POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Dezembro/2024

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor	Aprovação
19/12/2024	V1.0	Primeira versão da Política de Segurança da Informação	Equipe Técnica de Elaboração	Deborah Montenegro e Franklin Bonfim
20/03/2024	V1.1	Segunda versão da Política de Segurança da Informação	Equipe de T.I.	Tiago Silva e Alexandre de Abreu e Silva

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Política de Segurança da Informação do Sesc Goiás tem como objetivo estabelecer diretrizes, normas e procedimentos que garantam a proteção das informações institucionais, assegurando a confidencialidade, integridade e disponibilidade dos dados. Este documento orienta colaboradores, fornecedores e demais partes interessadas no uso adequado e seguro dos recursos de informação da instituição.

Para ampliar a cultura de segurança da informação e privacidade, o Sesc Goiás, alinhado às boas práticas e normas internacionalmente aceitas, atualizou sua Política de Segurança da Informação (PSI), a fim de adequá-la à legislação nacional vigente e garantir a proteção de todos os seus ativos tangíveis e intangíveis.

Em um ambiente cada vez mais digital e interconectado, o Sesc Goiás reconhece a importância da segurança da informação como um pilar essencial para a continuidade dos negócios, a preservação da reputação institucional e o cumprimento das legislações vigentes. Esta política busca mitigar riscos, prevenir incidentes e promover uma cultura organizacional voltada à proteção das informações.

2. CONCEITOS FUNDAMENTAIS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Para garantir o entendimento e a aplicação correta das diretrizes estabelecidas nesta política, são definidos os seguintes conceitos fundamentais:

- **Segurança da Informação:** Conjunto de práticas e medidas que visam proteger os dados e informações contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição.
- **Privacidade:** Direito do indivíduo de controlar o uso e a divulgação de suas informações pessoais, assegurando a proteção contra violações e usos inadequados.
- **Confidencialidade:** Garantia de que as informações sejam acessadas somente por pessoas autorizadas.
- **Integridade:** Propriedade que assegura que as informações sejam mantidas íntegras, sem alterações indevidas.
- **Disponibilidade:** Propriedade que garante que as informações estejam acessíveis sempre que necessário.

- **Autenticidade:** Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.
- **Ativos de Informação:** Recursos valiosos para a organização, que incluem dados, equipamentos, sistemas e processos relacionados à informação.
- **Ameaça:** Conjunto de fatores externos, internos ou eventos que podem resultar em um incidente indesejado e causar danos a um sistema ou à Instituição.
- **Evento:** Um evento de segurança refere-se a qualquer ocorrência que tenha o potencial de comprometer a confidencialidade, integridade, disponibilidade ou autenticidade dos sistemas de informação. Esses eventos podem incluir atividades anômalas, alertas de segurança ou outras situações que indiquem uma possível ameaça à segurança da informação.
- **Incidente de Segurança da Informação:** Evento que compromete a confidencialidade, integridade ou disponibilidade das informações, podendo causar prejuízos à organização.
- **Usuários:** empregados, terceirizados, consultores, auditores, conselheiros, estagiários, jovens aprendizes e visitantes que obtiveram autorização do responsável pela área interessada de acesso aos ativos de TI da Instituição.

Esses conceitos servem como base para orientar a compreensão e a execução das práticas de segurança da informação e privacidade dentro do Sesc Goiás.

3. ABRANGÊNCIA E APLICAÇÃO

Esta Política de Segurança da Informação aplica-se a todos os colaboradores, estagiários, prestadores de serviço, fornecedores, parceiros e qualquer pessoa que tenha acesso às informações e recursos tecnológicos do Sesc Goiás. A abrangência inclui, mas não se limita a:

i. Informações armazenadas, processadas e transmitidas em qualquer formato ou meio (físico ou digital).
ii. Equipamentos, sistemas e redes utilizados para processar ou armazenar informações institucionais.
iii. Instalações físicas onde as informações do Sesc Goiás são mantidas ou acessadas.
iv. Atividades realizadas dentro ou fora das dependências do Sesc Goiás que envolvam o uso de seus ativos de informação.

