INSTRUÇÃO DE SERVIÇO CONJUNTA Nº 01/2020

"Institui a nova Política de Segurança da Informação no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC."

O Diretor de Serviços Corporativos da CNI, do SESI/DN, do SENAI/DN e do IEL/NC em conjunto com o Superintendente de Tecnologia da Informação no uso de suas atribuições, e

CONSIDERANDO os termos da Ordem de Serviço Conjunta nº 02/2016 que revogou o Ato CSC nº 02/2006 que tratava da Política de Segurança da Informação, e deu outras providências;

CONSIDERANDO que a Ordem de Serviço Conjunta nº 02/2016 autorizou o Diretor de Serviços Corporativos, em conjunto com o Gerente Executivo da Área de Administração, Documentação e Informação, a baixar instrução de serviço conjunta instituindo a "Política de Segurança da Informação" que passou a reger a matéria no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC.

CONSIDERANDO a necessidade de atualização das regras do processo de gestão da informação;

RESOLVEM:

Art. 1° Instituir a Política de Segurança da Informação no âmbito da CNI, do SESI/DN, do SENAI/DN e do IEL/NC, conforme anexo único.

Art. 2° A Política de Segurança da Informação instituída por meio do presente ato poderá ser revisada e alterada a qualquer tempo, se houver necessidade.

Art. 3° Esta Instrução de Serviço revoga a Instrução de Serviço Conjunta 02/2016.

Art. 4° Esta Instrução de Serviço entrará em vigor a partir de sua assinatura.

Registre-se, dê-se ciência e cumpra-se.

Brasília, 14 de setembro de 2020.

Fernando Augusto Trivellato Andrade
Diretor de Serviços Corporativos

Augusto Antônio Carelli Filho
Superintendente de Tecnologia da Informação

POLÍTICA		Data da Criação -
POL Nº 01	Revisão	Data da Revalidação -
Título: Política de Segurança da Informação		
Processo: Governança		
Elaborador: - Comitê de Segurança da Informação e de Proteção de Dados - Augusto Antônio Carelli Filho	**Aprovador:** Fernando Augusto Trivellato Andrade	
Cargo do elaborador: Superintendente de Tecnologia da Informação **Área:** Superintendência de Tecnologia da Informação (STI)	**Cargo do aprovador:** Diretor de Serviços Corporativos **Área:** Diretoria de Serviços Corporativos (DSC)	

Sumário

1. Introdução

A Política de Segurança da Informação (PSI) no âmbito das entidades e dos órgãos nacionais do Sistema Indústria: Confederação Nacional da Indústria – CNI, Serviço Social da Indústria – Departamento Nacional (SESI/DN), Serviço Nacional de Aprendizagem Industrial – Departamento Nacional (SENAI/DN) e pelo Instituto Evaldo Lodi – Núcleo Central (IEL/NC), busca a conformidade com as leis e regulamentações vigentes e está totalmente alinhada às práticas de Governança Corporativa, e com os objetivos estratégicos dessas entidades e órgãos nacionais.

Seu principal interlocutor é o Comitê de Segurança da Informação e de Proteção de dados, criado em 2017, com o papel de direcionar as ações estratégicas de segurança. O comitê é formado por uma equipe multidisciplinar composta por diversas áreas das entidades e dos órgãos nacionais do Sistema Indústria.

Toda estrutura deste documento promove o desenvolvimento de outras políticas, normas e procedimentos específicos para garantir a segurança das informações.

Dessa forma evoluímos no quesito maturidade do Sistema de Gestão de Segurança da Informação, tornando possível atingir os objetivos estabelecidos, sempre atendendo à premissa de avaliar melhor as ameaças e vulnerabilidades existentes, permitindo um
entendimento maior dos riscos que possam afetar os ativos de informação, como os processos, ambiente físico, pessoas, sistemas, informações e equipamentos.

2. Glossário

- CNI – entidades e órgãos nacionais do Sistema Indústria - Confederação Nacional da Indústria.
- SESI/DN – Serviço Social da Indústria – Departamento Nacional.

