POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Controle do Documento			
Código:	PENSO_SGSI_PO_001 - Resumida	**Periodicidade:**	Anual
Revisão:	19/03/2024	**Versão:**	V 1.2
Elaborador(es):	Fernando Lima	**Aprovador(es):**	Erik Morais
Revisor(es):	CSGSI	**Classificação:**	PUBLICO
Gestão do Documento:	Sistema de Gestão de Segurança da Informação		

Sumário

1 Introdução

Esse documento tem os objetivos de prover um ambiente protegido em termos de segurança da informação baseado nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 e nas boas práticas descritas na ISO/IEC 27002:2013. Além disso, essa política da segurança da informação também tem o objetivo de estar em conformidade com as leis brasileiras. Com isso a PENSO TECNOLOGIA decide implantar um plano do SGSI (Sistema de Gestão de Segurança da Informação), onde a estrutura e diretrizes de segurança de informações são expressas nesse documento.

2 Escopo

A Política de Segurança da Informação e o Plano do Sistema de Gestão de Segurança da Informação formam a base para o estabelecimento dos padrões e procedimentos de segurança da PENSO TECNOLOGIA, abrangendo os seus sistemas e ambientes de Tecnologia da Informação.

É destinada a todos os seus funcionários e parceiros prestadores de serviços, que atuam sob contrato, e que, nas suas atribuições e/ou execução do contrato, fazem uso de informações de negócio ou administrativas.

3 Objetivo

A PENSO TECNOLOGIA em razão de seu compromisso com a proteção das Informações de sua propriedade, estabelece diretrizes para proteção dos ativos de informação e níveis aceitáveis de confiabilidade, devendo ser observadas por todos os seus colaboradores.

De modo geral, esta política resume os princípios de Segurança da Informação que a PENSO TECNOLOGIA reconhece como sendo importantes, devendo estar presentes no cotidiano de suas atividades. Assim, visa assegurar a confidencialidade, disponibilidade e integridade do processamento, transferência, manuseio e armazenamento das informações críticas que estão no escopo do Sistema de Gestão de Segurança da Informação (SGSI). Os objetivos definidos desta política são:

- Manter avaliações de riscos de segurança da informação dentro do escopo do SGSI de acordo com a Norma de Gestão de Riscos da PENSO TECNOLOGIA;
- Manter os níveis aceitáveis de risco residual para a organização;
- Garantir níveis aceitáveis de confidencialidade, integridade e disponibilidade das informações críticas;
- Atender aos requisitos regulamentares e legislativos;

- Realizar o treinamento e a conscientização da segurança da informação para todos os funcionários e prestadores de serviço da PENSO TECNOLOGIA;
- Relatar a avaliação de todas as violações da segurança da informação e vulnerabilidades para as partes interessadas;
- Apoiar a manutenção da norma do Sistema de Gestão De Segurança da Informação: ISO 27001 – Gestão da Segurança da Informação de forma a suportar a implementação de outras normas de padrão ISO.

A Política de Segurança da Informação também demonstra o comprometimento de seguir com os objetivos de Segurança de Informação descritos no Plano do Sistema de Segurança da Informação.

Todos os funcionários e prestadores de serviço que tenham qualquer envolvimento com os ativos e informações críticas coberto pelo escopo do SGSI são responsáveis por seguir suas políticas, diretrizes, normas e procedimentos de gestão da PENSO TECNOLOGIA.

4 Princípios de segurança da informação

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

Integridade: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, no processo, transporte e armazenamento, contra alterações indevidas, intencionais ou acidentais.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Toda informação deve ser protegida conforme as regras definidas nesta Política. A adoção de procedimentos que garantam a segurança da informação deve ser prioridade constante nas áreas da PENSO TECNOLOGIA, de forma que se possa reduzir falhas e danos que venham a comprometer a imagem da empresa ou trazer prejuízos a outrem.

Toda informação produzida ou recebida pelos funcionários, estagiários e prestadores de serviço como resultado de sua atividade profissional, ou em razão dela, pertence à PENSO TECNOLOGIA.

As exceções devem ser explícitas e formalizadas em contrato entre as partes. Isto também se aplica para os equipamentos de informática, comunicação, sistemas, informações e qualquer recurso utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos e equipamentos é permitido desde que esteja devidamente autorizado e não prejudique o desempenho dos sistemas e serviços da PENSO TECNOLOGIA.

A PENSO TECNOLOGIA, por meio da Segurança da Informação e outras áreas ligadas ao tema, poderá registrar e monitorar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Os critérios e requisitos estabelecidos nesta PSI deverão ser aplicadas em todas as áreas da PENSO TECNOLOGIA.

5 Proteção da informação

Define-se como necessária a proteção da informação da empresa, especialmente, de sua propriedade e informação imprescindível como fator primordial nas atividades profissionais de cada colaborador da PENSO TECNOLOGIA, sendo que:

- Os colaboradores devem assumir uma postura proativa no que diz respeito à proteção das informações da PENSO TECNOLOGIA e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido aos sistemas de informação sob responsabilidade da PENSO TECNOLOGIA;
- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções e autorizações;
- Assuntos sigilosos classificados com confidenciais não devem ser expostos publicamente;
- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- Somente softwares homologados podem ser utilizados no ambiente computacional da PENSO TECNOLOGIA;
- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
- Todo usuário, para poder acessar dados das redes de computadores utilizadas pela PENSO TECNOLOGIA, deverá possuir um login ou usuário de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de login ou usuário de acesso genérico ou comunitário, exceto previamente autorizado;
- Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;
- Todos os dados considerados como imprescindíveis aos objetivos da PENSO TECNOLOGIA devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos aos testes periódicos de recuperação;
- O acesso físico às dependências da PENSO TECNOLOGIA deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade, garantindo a rastreabilidade e a efetividade do acesso autorizado;