Todos os envolvidos devem aderir às diretrizes estabelecidas nesta política, garantindo o cumprimento das normas e boas práticas para preservar a segurança da informação e evitar incidentes que possam comprometer os ativos institucionais.

4. COMPROMISSOS COM A SEGURANÇA DA INFORMAÇÃO

O Sesc Goiás assume os seguintes compromissos para fortalecer sua gestão de segurança da informação:

i. **Satisfação dos Requisitos Aplicáveis:** Garantir o atendimento a todos os requisitos legais, regulamentares e contratuais aplicáveis relacionados à segurança da informação, assegurando a conformidade com normas e legislações vigentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

ii. **Medidas de Proteção:** Implementar medidas técnicas, administrativas e organizacionais adequadas para o tratamento e proteção de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado e outros incidentes de segurança.

iii. **Conscientização e Treinamento:** Conscientizar os colaboradores sobre a importância da segurança da informação e privacidade, além de oferecer treinamentos regulares e atualizados para fortalecer a cultura de proteção de dados.

iv. **Melhoria Contínua:** Implementar ações para o aperfeiçoamento contínuo do Sistema de Gestão da Segurança da Informação (SGSI), adotando melhores práticas e aprendendo com experiências internas e externas para fortalecer os processos e reduzir vulnerabilidades.

v. **Continuidade dos Negócios:** Garantir a continuidade das operações críticas, protegendo os processos contra falhas significativas e desastres que possam impactar a organização.

vi. **Definição de Responsabilidades:** Assegurar que todas as responsabilidades pela segurança da informação e privacidade estejam claramente definidas, e que as pessoas indicadas possuam a competência necessária para cumprir suas atribuições.

Esses compromissos reforçam a postura do Sesc Goiás em tratar a segurança da informação como prioridade estratégica, promovendo um ambiente seguro e alinhado às expectativas das partes interessadas.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

As atividades relacionadas à segurança da informação no Sesc Goiás são orientadas pelos seguintes princípios fundamentais:

- **Confidencialidade:** Garantir que a informação seja acessada apenas por pessoas autorizadas, protegendo-a contra acessos não autorizados ou divulgação inadequada.
- **Integridade:** Assegurar a exatidão e a completude das informações, prevenindo alterações indevidas ou danos que comprometam sua confiabilidade.
- **Disponibilidade:** Garantir que as informações e os recursos estejam acessíveis e utilizáveis sempre que necessário, minimizando interrupções e assegurando a continuidade das operações.
- **Autenticidade:** assegurar que os ativos de informação sejam produzidos, publicados, transmitidos, alterados ou apagados por uma pessoa, equipamento ou sistema autorizado, identificando e registrando a autoria.
- **Conformidade:** Cumprir todas as leis, regulamentações e normas aplicáveis relacionadas à segurança da informação, incluindo legislações nacionais e boas práticas reconhecidas internacionalmente.
- **Responsabilidade:** Promover a conscientização e o compromisso de todos os colaboradores e parceiros quanto ao papel de cada um na proteção das informações institucionais.
- **Proatividade:** Identificar, avaliar e tratar os riscos relacionados à segurança da informação de forma preventiva, reduzindo a probabilidade de incidentes.

Esses princípios norteiam a implementação e a gestão de medidas de segurança, assegurando que a informação seja tratada como um ativo estratégico e protegida em todas as suas dimensões.

6. DIRETRIZES

6.1. UDO DE E-MAIL

O correio eletrônico é um dos recursos de comunicação institucional do Sesc Goiás e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta Política. Portanto, fica proibido o uso de compartilhamento de informações do Sesc Goiás com e-mail pessoal, e é vedado o acesso a e-mails particulares de dentro da rede do Sesc Goiás.