- SENAI/DN – Serviço Nacional de Aprendizagem Industrial – Departamento Nacional.
- IEL/NC – Instituto Evaldo Lodi – Núcleo Central.
- PSI – Política de Segurança da Informação.
- CSIPD – Comitê de Segurança da Informação e Proteção de dados.
- SI – Segurança da Informação.
- ISO – Abreviação de International Organization for Standardization (Organização Internacional de Normalização).
- Dirigentes – São os diretores estatutários, regulamentares e regimentais, sem vínculo empregatício com as Entidades e órgãos nacionais do Sistema Indústria, que não recebem salário ou qualquer tipo de remuneração pelo trabalho prestado, e que têm acesso à informação.
- Colaboradores – empregados e estagiários que desempenham suas atividades nas entidades e órgãos nacionais do Sistema Indústria.
- Empregado – toda pessoa que desempenha atividades com vínculo empregatício nas Entidades e órgãos nacionais do Sistema Indústria.
- Estagiário - pessoa que se beneficia diretamente de ato educativo escolar supervisionado, desenvolvido no ambiente de trabalho, ambiente este que visa sua preparação para o trabalho produtivo, e que esteja frequentando o ensino regular em instituições de educação superior, de educação profissional, de ensino médio, da educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, e que tem, eventualmente, acesso à informação no âmbito das Entidades e órgãos nacionais do Sistema Indústria.
- Prestador de serviço - pessoa física ou jurídica que exerce suas atividades por conta própria, sem vínculo empregatício com seus contratantes, não possuindo horário determinado, nem recebendo salário, mas sim remuneração prevista em contrato.
- Terceiros – pessoa física contratada por uma empresa de trabalho temporário que a coloca à disposição de uma empresa tomadora de serviços, para atender à necessidade de substituição transitória de pessoal permanente ou à demanda complementar de serviços, e que possua acesso à informação.
- Parceiro – pessoa física ou jurídica que possui um relacionamento com as entidades e órgãos nacionais do Sistema Indústria, exercendo suas atividades sem vínculo empregatício com seus contratantes, não recebe salário, apenas estabelece acordos para atingir interesses incomuns visando a sustentabilidade empresarial.

- Visitantes – toda pessoa que acessa o ambiente físico das entidades e órgãos nacionais do Sistema Indústria por um período de tempo e sem ser dirigente, empregado, estagiário, terceiro, prestador de serviço, cliente ou parceiro, não desempenhando suas atividades nestas entidades e órgãos nacionais, e não possuindo acesso à informação.
- Usuário – pessoa física ou jurídica que faz uso de computadores e sistemas.
- Detentor da informação – Pessoa responsável pela administração das informações geridas nos processos de trabalho sobre sua responsabilidade.
- Titular – pessoa natural/física a quem se referem os dados pessoais que são objeto de tratamento.
- Tratamento – Toda operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à classificação, utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, à modificação, à comunicação, à transferência, à difusão ou à extração, seja por meios automatizados ou não.
- Política – documento com orientações e direcionamentos.
- Norma – define regra para a execução de procedimentos.
- Procedimento – Define ações técnicas e específicas.
- Incidentes de Segurança da Informação – Evento imprevisível que afeta os princípios de segurança.

3. Abrangência

A PSI por se tratar de uma política corporativa, estende-se a todos os colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, independentemente do nível hierárquico ou período do vínculo de trabalho. Considera-se que todos possuam acesso às informações, sejam elas transmitidas por meio social, interpessoal, mídia audiovisual, visual, verbal, no formato físico ou digital.

Todas as informações aqui tratadas pertencem exclusivamente às entidades e órgãos nacionais do Sistema Indústria e devem respeitar o processo de classificação da informação estabelecido em todo o seu ciclo de vida.

4. Referências normativas e conformidade

As diretrizes desta política foram embasadas nas melhores práticas de mercado alusivas à segurança de informação e também nas normas pertencentes à família ISO/IEC 27000, em sua última versão.

