INSTRUÇÃO DE SERVIÇO CONJUNTA CNI/SESI/SENAI/IEL/DSC/ADINF Nº 02/2016

"Institui a 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 gerente executivo da Área de Administração, Documentação e 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 passará 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. 1º 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. 2º A Política de Segurança da Informação instituída por meio do presente ato poderá ser revisada e alterada a qualquer tempo, se houver necessidade.

Art. 3º Determinar que esta Instrução de Serviço Conjunta entra em vigor na data de sua assinatura, revogando-se as disposições em contrário.

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

Brasília, 05 de maio de 2016.

FERNANDO AUGUSTO TRIVELLATO ANDRADE
Diretor de Serviços Corporativos

MAURÍCIO VASCONCELOS DE CARVALHO
Gerente Executivo da Área de Administração, Documentação e Informação

DIRETORIA JURÍDICA
Fabiola Pasini

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

1 OBJETIVO

1.1 Esta Política tem por finalidade formalizar o direcionamento estratégico das informações das entidades e órgãos nacionais do Sistema Indústria no que tange à integridade, confidencialidade e disponibilidade por meio de diretrizes que padronizem o comportamento relacionado à segurança da informação, em qualquer meio ou suporte, destinados às necessidades de negócio e de proteção legal da instituição e do indivíduo.

2 CONCEITOS E DEFINIÇÕES:

2.1 Segundo definição da norma ABNT NBR ISO/IEC 27002:2005, "*A <u>informação</u> é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada 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.*"

2.1.1 De acordo com a mesma norma, "*<u>Segurança da informação</u> é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*"

2.2 Para maior clareza deste documento são adotadas as seguintes definições:

a) **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335-1:2004]

b) **ABNT:** Sigla da Associação Brasileira de Normas Técnicas - órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.

c) **Ativo:** qualquer componente (humano, tecnológico, físico ou lógico) que

DIRETORIA JURÍDICA-DF
Fabiola Pasini

tenha valor para a organização. [ISO/IEC 13335-1:2004].

d) **Colaborador:** empregados e estagiários das entidades e órgãos nacionais do Sistema Indústria.

e) **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

f) **Controle:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005]

g) **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

h) **Gestor de informação:** Empregado das entidades e órgãos nacionais do Sistema Indústria, que exerça função de confiança, responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade.

i) **Informação:** todo e qualquer dado gerado, acessado, armazenado, transmitido, alterado ou descartado por meio de recurso físico ou computacional, como por exemplo: e-mail, arquivos textos, planilhas eletrônicas, base de dados, imagens, código-fonte de sistemas, sites Internet, apresentações, arquivos de som, arquivos de vídeo.

j) **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais. Somente alterações, supressões e adições autorizadas pela instituição devem ser realizadas;

k) **ISO:** International Organization for Standardization.

l) **Processos críticos:** processos que contenham informações críticas para os negócios das entidades e órgãos nacionais do Sistema Indústria ou de seus clientes.

m) **PSI-** Política de Segurança da Informação

DIRETORIA JURÍDICA-DF
Fabíola Pasini

n) **Recurso físico:** todo recurso não computacional utilizado na geração, processamento, armazenamento, transmissão, descarte e recuperação da informação, tais como: papel, gravador de voz, videocassete, filmadoras, máquinas fotográficas.

o) **Recursos computacionais:** todo recurso utilizado na geração, processamento, armazenamento, transmissão, descarte e recuperação da informação em meio eletrônico

p) **Rede Corporativa Local**: conjunto de servidores de rede e equipamentos de interconexão locais, interligados com o objetivo de disponibilizar serviços aos usuários das entidades e órgãos nacionais do Sistema Indústria.

q) **Risco:** combinação da probabilidade de um evento e de suas consequências. [ABNT ISO/IEC Guia 73:2005];

r) **Termo de cessão de direitos autorais:** documento formal que trata expressamente da cessão, total ou parcial, gratuita ou onerosa, dos direitos do autor, por ele ou por seus sucessores, pessoalmente ou por meio de representantes com poderes especiais, a um terceiro pessoa física ou jurídica, a título universal, obedecidas as limitações constantes dos incisos do artigo 49 da Lei nº 9610/98;

s) **Titular da Unidade/Área:** pessoa responsável pela Unidade/Área.

t) **Unidades/Áreas:** todas as partes integrantes da estrutura organizacional das entidades e órgãos nacionais do Sistema Indústria.