O uso de e-mails institucionais no Sesc Goiás está sujeito às seguintes diretrizes para garantir a segurança das informações e a privacidade:

i. **Uso exclusivamente profissional:** O e-mail institucional deve ser utilizado exclusivamente para atividades relacionadas às funções e responsabilidades profissionais dos colaboradores.

ii. **Confidencialidade das informações:** Os usuários devem ficar atentos com quem estão compartilhando informações confidenciais e sigilosas a fim de não compartilhais tais informações com quem não deveria ter acesso a elas.

iii. **Atenção ao conteúdo:** Os usuários devem garantir que os e-mails enviados estejam de acordo com as diretrizes da organização, evitando informações incorretas, inadequadas ou que possam comprometer a imagem do Sesc Goiás.

iv. **Prevenção contra ameaças:** Não abrir anexos ou clicar em links de e-mails suspeitos, a fim de evitar ataques como *phishing*, *malware* ou outros tipos de ameaças cibernéticas.

v. **Armazenamento seguro:** Os usuários devem arquivar e-mails de maneira organizada e segura, evitando o acúmulo desnecessário de informações e garantindo o descarte adequado quando permitido.

vi. **Monitoramento:** O Sesc Goiás reserva-se o direito de monitorar o uso de e-mails institucionais para garantir o cumprimento desta política, respeitando as legislações aplicáveis.

Essas diretrizes visam assegurar o uso responsável e seguro dos e-mails institucionais, prevenindo riscos à organização e protegendo os dados sensíveis.

6.2. USO DA INTERNET

A internet é uma ferramenta essencial para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências no Sesc Goiás. Contudo, seu uso está sujeito às seguintes diretrizes para garantir a segurança e a conformidade com os valores e objetivos institucionais:

- **Finalidade profissional:** A internet deve ser utilizada para fins profissionais, relacionados às atividades e responsabilidades dos colaboradores, vedado o uso para fins pessoais.
- **Regras de acesso e bloqueio:** O Sesc Goiás mantém regras específicas de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários e assinaturas, bem como limites de tráfego e armazenamento. Estas medidas visam proteger os ativos e as informações institucionais.
- **Proibição de conteúdos inadequados:** É estritamente proibido utilizar a internet institucional para acessar, compartilhar ou divulgar conteúdos ilegais, pornográficos, discriminatórios, de cunho religioso, político-partidário ou ideológico, ou que estejam em desacordo com os princípios éticos e morais da instituição.

- **Prevenção de ameaças cibernéticas:** Os colaboradores devem evitar o acesso a sites não confiáveis ou suspeitos e não realizar downloads de arquivos que possam comprometer a segurança dos sistemas institucionais.
- **Monitoramento de uso:** O Sesc Goiás monitora o uso da internet para garantir o cumprimento das diretrizes desta política e proteger os interesses da instituição, sempre em conformidade com a legislação vigente.

Essas diretrizes têm o objetivo de assegurar que o uso da internet seja feito de forma ética, segura e alinhada aos valores do Sesc Goiás, minimizando riscos e promovendo um ambiente de trabalho produtivo e protegido.

6.3. USO DE REDES SOCIAIS

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimentos e serviços, divulgando ou compartilhando informações do Sesc Goiás, deve ser previamente autorizada pelas áreas de gestão, em conformidade com as diretrizes do Código de Conduta, desta Política e com os objetivos estratégicos da organização.

- **Perfis Institucionais:** Apenas perfis oficiais, devidamente autorizados, podem ser utilizados para representar o Sesc Goiás nas redes sociais.
- **Conformidade com as Diretrizes:** Todo conteúdo publicado deve estar alinhado aos valores, princípios e objetivos do Sesc Goiás, respeitando as diretrizes éticas e de segurança estabelecidas.
- **Proibição de Conteúdos Inadequados:** É proibida a publicação de conteúdos inadequados, como materiais ilegais, discriminatórios, de cunho religioso, político-partidário, pornográfico ou que possam prejudicar a imagem da instituição.
- **Uso Pessoal de Redes Sociais:** O uso pessoal de redes sociais durante o horário de trabalho deve ser limitado e não comprometer a produtividade ou os recursos institucionais.
- **Monitoramento:** O Sesc Goiás reserva-se o direito de monitorar os perfis institucionais para garantir o cumprimento das diretrizes e preservar sua reputação.

