Este documento detalha a Política do Sistema de Gestão da Segurança da Informação – SGSI da Fundação de Seguridade Social Braslight.

A Fundação de Seguridade Social Braslight, em consonância com sua missão de administrar planos previdenciários, garantindo aos seus participantes e beneficiários, segurança e qualidade na concessão e manutenção de seus benefícios, observando as expectativas de suas patrocinadoras, reconhece que a proteção da confidencialidade, da integridade e da disponibilidade das suas informações contra vários tipos de ameaças, a garantia da continuidade dos seus negócios, bem como a qualidade e a excelência dos seus processos, são partes integrantes do desempenho empresarial e responsabilidade fundamental da direção da empresa.

As diretrizes quanto ao alinhamento estratégico com os requisitos de negócio e o estabelecimento dos objetivos e responsabilidades pela gestão desta Política são:

- A Fundação Braslight atribui grande importância à segurança de seus ativos físicos, de informação, pessoas, sistemas, processos e qualquer outro ativo de propriedade da Fundação;
- A Política do SGSI, estabelecida pela alta direção da empresa e cuja gestão é feita pelo Grupo de Segurança da Informação deve ser comunicada aos seus funcionários e aos terceiros contratados para atuar na gestão da área de Tecnologia da Informação;
- A segurança das informações a ser garantida leva em consideração os requisitos e obrigações de segurança contratuais, legais e/ou regulamentares a que a Braslight, uma entidade fechada de previdência complementar, tem que atender, bem como os riscos envolvidos;
- Para promover a adequada proteção dos ativos, a Fundação implantou o Sistema de Gestão da Segurança da Informação, estabelecido a partir do contexto estratégico da gestão de riscos em segurança da informação;
- Os funcionários e colaboradores da Fundação devem assumir a responsabilidade pessoal de proteger os ativos de informação, cumprindo as políticas e normas de segurança e relatando eventuais ameaças ou violações de segurança contrárias às definições do SGSI;

- Os gestores dos ativos de informação devem proteger os mesmos assegurando que as pessoas que têm acesso a estes ativos estão conscientes do seu papel na segurança organizacional, conhecem suas responsabilidades e estão capacitadas para alcançar os objetivos de segurança;
- A gestão dos riscos em segurança da informação ocorre a partir da identificação, avaliação e tratamento, de forma regular, das ameaças e riscos relativos à segurança da informação.

Os critérios estabelecidos para a avaliação de riscos foram estabelecidos segundo as seguintes diretrizes:

- A Fundação Braslight entende que a capacidade de manutenção dos níveis de serviço aos participantes depende da manutenção da integridade, confidencialidade e disponibilidade dos ativos de informação;
- A manutenção da confiança quanto aos serviços prestados depende diretamente do tratamento adequado das ameaças, com a eliminação dos riscos que possam afetar a continuidade dos negócios e a reputação da Fundação Braslight;
- Novas tecnologias a serem adotadas devem ser avaliadas quanto aos potenciais riscos antes de terem sua adoção aprovada;
- Mesmo que ofereçam vantagens, novas tecnologias com riscos inaceitáveis não devem ter sua adoção aprovada;
- A avaliação dos riscos deve ser realizada de forma a garantir a continuidade dos negócios e operações da Fundação, através da adoção de controles que minimizem ou eliminem totalmente o impacto de incidentes de segurança da informação;
- A análise de riscos deve ser realizada de forma que controles sejam implementados para que todos os ativos sejam protegidos de forma adequada e a divulgação de informações seja restrita às pessoas autorizadas.

Os controles a serem adotados pelo SGSI após a análise de riscos devem:

- Assegurar que somente pessoas autorizadas tenham acesso às informações e aos sistemas de informação da companhia;

- Proteger as informações e os sistemas de informação contra modificações não autorizadas;
- Registrar, analisar e investigar os incidentes de segurança da informação e criar mecanismos de prevenção para evitar a sua ocorrência;
- Proteger os processos críticos contra falhas ou desastres significativos para garantir a continuidade de seus negócios;
- Atender aos requisitos regulamentares e legais aplicáveis;
- Conscientizar, educar e treinar os usuários quanto às políticas e normas de segurança da informação da empresa;
- Melhorar continuamente o Sistema de Gestão da Segurança da Informação.

Esta Política deve ser revista ao menos anualmente e de forma ordinária a cada auditoria do Sistema de Gestão da Segurança da Informação.