3 REFERÊNCIAS LEGAIS E NORMATIVAS:

3.1 De forma não exaustiva as leis, e outros atos normativos, que correlacionam-se com a PSI, são as seguintes:

a) Lei 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

b) Lei 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

DIRETORIA JURÍDICA-DF
Fabiola Pasini

c) Lei 9279, de 14 de maio de 1996 (Regula direitos e obrigações relativos à propriedade industrial);

d) Lei 3129, de 14 de outubro de 1882 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

e) Lei 10406, de 10 de janeiro de 2002 (Institui o Código Civil);

f) Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

g) Lei 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias);

h) Guia de Direitos Autorais das entidades e órgãos nacionais do Sistema Indústria;

i) Código de Ética das entidades e órgãos nacionais do Sistema Indústria;

j) PSI – Política de Segurança da Informação Documento de Diretrizes e Normas Administrativas V.1.0 – SENAC;

k) Política de Segurança da Informação da Informática de Municípios Associados S/A (IMA);

l) Norma de Segurança da Tecnologia da Informação das entidades e órgãos nacionais do Sistema Indústria

4 PRINCÍPIOS

4.1 Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna das entidades e órgãos nacionais do Sistema Indústria, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

5 DIRETRIZES GERAIS

5.1 Esta política dá ciência de que os ambientes, sistemas, computadores e

DIRETORIA JURÍDICA-DF
Fabiola Pasini

redes de propriedade das entidades e órgãos nacionais do Sistema Indústria poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras e conforme definido na Norma de Segurança da Tecnologia da Informação.

5.2 Cabe ao colaborador, independentemente do nível hierárquico manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor, ou do gestor da PSI, sempre que julgar necessário para garantir a segurança quanto à aquisição, uso e/ou descarte de informações.

5.3 Toda informação produzida, recebida e transportada pelos colaboradores como resultado da atividade profissional contratada pelas entidades e órgãos nacionais do Sistema Indústria pertence à instituição. As exceções devem ser explicitadas e formalizadas em contrato entre as partes.

5.4 Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados pelo colaborador para a realização das atividades profissionais.

5.5 As entidades e órgãos nacionais do Sistema Indústria, por meio da Área de Tecnologia da Informação, poderão registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5.6 A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação. Todo colaborador deve ser orientado sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

5.7 Todo incidente que afete a segurança da informação deverá ser comunicado pelo colaborador ao seu gestor imediato, que deverá comunicar formalmente ao gestor da PSI para análise.

5.8 Destruição, modificação ou divulgação indevida das informações seja acidental ou intencional, que cause prejuízo ou dano às entidades e órgãos nacionais do Sistema Indústria e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas, será de inteira responsabilidade do colaborador que tenha dado causa.

5.9 Os recursos físicos ou computacionais das entidades e órgãos nacionais

DIRETORIA JURÍDICA-DF
Fabiola Pasini

do Sistema Indústria não poderão ser utilizados para constranger, assediar, ofender, caluniar, ameaçar ou praticar outros crimes, para fins políticos ou religiosos não institucionais, para causar prejuízos à pessoa física ou jurídica, nem para atividade particular que exceda o limite dos padrões aceitáveis de ética, bom senso ou razoabilidade, bem como usar a marca ou renome da instituição para se valer de interesses particulares.

5.10 TRATAMENTO DA INFORMAÇÃO

5.10.1 PROPRIEDADE DA INFORMAÇÃO

5.10.1.1 Toda informação produzida, recebida ou transportada pelo colaborador, no exercício de suas atividades, é de propriedade das entidades e órgãos nacionais do Sistema Indústria, e deverá ser protegida segundo as diretrizes descritas nesta política de segurança da informação e normas dela derivadas.

5.10.1.2 Toda informação gerada ou transportada por parceiros, mão-de-obra temporária ou prestadores de serviço, no exercício de atividades para as entidades e órgãos nacionais do Sistema Indústria, deverá ser protegida por meio de cláusulas contratuais que regulem a propriedade dos direitos autorais (Ver Guia de Direitos Autorais das entidades nacionais do Sistema Indústria).

