PSI – Política de Segurança da Informação

Exercício 2022-2023

Gerência de Tecnologia da Informação – Senac AL

V.2.0

Índice

1 – Introdução

Este documento declara o comprometimento da diretoria em estabelecer a PSI - Política de Segurança da Informação do Senac Alagoas, que é um conjunto das diretrizes, normas e procedimentos necessários à preservação e segurança dos bens de informação utilizados na empresa.

São bens de informação os seguintes componentes da TI - Tecnologia da Informação: sistemas aplicativos desenvolvidos e adquiridos, softwares básicos e de apoio, dados, hardware, instalações físicas, equipamentos de infraestrutura e documentos em qualquer forma de armazenamento.

Conforme definição da norma **NBR ISO/IEC 27001**, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A segurança da informação objetiva proteger a informação de diversos tipos de ameaças, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

2 - Objetivo

Estabelecer diretrizes que permitam aos colaboradores e clientes do Senac Alagoas seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Estabelecer políticas, normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

3 – Escopo e Abrangência

O escopo e abrangência dessa política de segurança da informação engloba não apenas os requisitos de segurança lógica, mas também os de segurança física, segurança dos processos e de pessoal, direta ou indiretamente relacionados com todos os departamentos da empresa.

4 – Integração com os Procedimentos Existentes

Os seguintes documentos são parte integrante dessa política e devem ter todo o seu conteúdo respeitado como todas as regras e diretrizes aqui descritas:

- Política de Privacidade Interna;
- Política de Privacidade Externa;
- Política de Proteção de Dados Pessoais;
- Termo de Confidencialidade dos Colaboradores;
- Contrato de Trabalho;
- Contratos com Fornecedores;

5 – Aplicações da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

6 – Princípios da PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo Senac Alagoas pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é
permitido desde que não prejudique o desempenho dos sistemas e serviços.

O Senac Alagoas, por meio da Gerência de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Os seguintes princípios são endereçados por esse documento:

- **Confidencialidade:** Somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;
- **Integridade:** A informação deve sempre ser alterada de forma íntegra para não gerar falsas interpretações;
- **Disponibilidade:** A informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;
- **Autenticidade:** Princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;
- **Criticidade:** Princípio de segurança que define a importância da informação para a continuidade da atividade fim da organização;
- **Não-Repúdio:** Garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;
- **Responsabilidade:** As responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.
- **Conhecimento:** Todos os colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência de normas,

procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

- **Ética:** todos os direitos e interesses legítimos de colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação devem ser respeitados;
- **Legalidade:** as ações de Segurança da Informação levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;

7 – Diretrizes

As seguintes diretrizes de alto nível serão utilizadas como origem dessa política, norteando todo o documento:

- **D1** - Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
- **D2** - Assegurar que os recursos colocados à disposição dos colaboradores sejam utilizados apenas para as finalidades aprovadas pela organização;
- **D3** - Garantir a continuidade dos negócios;
- **D4** - Atender às leis que regulamentam as atividades da organização e seu mercado de atuação;
- **D5** - Selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- **D6** - Comunicar imediatamente ao Comitê qualquer descumprimento da política corporativa de segurança da informação;
- **D7** – Inventariar e proteger os ativos de informação, além de ter os seus proprietários identificados;
- **D8** – Analisar os principais processos de negócios sob a ótica da segurança da informação, ajustando-os de acordo com as melhores práticas;

8 – Estrutura normativa

A estrutura normativa da Segurança da Informação do Senac Alagoas é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política):** Constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- **Normas de Segurança da Informação (Normas):** Estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- **Procedimentos de Segurança da Informação (Procedimentos):** Instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da empresa.

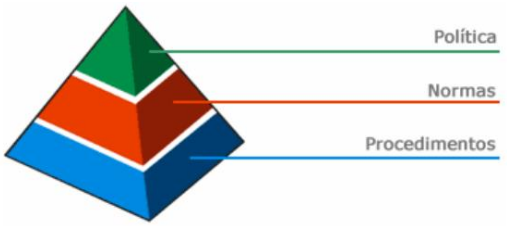

Figura 01 – Estrutura normativa da Segurança da Informação.