Essas diretrizes têm como objetivo garantir que o uso das redes sociais seja feito de maneira responsável, protegendo a imagem e os interesses do Sesc Goiás.

6.4. USO DE COMPUTAÇÃO EM NUVEM

O uso de recursos de computação em nuvem tem o objetivo de suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação.

O Sesc Goiás disponibiliza para os colaboradores um espaço no SharePoint para armazenamento de arquivos relacionados às atividades realizadas dentro da instituição, sendo vedado o acesso a drives em nuvens particulares.

- **Armazenamento Exclusivo:** Todos os documentos e informações institucionais devem ser armazenados exclusivamente no SharePoint ou outras plataformas autorizadas pelo Sesc Goiás.
- **Acesso Restrito:** É proibido o uso de serviços de nuvem pessoal para armazenamento ou compartilhamento de informações institucionais.
- **Confidencialidade e segurança:** Assegurar que os dados armazenados na nuvem institucional estejam protegidos por medidas de segurança adequadas, incluindo controle de acesso e criptografia.
- **Monitoramento:** O Sesc Goiás realiza monitoramento contínuo do uso dos serviços de computação em nuvem para garantir o cumprimento das diretrizes e prevenir riscos à segurança das informações.

Essas diretrizes asseguram o uso responsável e seguro dos recursos de computação em nuvem, promovendo a proteção das informações e a conformidade com os padrões institucionais.

6.5. USO DE DISPOSITIVOS MÓVEIS

As diretrizes gerais para uso de dispositivos móveis, como smartphones e tablets, no acesso às informações, sistemas, aplicações e e-mail do Sesc Goiás devem considerar, prioritariamente, os requisitos legais e a estrutura da organização, atendendo a esta Política de Segurança da Informação e as diretrizes específicas da Política de Privacidade.

- **Finalidade Profissional:** Os dispositivos móveis utilizados para acessar sistemas ou dados institucionais devem ser utilizados exclusivamente para fins profissionais.
- **Proteção de Dados:** Os dispositivos devem estar protegidos por senhas fortes ou outros mecanismos de autenticação seguros, e sua configuração deve incluir medidas de proteção contra acessos não autorizados.
- **Armazenamento Restrito:** É proibido o armazenamento de informações institucionais em dispositivos móveis não autorizados ou pessoais.

- **Uso da rede:** Os dispositivos móveis que não sejam adquiridos pela organização, não devem utilizar a rede Wi-Fi administrativa para acesso à internet ou a sistemas internos da organização. Para acesso à internet e outras necessidades operacionais, os dispositivos móveis devem utilizar redes segregadas, como exemplo a rede Wi-Fi de visitantes.
- **Gestão e Monitoramento:** O Sesc Goiás se reserva o direito de implementar soluções de gestão de dispositivos móveis (MDM) para monitorar, proteger e gerenciar o uso de dispositivos de sua propriedade e disponibilizados aos colaboradores.
- **Prevenção de Perdas:** Em caso de perda ou roubo de um dispositivo móvel autorizado, o colaborador deve comunicar imediatamente ao setor responsável para que medidas de proteção sejam tomadas.

Essas diretrizes garantem que o uso de dispositivos móveis para acessar recursos do Sesc Goiás seja realizado de forma segura e em conformidade com as políticas institucionais.

6.6. DIRETÓRIO DE ARMAZENAMENTO

As informações relacionadas aos negócios do Sesc Goiás devem ser armazenadas exclusivamente em diretórios de armazenamento designados pela área de tecnologia da informação. O armazenamento em estações de trabalho e dispositivos móveis, como laptops, pen drives, HDs externos, celulares e tablets, é proibido, a fim de assegurar a proteção e a realização de cópias de segurança regulares.

- **Responsabilidade dos colaboradores:** Cada colaborador é responsável por garantir que as informações relacionadas às suas atividades sejam transferidas para os diretórios de armazenamento indicados pela área de tecnologia da informação.
- **Segurança das informações:** O uso de diretórios apropriados possibilita a aplicação de medidas de segurança adicionais, como backups regulares e controles de acesso, protegendo as informações institucionais de forma eficaz.