5.10.1.3 Nos casos de obtenção de informação de terceiros, o Gestor da Informação, assessorado pela Diretoria Jurídica deverá, se necessário, providenciar junto ao fornecedor a documentação formal relativa à cessão de direitos sobre as informações, antes de seu uso.

5.10.1.4 Nos casos de cessão de informação das entidades e órgãos nacionais do Sistema Indústria a terceiros, o Gestor da Informação, assessorado pela Diretoria Jurídica deverá, se necessário, providenciar a documentação formal relativa à cessão de direitos sobre as informações.

5.10.2 CLASSIFICAÇÃO DA INFORMAÇÃO

5.10.2.1 Toda informação das entidades e órgãos nacionais do Sistema Indústria deverá ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita.

5.10.2.2 Os níveis de classificação abaixo foram definidos considerando a necessidade de balanceamento entre o nível de segurança a ser aplicado a

DIRETORIA JURÍDICA-DF
Fabiola Pasini

uma informação e sua importância para a continuidade dos processos das entidades e órgãos nacionais do Sistema Indústria.

5.10.2.2.1 Quanto à **Confidencialidade**:

a) **Confidencial** – Informação relacionada aos negócios, pessoas e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja divulgação somente será feita mediante autorização do Gestor da Informação, pois poderá comprometer seriamente seus processos, requerendo cuidados especiais para controlar seu acesso.

b) **De uso interno** – Informação relacionada aos negócios, pessoas e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja divulgação poderá ser feita no âmbito interno.

c) **De uso público** – Informação relacionada aos negócios, pessoas e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja divulgação poderá ser feita no âmbito externo.

5.10.2.2.2 Quanto à **Disponibilidade**

a) **Alta** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja indisponibilidade poderá ter consequências incontornáveis nos seus processos, requerendo cuidados especiais para garantir sua disponibilidade.

b) **Normal** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja indisponibilidade não terá consequências incontornáveis, mas, caso persista, poderá comprometer seus processos.

c) **Baixa** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja indisponibilidade não trará consequências para seus processos.

DIRETORIA JURÍDICA-DF
Fabiola Pasini

5.10.2.2.2.1 Quanto à disponibilidade, garantir que todo documento que deva ser de conhecimento do colaborador esteja acessível independente de sua condição física, localização geográfica ou idioma de origem. No caso de terceiros é de responsabilidade do gestor do contrato com terceiros fazer chegar o conhecimento da PSI.

5.10.2.2.3 Quanto à **Integridade**:

a) **Alta** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja falta de integridade poderá comprometer seriamente seus processos, requerendo cuidados especiais para garantir sua integridade.

b) **Normal** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja falta de integridade não terá consequências incontornáveis, mas, caso persista, poderá comprometer seus processos.

c) **Baixa** – Informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, cuja falta de integridade não trará consequências para seus processos.

5.10.2.3 A informação armazenada ou transportada nos recursos físicos ou computacionais das entidades e órgãos nacionais do Sistema Indústria, que não possuir uma classificação explícita será considerada de uso interno quanto à confidencialidade e de nível normal quanto à disponibilidade e integridade.

5.10.2.4 A classificação da informação é atribuição do Gestor da Informação, devendo este considerar o balanceamento entre a classificação da informação e o custo das medidas de segurança necessárias à sua proteção.

5.10.2.5 A informação eletrônica armazenada ou transportada fora da Rede Corporativa Local das entidades e órgãos nacionais do Sistema Indústria será tratada pela Área de Tecnologia da Informação como de baixa disponibilidade e baixa integridade, e deverá receber de seu portador os cuidados inerentes à sua confidencialidade.

5.10.3 SEGURANÇA ADEQUADA AO RISCO

DIRETORIA JURÍDICA-DF
Fabiola Pasini

5.10.3.1 Toda informação utilizada nas entidades e órgãos nacionais do Sistema Indústria deverá receber o tratamento adequado no momento da sua geração, atualização, acesso, guarda, proteção, controle e descarte, segundo a classificação recebida pelo seu Gestor da informação.