9 – Análise dos Processos de Negócio

Para o perfeito entendimento do funcionamento da empresa, em busca das customizações e ajustes necessários pelas boas práticas de segurança, foi feito o mapeamento dos principais processos de negócio existentes. Esses processos foram detalhadamente analisados, pela ótica da segurança da informação, e as sugestões de melhoria foram registradas no plano de ações para adequação à LGPD. Cada ação desse plano possui uma data limite para implementação e responsável, detalhados em outro documento que foi apresentado à diretoria da empresa. A figura a seguir demonstra, de forma macro, quais processos de negócio foram analisados:

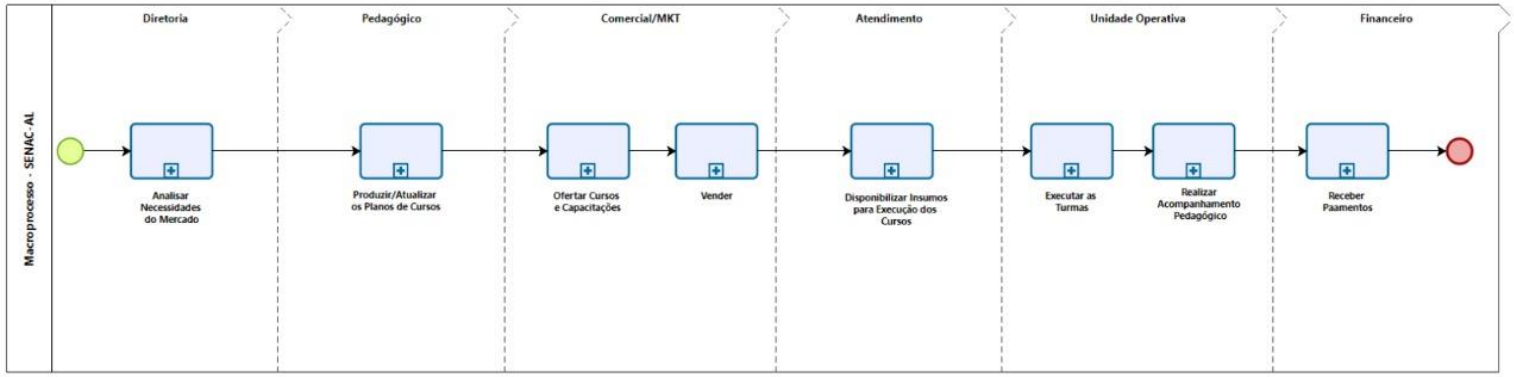

Figura 02 – Macroprocesso de negócio

9 – Requesitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores do Senac Alagoas a fim de que a política seja cumprida dentro e fora da empresa. Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos do Senac Alagoas o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Tecnologia da Informação e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Todos os requisitos de segurança da informação devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico,

nos sistemas comerciais e financeiros desenvolvidos pelo Senac Alagoas ou por terceiros. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

O Senac exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada no Senac Alagoas por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

10 – Gerenciamento da Versão e Manutenção da Política

A política de segurança deve ser revisada constantemente para adequar as normas e procedimentos aos novos requisitos do negócio e avanços tecnológicos.

Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política:**
  - Nível de Aprovação: Diretoria e Gestão de TI;
  - Periodicidade de Revisão: anual;
- **Normas:**

- Nível de Aprovação: Comitê Gestor de Privacidade;
- Periodicidade de Revisão: anual;

- **Procedimentos:**
  - Nível de Aprovação: Supervisor responsável pela área envolvida;
  - Periodicidade de Revisão: Semestral;

11 – Das Responsabilidades e Atribuições Específicas

11.1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Cabe aos colaboradores:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Conhecimento (**Anexo II**) desse documento, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento. As sanções pelo não cumprimento da política de segurança da informação estão descritas no item **38 – Punições;**
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;

- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente ao comitê gestor de segurança da informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao Senac Alagoas e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

11.2 - Atribuições e Responsabilidades da Diretoria:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Aprovar a nomeação dos “proprietários” da informação;
- Aprovar os investimentos necessários para manter a segurança dentro da organização;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação;

11.3 - Dos Gestores de Pessoas e/ou Processos

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do Senac Alagoas.
- Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se

comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do Senac Alagoas.

- Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

11.4 - Dos Custodiantes da Informação

11.4.1 - Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com o Gerente de Tecnologia da Informação o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os analistas e técnicos podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo 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.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Senac Alagoas.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos do Senac Alagoas;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos do Senac Alagoas;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

11.4.2 – Dos Responsáveis de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do Senac Alagoas.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do Senac Alagoas, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o Senac Alagoas.