Essas diretrizes têm como objetivo garantir a proteção, disponibilidade e integridade das informações institucionais, reduzindo os riscos associados ao armazenamento em dispositivos não monitorados ou vulneráveis.

6.7. USO DE ANTIVÍRUS

Todas as estações de trabalho e servidores do Sesc Goiás devem possuir *software* antivírus instalado e configurado para atualizações automáticas. As diretrizes para o uso de antivírus incluem:

- **Responsabilidade da área de TI:** A área de tecnologia da informação (TI) é responsável por gerenciar o controle de *malware*, garantindo a instalação, atualização e funcionamento adequado do *software* antivírus em todos os dispositivos corporativos.
- **Responsabilidade dos colaboradores:** É dever dos colaboradores comunicar à área de TI qualquer comportamento suspeito associado a *malwares, ransomware* ou outras ameaças detectadas em suas estações de trabalho.
- **Proibição de mídias removíveis:** O uso de dispositivos de mídia removível (como pen drives, discos externos e smartphones) é estritamente proibido em computadores e dispositivos corporativos.

Essas medidas visam proteger os sistemas e dados institucionais contra ameaças cibernéticas, garantindo um ambiente digital seguro e em conformidade com as diretrizes de segurança do Sesc Goiás.

6.8. USO DE INTELIGÊNCIA ARTIFICIAL (IA)

A utilização de ferramentas de Inteligência Artificial (IA) no Sesc Goiás deve ser realizada com responsabilidade e cautela, visando otimizar processos e auxiliar na tomada de decisões. As diretrizes abaixo devem ser observadas:

- **Aprovação prévia:** É permitido o uso de ferramentas de IA desde que aprovadas previamente pela Diretoria Jurídica e de *Compliance* e pela Diretoria Transformação Digital e Inovação. O uso de ferramentas não autorizadas é estritamente proibido.
- **Validação e restrições:** No caso de ferramentas de IA gratuitas e validadas e aprovadas pelas Diretoria Jurídica e de *Compliance* e Diretoria Transformação Digital e Inovação, é proibido inserir dados sigilosos ou sensíveis dos clientes ou da instituição.
- **Treinamento e conscientização:** Os colaboradores devem ser treinados para utilizar as ferramentas de IA de forma ética e responsável, evitando comprometer a segurança das informações.
- **Monitoramento de uso:** A área de TI é responsável por monitorar o uso de ferramentas de IA garantindo que sejam utilizadas de acordo com as diretrizes desta política e mitigando riscos associados à sua utilização.

Essas diretrizes asseguram que o uso de Inteligência Artificial no Sesc Goiás esteja alinhado às políticas institucionais, protegendo os dados e promovendo o uso ético e eficiente dessas tecnologias.

6.9. GRAVAÇÃO DE REUNIÕES

A gravação de reuniões é permitida no Sesc Goiás, desde que sejam observados os seguintes requisitos:

- **Consentimento:** Todas as pessoas presentes na reunião devem ser informadas sobre a gravação no início da reunião.
- **Ferramenta padrão:** As reuniões realizadas pelo Sesc Goiás devem ser gravadas utilizando a plataforma Microsoft Teams, garantindo a segurança e o controle do acesso às gravações.
- **Finalidade profissional:** As gravações de reuniões devem ser utilizadas apenas para fins profissionais e armazenadas de forma segura, respeitando a confidencialidade das informações discutidas.

6.10. MONITORAMENTO DE ACESSOS

O Sesc Goiás reserva-se o direito de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Esse monitoramento inclui o uso particular (pessoal) realizado por meio dos recursos institucionais, desde que haja indícios de atos ilícitos ou condutas inadequadas.

- **Finalidades do monitoramento:** Os registros podem ser utilizados para:
  - Identificar e prevenir incidentes de segurança;
  - Realizar análises estatísticas para melhorar a prestação de serviços;
  - Fornecer evidências em casos relacionados a investigações internas ou externas.
- **Transparência e conformidade:** Todos os colaboradores são informados sobre a possibilidade de monitoramento, garantindo conformidade com as legislações aplicáveis, como a LGPD.
- **Armazenamento seguro dos registros:** Os registros coletados serão armazenados de forma segura, com acesso restrito às pessoas devidamente autorizadas, respeitando a confidencialidade das informações.

