POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Finalidade, escopo e usuários

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação no Senac/ES.

Esta política aplica-se a todo o Sistema de Gestão da Segurança da Informação e Privacidade (SGSI).

Os usuários deste documento são colaboradores do Senac/ES, assim como as partes externas relevantes.

2. Terminologia básica de segurança da informação

Confidencialidade – Assegura que as informações, sistemas e recursos sejam acessíveis apenas a indivíduos, processos ou entidades autorizadas, prevenindo vazamentos, exposição indevida ou acesso não autorizado.

Integridade – Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Disponibilidade – Assegura que os sistemas, dados e serviços estejam acessíveis e operacionais sempre que necessário, garantindo a continuidade dos negócios mesmo em cenários de falhas ou ataques.

Segurança da informação – preservação da confidencialidade, integridade e disponibilidade da informação

Sistema de Gestão da Segurança da Informação e Privacidade – é um conjunto de políticas, procedimentos e tecnologias utilizadas para gerenciar e proteger os ativos associados com informação e dados pessoais de uma organização.

3. Gerenciando a segurança da informação

3.1. Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são os seguintes:

- Atender as exigências da Alta Direção relacionadas às demandas de mercado para a área de segurança da informação;
- Conscientizar os colaboradores sobre a importância da segurança da informação;
- Garantir a eficácia dos controles de segurança aplicáveis para assegurar a confidencialidade, integridade e disponibilidade das informações.

3.2. Requisitos de segurança da informação

Esta Política e deve estar em conformidade com os requisitos legais e regulamentares levantes à organização na área de segurança da informação, bem como com as obrigações contratuais.

3.3. Responsabilidades

As responsabilidades básicas para o SGSIP são:

- O DPO deve:
    - Garantir que a gestão da privacidade seja realizada em conformidade com esta Política e possua todos os recursos necessários.
    - Gerenciar e reportar sobre o desempenho de privacidade.
    - Reportar ao Diretor Regional sobre quaisquer preocupações relacionadas à Segurança da Informação.
- A equipe de Segurança da Informação deve:
    - Propor metodologias, processos e iniciativas que visem à segurança da informação.
    - Promover a conscientização dos funcionários em relação à relevância da segurança da informação para o Senac/ES, através de ações conjuntas com o RH.
    - Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
    - Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínio necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- A equipe de Suporte de TI deve:
    - Configurar os equipamentos, ferramentas e sistemas concedidos aos funcionários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e pelas normas de segurança da informação complementares.
    - Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Senac/ES.
- Gestores de Pessoas e/ou Processos devem:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os funcionários sob a sua gestão.
- Verificar se os funcionários sob sua gestão, na fase de contratação e de formalização dos contratos individuais de trabalho e de prestação de serviços foram informados desta política e se foi coletado o aceite.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política de segurança da informação.

- Os usuários da Informação devem:
  - Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança do SGSIP.
  - Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, e das normas e procedimentos de Segurança da Informação.
  - Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.
- A proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário de cada ativo.
- Todos os incidentes e as fragilidades de segurança devem ser reportados a equipe de Segurança da Informação, que irá definir quais informações relativas à segurança da informação serão comunicadas para qual parte interessada internamente e externamente, por quem e quando.

3.4. Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao Senac/ES, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais.

4. Suporte para a implementação do SGSIP

Deste modo, a alta direção do Senac/ES declara que a implementação do SGSIP e seu contínuo aprimoramento serão suportadas pelos recursos apropriados

para alcançar todos os objetivos definidos nesta Política, assim como atender todos os requisitos identificados.