Informação

As atividades, ações e campanhas relacionadas com o Sistema de Gestão de Segurança da Informação serão divulgadas em palestras, reuniões, treinamentos e na Intranet de Pinheiro Neto Advogados.

A Política da Segurança da Informação está publicada na intranet de Pinheiro Neto Advogados.

5.3. Monitoração e Melhoria Contínua (*Check*/*Act*)

5.3.1 Medição, Análise dos Controles e Planos de Melhorias de SI

O escritório Pinheiro Neto Advogados adota práticas de monitoramento, medição, análise e melhoria com o objetivo de assegurar a segurança da informação corporativa e melhorar continuamente a eficácia de seu Sistema de Gestão da Segurança da Informação (SGSI).

A medição e o monitoramento ocorrem no âmbito do SGSI e eventos de controle são aplicados ao longo de diferentes processos, possibilitando a medição e tomada de ação, quando aplicável.

A consolidação e o tratamento aplicado são fundamentalmente acompanhados por:

(a) Avaliação dos incidentes de segurança da informação;
(b) Auditorias internas;
(c) Ações corretivas;
(d) Ações preventivas;
(e) Análise crítica da Direção (Sócio Gestor + Comitê Diretivo).

Avaliação dos incidentes de segurança da informação

A Segurança da Informação é monitorada continuamente em todos os processos por meio das notificações de incidentes de segurança. As notificações são feitas por diferentes canais e têm a finalidade de propor um tratamento adequado para os problemas encontrados.

Os incidentes são avaliados pelo gestor de segurança da informação, em função de sua criticidade e de seu impacto potencial, e devem ser compilados e apresentados ao Grupo

Gestor de Segurança (Comissão de TI) e Alta Direção (Sócio Gestor + Comitê Diretivo) como instrumento de análise e melhorias para os ciclos de Planejamento Estratégico.

Ações corretivas devem ser implementadas no âmbito do processo da cadeia de valor e acompanhadas pelo Sistema de Gestão da Segurança da Informação.

Auditorias Internas

A auditoria interna é um instrumento gerencial para avaliar o planejamento, a aplicação, a efetividade e a adequação dos elementos do Sistema de Gestão da Segurança da Informação (SGSI) estabelecidos e aplicados na realização do processo da cadeia de valor.

A auditoria da segurança da informação tem por objetivo principal permitir uma informação independente e confiável da situação operacional do Sistema de Gestão de Segurança da Informação no instante da auditoria, contribuindo, dessa forma, para a prevenção de não conformidades e para a melhoria do desempenho da organização.

As auditorias internas são conduzidas sob a coordenação do gestor de segurança da informação e de acordo com o procedimento "**P002 - Procedimento Auditoria Internas de SGSI**".

Ações corretivas

Considerações gerais quanto às ações corretivas:

As ações corretivas devem ser implementadas em não conformidades apontadas em auditorias, reclamações formais de clientes e quando identificado oportunidade de melhorias durante análise/revisão de processos.

O conjunto de ativos não conforme identificados no dia a dia das operações, possivelmente podem resultar na necessidade de aplicação de ações corretivas, dependendo dos possíveis problemas que os mesmos possam trazer para o escritório em relação a criticidade e riscos envolvidos.

Para os casos no qual não existam tratamentos específicos, é recomendável a utilização do formulário "**F001 - Plano de Ação Corretiva Preventiva e de Melhoria – PACPM**", disponível na intranet de Pinheiro Neto Advogados.

Fontes de informação

Para propostas de ações corretivas, devem ser consideradas as seguintes fontes de informação:

(a) Relatórios de auditoria internas e externas;
(b) Reclamações formais de clientes;
(c) Registros de não conformidade de ativos de informação;
(d) Relatórios de avaliação de fornecedores;
(e) Relatórios de inspeção.

Investigação das causas

As causas de não conformidades devem ser investigadas e analisadas criticamente pelo gestor do ativo de informação. Caso o mesmo não tenha conhecimento ou habilidades para lidar com o item observado, cabe ao mesmo indicar pessoal adequado para esta atividade. Além disso, devem ser envolvidos o gestor de segurança da informação e demais partes envolvidas/interessadas no ativo de informação não conforme.

Plano de ação

As ações corretivas propostas devem ter como direcionamento a eliminação da causa raiz do problema, devendo ser as mais abrangentes possíveis, porém proporcionais aos riscos e magnitude dos problemas que se pretende sanar.

Deve ser considerada a possibilidade de eventual elaboração ou revisão de procedimentos/políticas e de treinamento para as pessoas envolvidas.

Os planos de ação devem identificar os responsáveis e estabelecer datas limite para implementação das ações. Convém que seja determinada uma data para a verificação da eficácia das ações implementadas.

Implementação e eficácia

É de total responsabilidade do gestor que estabeleceu o plano de ação assegurar a implementação do mesmo no prazo determinado e registrar as atividades de acompanhamento.

Para o fechamento do processo, deve ser feito um análise crítica e avaliação da eficácia das ações providenciadas. Por ação eficaz, entende-se que o item causador da não conformidade foi eliminado completamente, não havendo evidências para que o mesmo volte a ocorrer.

É importante observar que cada situação possui sua peculiaridade. Por isso, convém que a eficácia da ação corretiva aplicada, seja revista seis meses após sua implementação, considerando o término ou encerramento dos eventos envolvidos.