Essa política visa proteger os recursos institucionais e garantir um ambiente seguro e alinhado aos valores do Sesc Goiás.

6.11. USO DE COMPUTADORES CORPORATIVOS

No Sesc Goiás é obrigatório que todos os colaboradores utilizem exclusivamente os computadores e dispositivos fornecidos pela instituição para a realização de atividades profissionais.

- **Finalidade Profissional:** Os computadores corporativos utilizados para acessar sistemas ou dados institucionais devem ser utilizados exclusivamente para fins profissionais.
- **Alterações em computadores:** Qualquer modificação no sistema operacional, hardware ou outros componentes do computador deve ser previamente aprovada pela equipe de Tecnologia da Informação (TI). A instalação de aplicativos deve respeitar o uso de ferramentas e softwares homologados pela organização, e a remoção de aplicativos pré-configurados só é permitida com autorização da TI.
- **Suporte técnico:** A equipe de Tecnologia da Informação (TI) será responsável por fornecer o suporte técnico necessário e garantir que os equipamentos corporativos estejam em conformidade com as políticas de segurança, incluindo a aplicação de atualizações, configurações e monitoramento contínuos.

Essa prática visa mitigar riscos associados à segurança da informação, assegurando que os dispositivos utilizados para acessar, processar e armazenar dados institucionais estejam configurados, atualizados e monitorados de acordo com os padrões de segurança estabelecidos pela organização.

6.12. USO DE FERRAMENTAS E SOFTWARES HOMOLOGADOS PELA ORGANIZAÇÃO

O Sesc Goiás permite apenas o uso de ferramentas e *softwares* homologados pela instituição. A equipe de Tecnologia da Informação (TI) será responsável por avaliar, homologar e disponibilizar as ferramentas e *softwares* necessários para as atividades institucionais, garantindo que estejam devidamente atualizados e alinhados às políticas de segurança.

O uso de softwares ou ferramentas não autorizados, adquiridos externamente ou de fontes não verificadas, é estritamente proibido, visando mitigar riscos de segurança, como vulnerabilidades, malwares e violações de conformidade.

6.13. REGRAS PARA USO DE EQUIPAMENTOS CORPORATIVOS

Para reforçar a segurança da informação e a eficiência operacional, os equipamentos corporativos do Sesc Goiás estão sujeitos às seguintes diretrizes de uso:

- **Desligamento Automático:** Todos os equipamentos corporativos, como computadores e servidores, serão configurados para desligar automaticamente às 23h. Essa medida visa economizar recursos, reduzir riscos de acesso não autorizado e manter a integridade do ambiente tecnológico.

- **Casos Excepcionais:** Recepção de hotéis, restaurantes, eventos e situações específicas em que os funcionários precisem trabalhar após esse horário. Essa liberação será feita mediante justificativa formal e análise da necessidade.

7. CONTROLES DE SEGURANÇA DA INFORMAÇÃO UTILIZADOS PELO SESC GOIÁS

Para assegurar a proteção das informações e a conformidade com as melhores práticas de segurança, o Sesc Goiás adota uma série de controles, que são detalhados em políticas específicas, incluindo:

- **Controle de Acesso:** Regras e procedimentos para garantir que apenas pessoas autorizadas tenham acesso a informações, sistemas e recursos, bem como restringir e gerenciar a atribuição e o uso de direitos de acessos privilegiados.
- **Autenticação segura:** Implementação de tecnologias e procedimentos de autenticação seguros, com base em restrições de acesso à informação a fim de assegurar que o usuário seja autenticado com segurança, quando o acesso a sistemas, aplicações e serviços é concedido.
- ***Logs*:** Registro de atividades, exceções, falhas e outros eventos relevantes em sistemas e redes. Essas informações são protegidas e analisadas regularmente para identificar incidentes de segurança e apoiar investigações quando necessário.
- **Segurança física e do ambiente:** Medidas de proteção para garantir a integridade dos ativos físicos e instalações, prevenindo acessos não autorizados e danos.
- **Gestão de ativos:** Diretrizes para o inventário, classificação, proteção e descarte seguro de ativos de informação.
- **Transferência de informações:** Procedimentos para assegurar que informações sejam transmitidas de forma segura entre usuários, sistemas e organizações.
- **Configuração e manuseio seguros de dispositivos *endpoint*:** Padrões para a configuração e uso de dispositivos como computadores, celulares e tablets, reduzindo vulnerabilidades.
- **Segurança de redes:** Controles para proteger a infraestrutura de redes, incluindo *firewalls*, segmentação e monitoramento de tráfego.
- **Gestão de incidentes de segurança da informação:** Procedimentos para identificar, reportar, tratar e aprender com incidentes de segurança.
- ***Backup* das informações:** Políticas e procedimentos para a realização de cópias de segurança, assegurando a recuperação de informações críticas em caso de falhas ou incidentes.

- **Criptografia:** Uso de técnicas de criptografia para proteger dados em trânsito e em repouso, incluindo a gestão segura de chaves criptográficas.
- **Classificação e tratamento de informações**: Diretrizes para classificar informações de acordo com sua sensibilidade e implementar controles apropriados.
- **Gestão de vulnerabilidades técnicas:** Processos para identificar, avaliar e corrigir vulnerabilidades em sistemas e aplicações.
- **Desenvolvimento Seguro:** Práticas para garantir que sistemas e aplicações sejam projetados e desenvolvidos com segurança desde o início.

Esses controles formam a base para a proteção das informações institucionais e serão detalhados em documentos específicos, assegurando a clareza e a efetividade na aplicação de cada medida.

8. RISCOS DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos é fundamental para proteger os ativos institucionais e assegurar a continuidade das operações do Sesc Goiás. Todos os colaboradores, fornecedores e parceiros devem seguir as diretrizes desta política para identificar, mitigar e prevenir riscos. A não observância dessas diretrizes pode comprometer os negócios, causar violações legais e impactar negativamente a reputação da instituição.

Incidentes de segurança e suspeitas de violações de dados pessoais devem ser comunicados imediatamente ao superior imediato e ao Encarregado pelo Tratamento de Dados Pessoais, pelo e-mail: dpo@sescgo.com.br.

9. PAPEIS E RESPONSABILIDADES

9.1. Colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT, estagiário, menor ou jovem aprendiz, terceirizado, prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do Sesc Goiás.

É dever dos colaboradores:

- Cumprir e respeitar esta política e documentos complementares.
- Proteger os recursos computacionais sob sua responsabilidade.
- Manter sigilo sobre credenciais e informações institucionais.
- Relatar prontamente incidentes ou ameaças à segurança à área de TI e ao Encarregado de Dados.

- Participar de treinamentos de segurança e privacidade promovidos pela organização.
- Assegurar que informações do Sesc Goiás não sejam compartilhadas sem autorização.
- Abster-se de qualquer conduta que configure colaboração para causar invasão de computadores ou da rede, conforme previsto no artigo 154-A do Código Penal Brasileiro.

9.2. Gestão de Pessoas

- Analisar candidatos para cargos com acesso a informações sensíveis.
- Garantir que novos colaboradores recebam orientações sobre segurança da informação e privacidade de dados pessoais.
- Solicitar criação, alteração ou desativação de acessos quando necessário.
- Quando requisitado, auxiliar na implementação de treinamentos sobre segurança e privacidade.
- Garantir devolução de ativos e remoção de acessos ao término de contratos.
- Aplicar medidas disciplinares em casos de violações ou incidentes de segurança.