5.10.3.2 A Área de Tecnologia da Informação e/ou à área de Informação e Documentação, ao definir as medidas de segurança aplicáveis aos recursos físicos ou computacionais das entidades e órgãos nacionais do Sistema Indústria, deverão considerar o balanceamento entre os custos inerentes ao grau de segurança e a classificação da informação a proteger.

5.10.3.3 Toda informação relacionada aos negócios e políticas administrativas das entidades e órgãos nacionais do Sistema Indústria, se eletrônica, deverá ser armazenada nos servidores da sua Rede Corporativa Local; se não eletrônica, deverá ser mantida em local que a salvaguarde adequadamente, no arquivo local de cada área ou no arquivo central das entidades e órgãos nacionais do Sistema Indústria.

5.10.3.4 No descarte de informações das Entidades e órgãos Nacionais do Sistema Indústria deverão ser observados: a temporalidade prevista na legislação, as políticas, as normas, procedimentos internos e a classificação quanto à confidencialidade, cabendo ao Arquivo Central das entidades e órgãos nacionais do Sistema Indústria realizar o descarte de documentos obsoletos que se enquadrem nessas observações.

5.10.3.5 O descarte de informações classificadas como confidenciais deverá ser realizado de forma a impossibilitar sua recuperação total ou parcial.

5.11 GESTÃO DE RISCO

5.11.1 A inserção de recursos computacionais no ambiente das Entidades traz riscos que deverão ser controlados, conforme fixado em normas próprias, observando-se quanto a software, a necessidade de autorização dos fabricantes para uso nas entidades e órgãos nacionais do Sistema Indústria.

5.11.2 De forma a preservar a segurança das informações, os empregados das entidades e órgãos nacionais do Sistema Indústria deverão, sempre que necessário, ser orientados para a correta utilização dos recursos físicos e computacionais.

DIRETORIA JURÍDICA DF
Fabiola Pasini

5.11.3 Os Titulares das Unidades/Áreas, de forma a garantir a integridade das informações, deverão assegurar que não haja um único colaborador com a operação exclusiva de processos críticos.

5.11.4 No caso de perda indevida de informações, desenvolver metodologia sólida e estruturada, alinhada às principais normas e padrões internacionais. A gestão inclui as atividades de inventariar, analisar, avaliar e tratar os riscos, fornecendo suporte à tomada de decisões e facilitando o desenvolvimento de estratégias para controlar e minimizar os riscos a níveis aceitáveis pela organização.

5.12 GESTÃO DE CONTINUIDADE

5.12.1 A gestão de continuidade é o plano de operações estratégicas em um evento de interrupção, seja devido a um grande desastre ou um incidente menor. A ISO 22301, foi desenvolvida para minimizar tais risco de interrupções nos negócios. Caberá à alta gestão alinhar com os dirigentes institucionais para traçar o plano de continuidade das áreas de negócios

5.12.2 Os processos críticos deverão ser suportados por um plano de contingência, consistente com a sua importância, que garanta a continuidade dos serviços ou solucione situações de anormalidade. Este plano deve ser documentado e, periodicamente, testado e revisado pela área que possua a administração dos recursos que sustentam os processos.

5.13 CONTROLES DE ACESSO

5.13.1 Para garantir as regras mencionadas nesta PSI, as entidades e órgãos nacionais do Sistema Indústria poderão:

5.13.1.1 Implantar sistemas de monitoramento nos equipamentos e sistemas de propriedade das entidades e órgãos nacionais do Sistema Indústria (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;

5.13.1.2 Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gestor (ou superior) ou por determinação do Comitê de Segurança da Informação;

DIRETORIA JURÍDICA-DF
Fabiola Pasini

5.13.1.3 Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

5.13.1.3.1 Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

5.13.1.3.2 O acesso à informação e aos recursos físicos ou computacionais, pelo colaborador, deverá ser relacionado às suas atividades profissionais e aos interesses de negócios das entidades e órgãos nacionais do Sistema Indústria.

5.13.1.3.3 O perfil de acesso deverá ser definido pelo Titular da Unidade/Área à qual o colaborador está vinculado.

5.13.1.3.4 Quando do desligamento do colaborador das suas atribuições junto às entidades e órgãos nacionais do Sistema Indústria, este deverá ter seu acesso aos recursos físicos e computacionais bloqueado imediatamente.