Obs. Para o plano de ação decorrente de não conformidade de auditoria, externa ou interna, ver "**P002 - Procedimento Auditoria Internas de SGSI**".

Ações preventivas

Considerações gerais quanto às ações preventivas

As ações preventivas visam eliminar/mitigar as causas de uma possível não conformidade ou situação indesejável que possa vir a ocorrer.

É de interesse dos gestores de ativos de informação, bem como do gestor de segurança da informação, Grupo Gestor de Segurança (Comissão de TI) e Alta Direção (Sócio Gestor + Comitê Diretivo) identificar ações preventivas durante o acompanhamento de processos rotineiros a fim de observar potenciais ocorrências de não conformidade ou necessidade de melhoria do processo.

A iniciativa e análise dos processos de Pinheiro Neto Advogados é de responsabilidade dos gestores dos ativos de informação, porém todos os integrantes devem ser incentivados a colaborar e propor ações preventivas e de melhoria a seus respectivos gestores de ativos de informação, os quais deverão analisar e documentar as mesmas quando aplicável.

O procedimento para a aplicação das ações preventivas é semelhante ao das ações corretivas, a diferença está no fato de que, neste último, o problema já ocorreu.

É recomendável a utilização do formulário "**F001 - Plano de Ação Corretiva Preventiva e de Melhoria – PACPM**", disponível na intranet de Pinheiro Neto Advogados. Para propostas de ações preventivas, devem ser consideradas as seguintes fontes de informação:

(a) Resultado do processo de análise de risco das operações;
(b) Processos e atividades que afetaram a qualidade do serviço;
(c) Relatórios de auditoria internas e externas;
(d) Reclamações formais de clientes;
(e) Relatórios de avaliação de fornecedores;
(f) Relatórios de inspeção.

Plano de ação

As ações preventivas propostas devem ter como direcionamento a eliminação/mitigação da causa raiz do problema, devendo ser as mais abrangentes possíveis, porém proporcionais aos riscos e magnitude dos problemas que se pretende sanar.

Assim como para os planos de ação corretivas, os planos de ação preventivas devem considerar a possibilidade de eventual elaboração ou revisão de procedimentos/políticas e de treinamento para as pessoas envolvidas.

Os Planos de ação devem identificar os responsáveis e estabelecer datas limite para implementação das ações. Convém que seja determinada uma data para a verificação da eficácia das ações implementadas.

Implementação e eficácia

É de total responsabilidade do gestor que estabeleceu o plano de ação assegurar a implementação do mesmo no prazo determinado e registrar as atividades de acompanhamento.

Para o fechamento do processo, deve ser feito um análise crítica e avaliação da eficácia das ações providenciadas. Por ação eficaz, entende-se que evitou a ocorrência do problema que se propunha evitar, em um período razoável de observação.

É importante observar que cada situação possui sua peculiaridade. Por isso, convém que a eficácia da ação preventiva aplicada, seja revista seis meses após sua implementação, considerando o término ou encerramento dos eventos envolvidos.

Análise Crítica da Direção

As atividades de análise crítica do Sistema de Gestão da Segurança da Informação (SGSI) são planejadas anualmente pela Gerência de Segurança da Informação de Pinheiro Neto Advogados e analisadas criticamente pela Alta Direção (Sócio Gestor + Comitê Diretivo) e Grupo Gestor de Segurança da Informação (Comissão de TI), de forma a assegurar sua contínua pertinência.

Entradas para a análise crítica

As entradas para a análise crítica pela Alta Direção (Sócio Gestor + Comitê Diretivo) devem incluir informações sobre adequação e eficácia do SGSI, incluindo a análise crítica da Política da Segurança da Informação e dos objetivos da segurança da informação, bem como a respeito de:

(a) Acompanhamento das ações oriundas das análises críticas anteriores;
(b) Mudanças internas e externas relevantes para o SGSI;
(c) Desempenho do sistema;
(d) Monitoramento das ações preventivas e corretivas;
(e) Monitoramento e resultados da medição;
(f) Resultados das auditorias internas e externas;
(g) Cumprimentos dos objetivos de segurança da informação;
(h) Realimentação das partes interessadas;
(i) Resultados da avaliação dos riscos e situação dos planos de tratamento de risco;
(j) Recomendações para melhoria.

Saídas da análise crítica

As saídas para a análise crítica pela Alta Direção (Sócio Gestor + Comitê Diretivo) devem incluir informações sobre decisões e ações relacionadas a:

(a) Melhoria da eficácia do SGSI e de seus processos;
(b) Melhoria da segurança da informação;
(c) Necessidades de recursos.

6. REVISÃO DO PROCESSO

Para garantir a efetividade dos processos relacionados ao SGSI, é necessário a revisão periódica, conforme critérios da tabela abaixo:

Periodicidade	Descrição da Periodicidade
Anualmente	Executar anualmente para avaliar a conformidade e proporcionar melhorias para o sistema
Eventualmente	Executar quando houver alguma adição/alteração/exclusão de itens específicos
Exclusivamente	Executar quando houver uma mudança significativa de escopo de negócio do escritório ou quando solicitado pela alta direção

Tabela 9 – Periodicidade de Atualização

O **calendário de segurança da informação** de Pinheiro Neto Advogados, possui datas específicas para avaliação dos itens relacionados ao Sistema de Gestão de Segurança da Informação.