Faz-se também referência às políticas e normas em vigor nas entidades e órgão nacionais do Sistema Indústria tais como o Código de Ética, estatutos, regulamentos e regimentos.

5. Objetivo

Estabelecer diretrizes e orientações aos colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, quanto ao tema Segurança da Informação, estabelecendo padrões de gestão da informação adequados ao modelo de negócio aplicável às entidades e órgão nacionais do Sistema Indústria, garantindo a proteção legal da empresa e de todas as pessoas.

6. Responsabilidades

6.1 Colaboradores, dirigentes, terceiros e prestadores de serviço

- Compreender e cumprir a Política de Segurança da Informação.
- Obedecer à devida classificação das informações.
- Estar de acordo com os termos de responsabilidade e confidencialidade.
- Comunicar possíveis desvios de conduta quanto à política através do canal de reporte a incidentes de segurança.
- Fazer bom uso das informações.
- Ser agentes de segurança da informação dentro e fora da organização, apoiando as demais Federações e Departamentos Regionais (DRs) sempre que necessário.
- Reportar qualquer desvio identificado para o responsável imediato.

6.2 Presidência

- Direcionar as ações estratégicas de segurança da informação.

6.3 Comitê de Segurança da Informação e Proteção de dados

- Fomentar o assunto Segurança da Informação e Proteção de Dados em toda estrutura organizacional.
- Debater, definir e aprimorar os controles estabelecidos na PSI.
- Apoiar as diretorias e os gestores na tratativa de incidentes de segurança.
- Estruturar os programas de comunicação focados em conscientização dos colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, no tema Segurança da Informação e Proteção de Dados.

6.4 Diretorias, Superintendências e Gerências

- Apoiar na divulgação do tema e promover a conscientização dos colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes.
- Fiscalizar e certificar colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes, quanto à aderência das práticas às ações de segurança.
- Comunicar incidentes de segurança da informação através do canal de reporte a incidentes de segurança.

6.5 Parceiros e Visitantes

- Seguir as políticas e os normativos de segurança estabelecidos.

7. Princípios

Os princípios de Segurança da Informação devem ser a referência para a definição de controles de proteção à informação. Dessa forma, têm-se as seguintes definições:

- **Integridade** – as informações devem ser íntegras, não podendo sofrer modificações não autorizadas.
- **Confidencialidade** – as informações devem obedecer à sua classificação, sendo que apenas pessoas autorizadas devem ter acesso à informação.
- **Disponibilidade** – as informações devem estar acessíveis e utilizáveis sempre que forem requisitadas.
- **Autenticidade** – as informações devem ser autênticas, garantindo a origem. Não podem haver ações de não repúdio.
- **Legalidade** – as informações devem obter seu devido tratamento e atender às leis e regulamentações vigentes.

8. Acesso à Política de Segurança da Informação

Os Colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros e visitantes podem e devem ter acesso à Política de Segurança da Informação (PSI) sempre que for necessário.

9. Treinamento

Todo conteúdo disponível nos treinamentos relacionados à Segurança da Informação atende às necessidades comuns, transversais a todas as áreas, alinhadas às necessidades estratégicas da área de atuação dos colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros, visitantes, e, por consequência, da organização. Todo o programa está alinhado às diretrizes estabelecidas na Política de Educação, Treinamento e Desenvolvimento (ETD).

Todas as dúvidas referentes ao tema podem ser reportadas para o *e-mail* segurancadainformacao@cni.com.br.

10. Comitê de Segurança da Informação e de Proteção de Dados

O comitê foi constituído para atuação de forma estratégica, com o objetivo de estabelecer novos direcionamentos, manter e aprimorar a PSI, bem como elevar a maturidade da organização quanto aos assuntos referentes à Segurança da Informação. Esse comitê é multidisciplinar e interdepartamental capaz de apoiar todos os colaboradores no esclarecimento e na aderência aos assuntos relacionados à Segurança da Informação e Proteção de Dados.

Todos os informativos e reportes ao comitê devem ser feitos por meio do e-mail: segurancadainformacao@cni.com.br.