Buscar alinhamento com as diretrizes corporativas da instituição.

11.4.3 - Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores da GTI - Gerencia de Tecnologia da Informação e de colaboradores de outros setores com nível hierárquico mínimo gerencial**,** nomeados para participar do grupo.

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o Senac Alagoas.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação e propor a relação de “proprietários” das informações;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

11.5 - Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas neste PSI, bem como de sua versão educacional, o Senac Alagoas poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e

outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

11.6 - Atribuições e responsabilidades da assessoria jurídica

- Manter as áreas da empresa informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação e LGPD, com o objetivo de proteger os interesses do Senac Alagoas e avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da empresa;

11.7 - Atribuições e responsabilidades do departamento de recursos humanos

- Obter referências pessoais e profissionais de todos os colaboradores a serem contratados pela empresa;
- Verificar a exatidão e inteireza do curriculum vitae, profissional e acadêmico;
- Obter pelo menos uma referência bancária;

- Providenciar o ajuste do perfil de acesso aos sistemas, quando houver transferência de setor;
- Colher a assinatura do Termo de Conhecimento dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Informar, previamente, à área de TI, todos os desligamentos, afastamentos e modificações no quadro funcional da empresa;
- Providenciar a eliminação do *login*, quando houver saída de pessoal, quer seja por demissão ou por suspensão de contrato;
- Solicitar ao departamento de TI que bloqueie os acessos dos colaboradores durante o período de férias ou licenças.

11.8 - Atribuições e responsabilidades do DPO

- Contribuir na Definição das Políticas e Diretrizes do Programa de Governança em Privacidade;
- Assegurar o cumprimento das políticas de Privacidade e Proteção de Dados através de auditorias mensais;
- Articular a aderência do corpo diretivo com as políticas, estratégias, diretrizes e regulações referentes à proteção de dados pessoais;
- Gerir a Revisão da posição da organização como agente de tratamento de Dados Pessoais;
- Auxiliar na definição e gerir o fluxo de atendimento a requisições de direitos dos Titulares de Dados Pessoais;
- Revisar práticas de Segurança da Informação voltadas a tratamento de Dados Pessoais e Dados Pessoais Sensíveis;

- Propor oportunidades de Anonimização e Pseudoanonimização dos dados pessoais tratados pela empresa;
- Revisar e Propor melhorias no Processo de Gestão de Incidentes voltado a dados pessoais e dados pessoais sensíveis;
- Revisar e propor métodos de armazenamento e compartilhamento de dados seguros;
- Auxiliar na definição e gerir processo de mapeamento de ciclo de vida dos dados, aplicações e terceiros;
- Realizar avaliação do impacto da proteção de dados (RIPD), de acordo com a metodologia definida;
- Acompanhamento e apoio nos projetos de software que envolvem Gestão de Privacidade de Dados Pessoais e Dados Pessoais Sensíveis;
- Aconselhar sobre proteção de dados na arquitetura de TI na organização;
- Aconselhar programadores e administradores de sistemas sobre a proteção prática de sistemas de acordo com as boas práticas;
- Aconselhar sobre tecnologias de aprimoramento da privacidade, incluindo criptografia, anonimização e pseudonimização;
- Atender as solicitações dos titulares dos dados através da plataforma contratada e dentro dos SLAs acordados;
- Coletar informações de violações de segurança;
- Ajudar o cliente a manter, armazenar e documentar as revogações da gestão de consentimento dos titulares dos dados;
- Apoiar o cliente no registro e documentação dos incidentes relacionados a privacidade e proteção de dados;

- Apoiar nas decisões do comitê de privacidade e acompanhar as ações relacionados aos incidentes;
- Apoiar o cliente na investigação de incidentes de segurança e privacidade;
- Entender o impacto do incidente e ajudar o cliente a gerir as crises objetivando evitar sanções;
- Ajudar o cliente a notificar a agência de proteção e dados sobre uma violação de segurança dentro do prazo estabelecido em Lei;
- Ajudar o cliente a notificar os titulares dos dados da violação de segurança;
- Garantir a conformidade com os requisitos da LGPD;
- Realizar controle anual de conformidade de segurança de TI para dados Pessoais e dados pessoais sensíveis;
- Ajudar o cliente a garantir mais foco na segurança de TI para dados pessoais e dados pessoais sensíveis;
- Recomendações técnicas e operacionais para proteger sistemas, redes e dispositivos;
- Apresentar relatórios de acompanhamento de nível de conformidade com a LGPD e segurança da TI para a Administração.