9.3. Tecnologia de Informação

- Manter a Política de Segurança da Informação (PSI) e as normas internas de segurança da informação atualizadas, divulgadas e em conformidade com a legislação vigente.
- Promover a conscientização e a capacitação sobre a importância da segurança da informação, incentivando a adoção de boas práticas.
- Implementar um plano de gestão de incidentes.
- Tomar todas as providências necessárias diante de um incidente de segurança da informação a fim de mitigar possíveis consequências para a instituição.
- Prover pareceres sobre assuntos relativos à segurança da informação, elaborar documentos e relatórios quando solicitado pela Direção ou no âmbito de suas atribuições.
- Implementar medidas de segurança para sistemas da informação.
- Configurar equipamentos, inclusive os de uso particular quando utilizados para prestação de serviços para a Instituição, ferramentas e sistemas concedidos aos usuários com todos os controles necessários para atender aos requisitos de segurança.
- Implementar a segregação de funções administrativas e operacionais para minimizar o risco de acessos indevidos.

- Atribuir cada conta de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como usuário.
- Proteger continuamente todos os ativos de informação da Instituição, garantindo que estejam livres de código malware e outras ameaças cibernéticas.
- Administrar, proteger e testar regularmente as cópias de segurança dos sistemas críticos e relevantes para a instituição, garantindo a recuperação rápida e completa dos dados em caso de desastre.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Realizar administração, manutenção e monitoramento dos sistemas computacionais, podendo acessar os arquivos e dados para a execução de atividades operacionais sob sua responsabilidade.
- Gerenciar e responder a incidentes de segurança e violações de dados de forma eficaz, minimizando o impacto no negócio.

9.4. Encarregado de Proteção de Dados Pessoais

- Atuar como canal de comunicação entre a Instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- Estabelecer normas e padrões para assegurar que a Instituição cumpra a Lei Geral de Proteção de dados Pessoais.
- Disseminar as boas práticas em proteção de dados pessoais.
- Monitorar a conformidade em relação a proteção de dados pessoais.

9.5. Conformidade

- Validar contratos e cláusulas de proteção de dados e confidencialidade.
- Colaborar na atualização de políticas e documentos complementares.
- Zelar pela aplicação efetiva das melhores práticas em Segurança da Informação e Privacidade.
- Facilitar a identificação das obrigações legais de segurança da informação, bem como proteção e privacidade de dados pessoais.
- Documentar a avaliação dos riscos de segurança da informação e privacidade.
- Prover aconselhamento sobre assuntos relacionados a conformidade.

9.6. Alta Direção

- Aprovar esta Política.
- Garantir aplicação das melhores práticas em segurança e privacidade.
- Assegurar recursos adequados para implementar as diretrizes.
- Tomar medidas corretivas em casos de desconformidades.
- Promover a cultura em segurança da informação e privacidade.

10. POLÍTICAS COMPLEMENTARES

Serão criadas, aprovadas e implementadas as seguintes políticas complementares, para apoiar o Programa de Privacidade e Proteção de Dados do Sesc Goiás:

1. Política de Backup e Recuperação de Dados;
2. Política de uso dos ativos TI;
3. Política de Controle de Acesso;
4. Política de uso de dispositivos móveis;
5. Política de Acesso Remoto;
6. Política de Gestão de Vulnerabilidades;
7. Política de Privacidade;
8. Plano de Respostas a Incidentes;
9. Política de Atendimento aos Titulares.

11. DÚVIDAS E INFORMAÇÕES

Se precisar de esclarecimentos sobre suas informações ou desejar exercer seus direitos como Titular de Dados Pessoais, entre em contato com o Encarregado de Dados pelo e-mail dpo@sescgo.com.br. Todas as solicitações serão atendidas de forma gratuita, mediante a confirmação da sua identidade e a análise da viabilidade de atendimento, em conformidade com as exigências legais e regulatórias aplicáveis.

12. DOCUMENTOS DE REFERÊNCIAS

- ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação;

- ABNT NBR ISO/IEC 27701:2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;
- Lei n. 13.709/2018 - Lei Geral de Proteção de Dados.
- Marco Civil da Internet – Lei nº 12.965/2014.

Atualizações da Política de Segurança da Informação

Esta Política de Segurança da Informação é mantida atualizada para refletir a preocupação do Sesc Goiás com a privacidade e proteção de dados. Modificações serão realizadas para adequação à legislação, em novos riscos identificados que possam prejudicar a segurança da informação ou para trazer melhorias.