11. Normas gerais

11.1 Segurança em recursos humanos

- É assegurado que colaboradores, dirigentes, terceiros, prestadores de serviço entendam as suas responsabilidades e estejam em conformidade com os papéis para os quais foram selecionados, em destaque, posições estratégicas e que atuem com Segurança da Informação.
- Conscientização, educação e treinamento de Segurança da Informação.
  - Todos os colaboradores devem ter o conhecimento das diretrizes estabelecidas na PSI e demais normas relacionadas.
  - São obrigatórias a leitura e a assinatura formal do termo de ciência aos colaboradores concordando com a PSI.
  - A não observância da PSI será considerada uma não conformidade e, após as devidas apurações, o Comitê de Segurança da Informação e de Proteção de Dados poderá sugerir medidas disciplinares.

11.1.1 Processo disciplinar

- As violações das diretrizes da PSI são caracterizadas como um incidente de Segurança da Informação e podem ser cometidas por colaboradores, dirigentes, terceiros, prestadores de serviço e visitantes. Tais violações deverão ser registradas e tratadas pontualmente pelo Comitê de Segurança da Informação e de Proteção de Dados, considerando as seguintes ações de contorno:
  - Ações de esclarecimento, educação e treinamento.
  - Ajustes de processos, situações ou condutas.
  - Advertência verbal, advertência por escrito, suspensão ou demissão.
  - Destituição do representante designado.

11.1.2 Encerramento e mudanças da contratação

- O encerramento das atividades do colaborador, deve ser devidamente comunicado pelo gestor imediato aos demais colaboradores, dirigentes, terceiros, prestadores de serviço, parceiros, sempre que for necessário.

11.2 Gestão de ativos

- Os ativos devem possuir controles de segurança adequados que atendam aos requisitos do negócio e que possam garantir o mínimo de segurança a processos, pessoas, tecnologia, informação e ambiente.

  Desta forma um inventário dos ativos deve ser mantido atualizado.

11.3 Classificação da informação

- As informações transmitidas por meio da fala, em formato digital ou físico, devem possuir a sua devida classificação. São elas:

- **Sigiloso**: são informações que contém restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do estado.
- **Confidencial**: Os documentos classificados como confidenciais são limitados, e sua divulgação pode trazer prejuízos e impactos.
- **Restrita**: Os documentos de caráter restrito são limitados a um grupo de pessoas, a divulgação pode violar a integridade das informações caso seja acessada por pessoas indevidas.
- **Interna**: Documentos internos limitam-se à organização e não devem ser divulgados externamente.
- **Pública**: as informações de caráter público podem ser acessadas sem controle de acessos.

- A rotulação das informações não é obrigatória, porém devem ser realizadas quando necessário pelo responsável da informação, obedecendo o layout estabelecido do documento.
- A classificação é feita pelos próprios donos da informação, garantindo o acesso ou limitando-o a pessoas não autorizadas.
- O manuseio das informações deve ser realizado conforme a classificação estabelecida.
  - Deve ser evitado o envio de documentos **Confidenciais** por *e-mail*, ou qualquer outro meio físico ou eletrônico a terceiros. Caso seja necessário, deve-se rotular a informação com a sua classificação e definir as restrições de acesso.
  - Documentos **Restritos** devem ser compartilhados somente a grupos internos específicos, obedecendo o nível de permissão estabelecido.
  - Documentos **Internos** não devem ser compartilhados externamente.

- Documentos públicos podem ser acessados ou compartilhados externamente, porém o compartilhamento deve ser realizado pela da área responsável pela Comunicação.

11.4 Transporte de mídias

- As informações que são transportadas via mensageiro ou transportadora devem ser de origem confiável e adequadas conforme a classificação da informação.
- O transporte de mídia com informações pertencentes às entidades e órgão nacionais do Sistema Indústria devem possuir controles adequados de segurança e que seja feito apenas por pessoas autorizadas.