12 - Correio Eletrônico

O objetivo desta norma é informar aos colaboradores do Senac Alagoas quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do Senac Alagoas é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Senac e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do Senac Alagoas:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Senac Alagoas ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do Senac Alagoas estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Senac Alagoas;

- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da empresa
- Telefone(s)

- Correio eletrônico

13 - Internet

Todas as regras atuais do Senac Alagoas visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o Senac Alagoas, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O Senac, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse do Senac Alagoas que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome do Senac Alagoas para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no Senac e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela GTI.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela GTI.

Os colaboradores não poderão em hipótese alguma utilizar os recursos do Senac Alagoas para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao Senac Alagoas ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do Senac para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerencia de Sistemas.

Não é permitido acesso a sites de proxy.

14 - Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Senac Alagoas e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados no Senac Alagoas, como as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O colaborador, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o Senac e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Coordenação de Departamento de Pessoal do Senac Alagoas é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Tecnologia da Informação do Senac Alagoas.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 120 (cento e vinte) dias, não podendo ser repetidas as 5 (cinco) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Coordenação de Departamento de Pessoal deverá imediatamente comunicar tal fato a Gerencia Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

15 - Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade do Senac Alagoas, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações

constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Tecnologia da Informação do Senac Alagoas, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à GTI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk ou através do e-mail de suporte técnico.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio do Senac Alagoas (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores do Senac Alagoas e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Tecnologia da Informação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Tecnologia da Informação do Senac Alagoas, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Tecnologia da Informação do Senac Alagoas ou por terceiros devidamente contratados para o serviço.
- O colaborador deverá manter a configuração do equipamento disponibilizado pelo Senac, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pelo Senac Alagoas devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do Senac Alagoas.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

16 - Dispositivos Móveis

O Senac Alagoas deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Tecnologia da Informação, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

O Senac Alagoas, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no Senac Alagoas, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade do Senac Alagoas e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Tecnologia da Informação.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Tecnologia da Informação do Senac Alagoas.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Senac, notificar imediatamente seu gestor direto e a Gerência de Tecnologia da Informação. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao Senac Alagoas e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Senac deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Tecnologia da Informação.

Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

17 - Datacenter

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do responsável pelo Datacenter, a outra, de posse do Gerente de Tecnologia da Informação.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

18 - Backup

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, distante no mínimo 5 quilômetros do Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do Senac, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore. Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Gerente de Tecnologia da Informação, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

19 – Classificação da informação

A classificação da informação é o processo de estabelecer o grau de importância das informações mediante o seu impacto para o negócio, ou seja, quanto mais estratégica e decisiva para a manutenção ou sucesso da organização, maior será a sua importância. A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento.

Existem regras que devem ser consideradas durante a classificação e a principal delas é a determinação de proprietários para todas as informações, sendo este o responsável por auxiliar na escolha do meio de proteção.

Nos casos onde houver um conjunto de informações armazenadas em um mesmo local, e elas possuírem diferentes níveis, deve-se adotar o critério de classificar todo o local com o mais alto nível de classificação.

As informações armazenadas em qualquer local devem estar de acordo com os critérios de classificação e devem possuir uma identificação que facilite o reconhecimento do seu grau de sigilo. O inventário dos ativos de informação do Senac Alagoas seguirá o seguinte padrão:

Documentos em papel	• Contratos; • Documentos da empresa; • Relatórios
Software	• Aplicativos; • Sistemas operacionais; • Ferramentas de desenvolvimento; • Utilatários de sistema; • Atestados médicos
Hardware	• Servidores, desktops, netbooks, talets; • Storages, unidades de backup, fitas de backup; • Impressoras e copiadoras; • Equipamentos de comuicação (FAX, modem, access points, roteadores, switches etc.); • Mídias magnéticas; • Nobreak, ar condicionados; • Móveis, prédios e salas
Pessoa	• Empregados; • Estagiários; • Jovem aprendiz; • Terceirizados; • Fornecedores
Serviço ou atividade	• Computação (Aplicação de paths, backup etc); • Comunicação (Ligações telefônicas, vídeo conferência etc.); • Atendimento a usuários

20 – Reclassificação da Informação

Toda informação classificada, quando passar por alteração de conteúdo, deve ser submetida a novo processo de classificação, com o objetivo de rever o nível mais adequado.