- O acesso lógico aos sistemas computacionais disponibilizados pela PENSO TECNOLOGIA deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;
- São de propriedade da PENSO TECNOLOGIA todas as criações, códigos ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo com a empresa, nos limites legais (Leis nº 9.279/96, 9.609/98 e as demais aplicáveis).
- Documentos imprescindíveis para as atividades da empresa deverão ser salvos em nuvem nos produtos da PENSO TECNOLOGIA como o Penso vBox e o Pensomail Zimbra. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no mesmo, sendo, portanto, de responsabilidade do próprio colaborador.
- Arquivos pessoais e/ou não pertinentes às atividades diretas da PENSO TECNOLOGIA não deverão ser copiados ou movidos para os produtos de nuvem, pois podem sobrecarregar o armazenamento da infraestrutura de datacenter. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao colaborador.
- Os projetos gerenciados e realizados pela PENSO TECNOLOGIA deverão adotar critérios de segurança da informação para o cumprimento desta política.

6 Privacidade da informação

Define-se como necessária a privacidade das informações que são manipuladas ou armazenadas nos meios às quais a PENSO TECNOLOGIA detém total controle administrativo, físico, lógico e legal. As diretivas abaixo refletem os valores institucionais da PENSO TECNOLOGIA e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são geradas, manipuladas, recebidas, tratadas e armazenadas de forma segura e íntegra, com métodos apropriados de segurança, podendo utilizar criptografia ou certificação digital, quando aplicável;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- As informações podem ser disponibilizadas a quem tem direito de acesso, sendo exigido o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
- As informações somente são fornecidas a terceiros, mediante autorização prévia da PENSO TECNOLOGIA, ou do cliente, ou para o atendimento de exigência legal ou regulamentar;

- As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

7 Data Center

Define-se como necessário, as seguintes diretrizes da PENSO TECNOLOGIA:

- A administração de dados e de serviços de data center é tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.
- O acesso físico ao data center deverá ser feito por sistema forte de autenticação. O acesso físico por meio de recursos mecânicos-manuais apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.
- O acesso ao data center por visitantes ou terceiros somente poderá ser realizado com autorização de um colaborador da PENSO TECNOLOGIA, que deverá preencher a solicitação de acesso prevista, conforme estabelecida na norma própria.
- Deverá ser executada, em frequência predeterminada, auditoria dos acessos ao datacenter – por meio de relatório do sistema de registro próprio.
- A lista de funções com direito de acesso ao data center deverá ser constantemente atualizada, de acordo com os termos de norma própria, salva em locais seguros e apropriados.
- No caso de desligamento de usuários que possuam acesso ao data center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de usuários autorizados.

8 Tratamento de incidentes de Segurança da Informação

Define-se como necessário, as seguintes diretrizes da PENSO TECNOLOGIA:

- Todos os incidentes de segurança da informação notificados ou detectados deverão ser registrados, com a finalidade de assegurar o histórico das atividades desenvolvidas.
- O tratamento de incidentes de segurança da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade e confidencialidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.
- Durante o gerenciamento de incidentes de segurança da informação, havendo indícios de ilícitos criminais, a Equipe Governança, ou Recursos Humanos, ou Departamento Pessoal, ou

membros da Equipe Técnica ligadas as atividade de segurança da Informação tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da PENSO TECNOLOGIA.

9 Regulamentação e legislação aplicáveis

Correlacionam-se com a política, diretrizes e normas do Sistema de Gestão De Segurança da Informação as leis abaixo relacionadas, mas não se limitando às mesmas:

- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988;
- CÓDIGO TRIBUTÁRIO NACIONAL pelo art. 7º do Ato Complementar nº 36, de 13.3.1967;
- CONSOLIDAÇÃO DAS LEIS DO TRABALHO -DECRETO-LEI N.º 5.452, DE 1º DE MAIO DE 1943 alterada pela Lei Federal 13.467/2017;
- Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
- Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias);
- LEI Nº 9.472, DE 16 DE JULHO DE 1997;
- Lei de direito autoral Nº 9610/98;
- Lei de marcas e patentes Nº 9.279 de 14/05/1996;
- Lei das telecomunicações Nº 9.472 de 16/07/1997;
- Lei de propriedade intelectual de programa de computador Nº 9.609 de 19/02/1998;
- LEI Nº 12.737 - Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
- Lei Nº 12.965 de 23/04/2014 (Marco Civil da Internet).
- Lei 8666/95 - Lei de Licitação
- Lei 12.846 - Lei anticorrupção
- ABNT NBR ISO/IEC 27001 – 2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos
- ABNT NBR ISO/IEC 27005 - 2008 - Tecnologia de Informação - Técnicas de segurança - Gestão de riscos de segurança da informação
- ABNT NBR ISO/IEC 31000 – 2009 – Gestão de Riscos – Princípios e Diretrizes.

- Lei Geral de Proteção de Dados – 13.709

O Sistema de Gestão De Segurança da Informação estabelece responsabilidade, regras e realiza ações de melhorias para evitar violações de aspectos legais e regulamentares de requisitos de segurança da informação sendo elas:

- Decisões que incluem obrigações legais;
- Projeções de custo-benefício para o sistema de gestão e serviços;
- Análise de risco e benefícios intangíveis para o sistema de gestão e serviços, bem suas obrigações éticas com o conteúdo dos dados.