11.5 Descarte de informações

- Informações físicas devem ser descartadas via desfragmentadora ou manualmente até que impossibilite a reconstrução da informação.
- As mídias, como pen-drive, HDs, CDs, fitas de backup, devem ser descartadas seguindo um processo de descarte e controlado via inventário de ativos.

11.6 Controle de Acesso

- O controle de acessos, no âmbito lógico ou físico, deve ser concedido mediante a solicitação e possuir autorização formal do responsável ou gestor imediato.
- As regras para a concessão dos acessos devem ser apropriadas, com base em papéis específicos dos colaboradores, dirigentes, terceiros e prestadores de serviço e considerar a devida classificação da informação.

11.7 Uso de correio eletrônico e Internet

- Os recursos de correio eletrônico e Internet estão disponíveis para todos os colaboradores, dirigentes, terceiros, prestadores de serviço e visitantes, que estiverem de acordo com as diretrizes de segurança. A **'Norma de utilização - Correio eletrônico e acesso à Internet'** está disponível na intranet e orienta todas as Entidades e órgão nacionais do Sistema Indústria quanto às regras de utilização, de forma a preservar os princípios básicos da segurança da informação, assim como, garantir que os recursos aplicados sejam utilizados para atender aos objetivos de negócio.

11.8 Recursos computacionais

- O uso dos recursos computacionais deve ser feito de forma adequada, conforme as orientações descritas na **'Norma de utilização - Recursos Computacionais'** disponível na intranet.

11.9 Áreas Seguras

- As entradas principais e demais áreas comuns contém acesso controlado.
- Apenas pessoas autorizadas devem possuir acesso.
- Todos os visitantes devem sempre estar devidamente autorizados e identificados.
- Todos os acessos devem registrar data e horário de passagem pela catraca.
- Todos os colaboradores devem possuir o crachá de identificação em um local visível. Caso um colaborador esteja sem identificação, este deve ser abordado e orientado.

11.10 Impressoras e Multifuncionais

- O uso de equipamentos de impressão e reprografia devem ser feitos exclusivamente para impressão e/ou reprodução de documentos que sejam de interesse da organização ou que

estejam relacionados com o desempenho das atividades profissionais do usuário.

- As impressões devem ser controladas através de usuário e senha individual.
- As cópias devem ser recolhidas na impressora sempre que forem impressas pelos usuários principalmente quando se tratar de informações confidenciais e/ou sigilosas.

11.11 Uso de Senhas

- As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo. Todos os colaboradores, dirigentes, terceiros, parceiros de serviço e visitantes devem seguir as orientações estabelecidas para o uso de senhas por meio da **'Norma – Política de Senhas'** disponível na intranet.

11.12 Política de Mesa e tela limpa

- As informações quando físicas (impressas) ou até mesmo em formato digital, devem ser posicionadas de maneira organizada para mitigar a possibilidade de acesso indevido.
- Sempre que possível as informações físicas devem ser armazenadas em gavetas ou armários com chave.
- A classificação da informação deve ser considerada para que o tratamento seja adequado.

É dever de todos os colaboradores, dirigentes, terceiros, prestadores de serviço:

- Fora do expediente de trabalho, garantir que os documentos impressos, mídias eletrônicas e demais objetos sejam guardados

em locais apropriados como armários, cofres, ou qualquer tipo de mobília que possua chave.

- Todas as estações de trabalho devem ser desligadas no final do expediente.
- Após o uso das salas, descartar os Flip Chart usados e apagar todas as informações da lousa.
- Sempre que se ausentar da estação de trabalho a tela deve ser bloqueada.
- Sempre que possível, evitar a impressão de documentos sensíveis.

11.13 Segurança nas Operações

A operação deve atender aos requisitos de segurança para que não resulte em violação aos princípios de segurança como a confidencialidade, disponibilidade, integridade, autenticidade e legalidade. Dessa forma, foram estabelecidos controles para as frentes detalhadas a seguir:

11.13.1 Gestão de Mudanças

- Todas mudanças que modifiquem o ambiente produtivo devem ser documentadas, testadas e validadas antes e depois de aplicadas em ambiente de produção.
- As janelas de mudanças devem ser respeitadas conforme o planejamento interno.
- As exceções devem ser tratadas como mudanças emergenciais.