21 – Níveis de Classificação

A classificação quanto ao sigilo obedecerá aos seguintes critérios:

- **Públicas** – São aquelas que não necessitam de sigilo algum. Podendo ter livre acesso para os colaboradores. Não há necessidade de investimentos em recursos de proteção. São informações que se forem divulgadas fora da organização, não trarão impactos para os negócios.

- **Internas** – O acesso externo a essas informações deve ser evitado. Entretanto, se esses dados se tornarem públicos, as consequências não serão críticas. Exemplo: agendas de telefones e ramais, benefícios da organização para os colaboradores, procedimentos operacionais simples;

- **Confidenciais** – As informações dessa classe devem ser confidenciais dentro da organização e protegidas do acesso externo. Se alguns desses dados forem acessados por pessoas não autorizadas, as operações da organização poderão ser comprometidas, causando perdas financeiras e de competitividade. Exemplos: Salários, dados pessoais, dados dos clientes, estratégias de mercado e senhas.

22 – Formas de Classificação

A classificação das informações deve ser implementada de acordo com a tabela a seguir:

Tipo do documento	Procedimento
Documento em papel	Caso seja confidencial e gerado dentro da organização, deve apresentar o nível de segurança na primeira página do documento. Caso venha de fora, deve ser marcado com uma etiqueta ou carimbo.
E-mail	Caso seja confidencial, deve ter o assunto iniciado com "[Confidencial]".
Documento eletrônico	Deve conter o nível de segurança no rodapé na primeira página do documento.
Outros tipos de mídia	A classificação de segurança deve ser visível por etiquetas ou outros recursos que se façam necessários

23 - Proprietário da informação

O proprietário da informação é um diretor ou um gestor do Senac Alagoas, formalmente indicado pelos sócios, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações sob a sua guarda. Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções com as autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;

- Analisar os relatórios de controle de acesso fornecidos pela área de Gestão de Segurança da Informação, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão de Privacidade, prestando os esclarecimentos solicitados.

A tabela a seguir descreve os proprietários das informações de cada departamento do Senac Alagoas:

Departamento	Proprietário da Informação
Coordenação EAD	Juliana Alves
Diretora Regional	Telma Ribeiro
Financeiro	Jádsia Buarque
Apoio e Infraestrutura	Rafael Duda
Ouvidoria	Aline Baracho
Planejamento/Controladoria	Vagner Cavalcanti
TI	Samuel Vasconcelos
Contabilidade	Jonhnatan Rodrigues
Comunicação e Marketing	Cristiane Calaça
Controladoria	Mony Cely
Call Center/Centrais de Atendimento	Cristiane Calaça
Banco de Oportunidades	Daniela Araújo

Recursos Humanos	Adriana Palmeira
Educação Profissional	Aristóteles Oliveira
Biblioteca	Aristóteles Oliveira
Secretaria Escolar	Aristóteles Oliveira
Comercial	Daniela Araújo
Suprimentos, Licitação e Contratos	Felipe Dietschi

24 - Usuários da informação

É todo funcionário interno, trabalhador temporário, estagiário ou terceirizado, que tenham acesso aos bens de informação do Senac Alagoas.

O usuário da informação terá responsabilidade de:

- Zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação de acesso;
- Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
- Notificar não conformidades de segurança.

25 - Controle da Divulgação

- **Informações Confidenciais** – Só devem ser divulgadas para quem precisa da informação em função da necessidade de serviço. Para acessá-la, é preciso que se faça parte de uma lista formal de autorização elaborada pelo proprietário da informação ou seu representante autorizado;

- **Informações de uso interno** – Podem ser divulgadas para qualquer funcionário do Senac Alagoas;
- **Informações Públicas** – Podem ser divulgadas livremente sem nenhum controle de acesso;

26 - Armazenamento

- **Informações Confidenciais** – Devem ser armazenadas em locais que garantam apenas o acesso das pessoas permitidas. Ferramentas como servidores de arquivos, sistemas de gerenciamento de documentos e locais com acesso restrito devem ser utilizadas para garantia da confidencialidade. As listas de controle de acesso devem ser periodicamente auditadas para identificar inconformidades de acesso;

- **Informações de Uso Interno** – Devem ser disponibilizadas em meios onde os colaboradores possam ter apenas o mínimo acesso necessário. As ferramentas de armazenamento utilizadas devem garantir que as informações não serão indevidamente alteradas, copiadas ou excluídas.