11.13.2 Gestão de Incidentes de Segurança da Informação

São considerados incidentes de segurança da informação os eventos que afetam os princípios de segurança como a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade, e estes são divididos em duas categorias:

- Incidentes técnicos: afetam os equipamentos tecnológicos causando alguma indisponibilidade ou limitação no seu funcionamento.
- Incidentes corporativos: afetam a organização no que diz respeito aos processos e pessoas.

Dessa forma devemos:

- Seguir o processo padrão para tratamento de incidentes de Segurança da Informação.
- A comunicação interna deve ser realizada obedecendo os prazos estabelecidos pelo processo.
- Times de especialistas para tratamento do incidente devem ser acionados sempre que necessário.
- Uma investigação deve ser realizada e documentada para identificar a causa raiz via chamado.
- Os incidentes de segurança críticos devem ser reportados para o Comitê de Segurança da Informação e de Proteção de Dados.
- Em casos de incidentes de segurança que causarem indisponibilidades que afetam o negócio, deve-se acionar planos de continuidade do negócio até que o ambiente seja recuperado.

11.13.3 Gestão de Vulnerabilidades

- Os sistemas, os aplicativos, e os demais ambientes devem ser avaliados periodicamente com o objetivo de identificar vulnerabilidades.
- As vulnerabilidades encontradas devem ser tratadas e resolvidas pelas áreas responsáveis.

11.13.4 Backup e Recuperação de dados

- O processo de backup das informações deve ser realizado periodicamente conforme a política estabelecida, incluindo os principais sistemas, a base de dados, os arquivos departamentais e de usuários.
- Testes de recuperação de dados devem ser realizados periodicamente com o objetivo de validar a sua integridade.
- A recuperação de dados somente será possível mediante a solicitação formal e aprovação do dono da informação ou gestor imediato.

11.14 Desenvolvimento Seguro

- A arquitetura de aplicativos, de serviços e de sistemas desenvolvidos internamente deve seguir as melhores práticas de mercado, obedecendo a critérios de segurança, seja ele internamente ou realizado através de parceiros.

11.15 Continuidade do Negócio

- Os processos para tratar a continuidade do negócio, devem ser estabelecidos com base nos processos mais críticos.
- Os testes de mesa devem ser realizados para que se tenha a validação dos planos de continuidade.

11.16 Privacidade e Proteção de Dados

A privacidade deve ser garantida para todos os titulares de dados, inclusive, para a organização por meio da implementação de controles de segurança específicos. Dessa forma as ações para atingir a conformidade com as leis e regulamentações, devem seguir as práticas e controles que atendam a proteção e a privacidade das informações conforme descritas na "Política de Privacidade e Proteção de Dados" em vigor.

11.17 Redes Sociais

As entidades e órgãos nacionais do Sistema Indústria, participam efetivamente de redes sociais, sendo esse um importante canal de sua comunicação com a sociedade. Desta maneira:

- Apenas a área da Gerência Executiva de Mídias Sociais está autorizada a criar e/ou compartilhar informações em nome das entidades e órgão nacionais do Sistema Indústria.
- Em suas redes pessoais, os colaboradores devem estar atentos ao citar o nome das entidades e órgão nacionais do Sistema Indústria e ao abordar temas de interesse da instituição ou temas políticos para que esses posicionamentos pessoais não interfiram no trabalho desempenhado na instituição. Dessa maneira, o conteúdo citado ou compartilhado não pode ferir a imagem da instituição e deve respeitar a sua classificação.
- Dúvidas podem ser reportadas à área de comunicação.

Qualquer ação que viole essa política deve ser reportada ao Comitê de Segurança da Informação e de Proteção de Dados pelo e-mail segurancadainformacao@cni.com.br ou pelo formulário "Fale Conosco" do site principal do Portal da Indústria.