27 - Transporte Interno e Expedição

- **Informações Confidenciais** – Em recipiente simples com identificação do grau de sensibilidade, evitando-se a entrega em malotes internos. Deve-se dar preferência à entrega pessoal por pessoa devidamente autorizada, com registro de protocolo;

- **Informações de uso interno** – Pode ser transportada aberta;

28 - Transporte Externo

- **Informações Confidenciais** – Em recipiente de segurança com identificação do grau de sensibilidade. O transporte e a entrega devem sempre ser realizados por pessoa devidamente autorizada, com registro de protocolo;

- **Informações de uso interno** – Em recipiente simples;

29 - Transmissão de Voz

- **Informações Confidenciais** – Permitida a transmissão através de linhas telefônicas, apenas dentro de ambientes controlados.
- **Informações de uso interno** – Sem restrições.

30 - Transmissão de Dados

- **Informações Confidenciais** – Se o meio de transmissão estiver totalmente em área sob o controle da organização, pode ser transmitido em texto claro (sem encriptação), caso contrário deve ser criptografado.
- **Informações de uso interno** – Permitida a transmissão em texto livre para qualquer caso.

31 - Descarte de Informações

Toda mídia impressa que contenha informações relevantes deve ser destruída antes de ser descartada. Essa destruição deve ser feita com o picotador de papel existente na empresa. CDs, DVDs, pen drives, discos externos e qualquer outro tipo de mídia física devem ser totalmente destruídos antes de serem descartados.

32 – Controle de mudanças no ambiente

Toda e qualquer mudança crítica que precise ser realizada no ambiente de TI do Senac Alagoas deve ser feita fora do horário de expediente e, sempre que possível, prioritariamente validada no ambiente de homologação.

33 – Manutenção de equipamentos de informática

Quando qualquer equipamento de informática como computadores pessoais, celulares, *notebooks*, *tablets*, servidores, *storages,* etc., necessitarem de assistência técnica fora da empresa, a equipe de TI deve apagar ou remover todos os dispositivos de armazenamento como discos, cartões de memória, pen drives etc. Essa ação evitará que os dados sejam acessados por pessoas não autorizadas.

34 - Computação Móvel e Trabalho Remoto

Os trabalhos remotos, sempre que necessários, só estão liberados através de acesso VPN para alguns membros da equipe de TI, de acordo com a necessidade. Para os funcionários, só será permitido esse acesso em situações especiais e com aprovação prévia do diretor de cada área, observando o período e os horários em que os acessos serão permitidos.

Para os fornecedores, o acesso só será permitido depois da criação de um perfil de acesso que libere apenas os servidores envolvidos nas atividades. As contas dos mesmos devem ser desabilitadas imediatamente após a conclusão dos trabalhos e por padrão só poderão ocorrer em horário comercial. Casos especiais serão tratados pontualmente.

35 - Níveis de Operação

- **Rotina** – Caracteriza a situação onde não existe suspeita de falhas na segurança do sistema, que deve estar monitorado continuamente;

- **Emergência** – Existe a suspeita de algum ataque à segurança, com possíveis danos ao funcionamento seguro do sistema;

- **Crise** – Situação na qual um problema à segurança está confirmado e ações devem ser tomadas para tratar o ataque e suas consequências.

Todo e qualquer incidente de segurança deve ser imediatamente informado ao Comitê, ao DPO e a equipe de TI para que as medidas cabíveis sejam tomadas no menor espaço de tempo possível;

36 – Segurança Física

- A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. As seguintes regras devem ser obedecidas por todos:
- Todos os visitantes, colaboradores e prestadores de serviço devem usar o crachá de identificação em local visível;
- Os visitantes não podem ficar circulando nas dependências da empresa. Devem ser conduzidos da portaria diretamente para o setor que deseja visitar;
- Todo e qualquer equipamento ou material só poderá ser retirado das instalações do Senac Alagoas com a devida autorização dos gestores ou da diretoria;
- Todas as áreas de circulação, incluindo as salas de aula, devem ser monitoradas através de circuitos internos de TV;
- A sala dos servidores e equipamentos de TI, Datacenter, tem acesso reservado aos funcionários desse setor. É terminantemente proibido o uso de qualquer tipo de alimentos ou líquidos devido aos riscos de dano aos ativos existentes;

- As portarias de acesso à empresa são monitoradas continuamente por profissionais de empresa especializada em segurança;
- Todos os colaboradores devem manter a política da mesa limpa, evitando que informações confidenciais fiquem expostas e possam ser observadas por pessoas não autorizadas;
- Uma cópia das mídias de backups semanais, mensais e anuais devem ser removidas continuamente das instalações do Senac Alagoas para garantir a continuidade dos negócios em caso de incidentes com a estrutura física;
- Ao encaminhar qualquer equipamento para assistência técnica, as informações existentes nas mídias de armazenamento devem ser definitivamente excluídas para evitar acesso indevido;

37 – Gestão de incidentes de segurança

Um incidente de segurança da informação é qualquer ação ou omissão que pode ter impacto na segurança das informações, no negócio ou nos ativos da instituição. A tabela a seguir descreve quem deve ser acionado a depender da natureza do incidente:

Tipo de incidente	Empresa	Telefone
Problemas envolvendo privacidade de dados pessoais	ADX	3013-4140
Problemas com energia elétrica	EQUATORIAL ENERGIA	0800 082 0196

Problemas com incêndios	BOMBEIROS	193
Problemas de roubo ou assalto	Polícia Militar Polícia Civil	190 3521-6554
Problemas de infraestrutura civil	Defesa Civil	3315-2822
Problemas de saúde com alunos, colaboradores ou visitantes	SAMU	192

38 – Punições

Quando qualquer item da política de segurança da informação for violado, por um colaborador que tenha assinado o Termo de Conhecimento, o Comitê vai levar ao conhecimento da diretoria para definir a punição aplicada. As punições possíveis são:

- Advertência verbal;
- Advertência por escrito;
- Desconto de período de trabalho;
- Desligamento do colaborador sem justa causa;
- Desligamento do colaborador por justa causa;

39 – Das Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do Senac Alagoas. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

40 – Referências bibliográficas

[1] ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 270005 e ISO/IEC 22301;

[2] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**, versão 3.1. São Paulo: Comitê Gestor da Internet no Brasil, 2006. Disponível em: <http://cartilha.cert.br/livro/>.

[3] Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu. Política da Segurança da Informação: Guia Prático para Elaboração e Implementação. Editora Ciência Moderna, 2006.

[4] Sêmola Marcos. Gestão da segurança da informação, uma visão executiva. Editora CAMPUS 2003.

[5] Fontes Edilson. Políticas e Normas para a Segurança da Informação. Editora Brasport, 2012.

[6] FONTES, Edson. Praticando a Segurança da Informação. Brasport, 2008.

[7] Ferreira Fernando e Araújo Márcio. Política de Segurança da Informação. Ciência Moderna, 2008.

ANEXOS

ANEXO I – Conceitos e definições

- **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;
- **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Capacitação em SIC**: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;
- **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;
- **Comitê Gestor de Privacidade**: Comitê de caráter deliberativo, responsável pela normatização e supervisão da segurança da informação;
- **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- **Conscientização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;
- **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **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;
- **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;
- **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para

que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

- **Gerenciamento de operações e comunicações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;
- **Gestão de riscos de segurança da informação e comunicações - GRSIC**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;
- **Gestão de segurança da informação e comunicações - GSIC**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- **Incidente de Segurança**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **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;
- **Infraestrutura de TI**: 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 que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;
- **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- **Recursos criptográficos**: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
- **Risco**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

- **Sensibilização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;
- **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Senac Alagoas;
- **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- **Tratamento da informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação; e
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

ANEXO II - Termo de Conhecimento para os Colaboradores

NOME:	
MATRÍCULA:	
CPF:	

AFIRMO QUE ESTOU CIENTE E COMPROMETO-ME a cumprir a Política de Segurança da Informação do Sena Alagoas na sua íntegra, respondendo em todas as instâncias pelas consequências das ações ou omissões da minha parte, que possam pôr em risco ou comprometer qualquer diretiva descrita nesse documento.

Alagoas, _____ de _____ de 20___.

_____

Assinatura do Colaborador/Estagiário/Fornecedor

Comentado [LF1]: Eliminar ou ocultar página com as assinaturas quando apresentada ao colaborador (é um dado pessoal sensível)