5.13.1.3.5 Após o bloqueio, o colaborador que necessitar retirar suas informações particulares deverá solicitar a autorização de acesso ao seu superior imediato.

5.13.1.3.6 Os acessos do colaborador ao ambiente físico, que contenha informações das entidades e órgãos nacionais do Sistema Indústria, deverão se restringir aos necessários e indispensáveis à realização de suas atividades.

5.13.1.3.7 O acesso de visitante ao ambiente físico das entidades e órgãos nacionais do Sistema Indústria deve obedecer às políticas e normas específicas, de modo a assegurar a proteção das informações.

5.13.1.3.8 Não será permitida a captura ou transmissão de informações audiovisuais, por qualquer meio, nas instalações das entidades e órgãos nacionais do Sistema Indústria sem prévia autorização do Gestor da Informação.

6 PENALIDADES

DIRETORIA JURÍDICA-DF
Fabiola Pasini

6.1 A violação à PSI, às normas ou aos procedimentos de segurança da informação são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

7 COMPETÊNCIAS E RESPONSABILIDADES

7.1 A estrutura de segurança da informação é composta por:

a) Diretoria de Serviços Corporativos (DSC);
b) Gestor da Política de Segurança da Informação;
c) Colaboradores das Entidades Nacionais do Sistema Indústria

7.1.1 Diretoria de Serviços Corporativos (DSC)

7.1.1.1 Responsabilidades:

a) Indicar o Gestor da PSI, sem que esta indicação implique na necessidade de criação de algum cargo ou função na estrutura organizacional das entidades e órgãos nacionais do Sistema Indústria, ou alteração no enquadramento funcional do empregado indicado;

b) Constituir, sob demanda, grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e

c) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

7.1.2 Gestor da Política de Segurança da Informação

7.1.2.1 Responsabilidades

a) Promover cultura de segurança da informação e comunicações;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de segurança da informação e comunicações;

DIRETORIA JURÍDICA-DF
Fabiola Pasini

d) Acompanhar a resolução dos incidentes junto à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

e) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito das entidades e órgãos nacionais do Sistema Indústria.

7.1.3 Colaboradores das entidades e órgãos nacionais do Sistema Indústria

7.1.3.1 Os colaboradores das entidades e órgãos nacionais do Sistema Indústria têm por obrigação cumprir esta Política de Segurança da Informação e demais normas que a complementarem.

7.1.3.2 O colaborador é responsável pelos danos que, por sua ação ou omissão, possam ser causados às informações ou aos recursos físicos e computacionais das entidades e órgãos nacionais do Sistema Indústria.

7.1.3.3 O Gestor da Informação deve definir, em comum acordo com a área que possua a administração do recurso físico ou computacional, o período de retenção, guarda ou preservação da informação.

7.1.3.4 As áreas responsáveis pela administração dos recursos físicos ou computacionais em parceria com a área de recursos humanos e/ou comunicação devem, periodicamente, promover a disseminação e aplicação dos conceitos de segurança da informação.

8 ATUALIZAÇÃO

8.1.1 Esta Política e as normas que a complementam deverão ser revisados periodicamente pelas áreas envolvidas em sua elaboração e submetidas à Diretoria de Serviços Corporativos para aprovação.

9 DISPOSIÇÕES FINAIS

9.1 As infrações a esta Política e normas correlatas deverão ser comunicadas pelo gestor da PSI ao Gestor da Informação e ao superior imediato do infrator.

DIRETORIA JURÍDICA-DF
Fabiola Pasini

9.2 Em casos de quebra de segurança da informação por meio de recursos computacionais, a Área de Tecnologia da Informação deverá ser imediatamente acionada para tomar as providências necessárias para sanar as causas, podendo inclusive restringir temporariamente o acesso às informações e/ou ao uso dos recursos computacionais das entidades e órgãos nacionais do Sistema Indústria.

9.3 Ao autor de infração a esta política e normas correlatas deverão ser aplicadas as sanções legais cabíveis.

9.4 Os terceirizados somente estarão vinculados às regras desta Política de Segurança da Informação na medida e no limite em que as obrigações e sanções aqui descritas estiverem previstas nos contratos de seus empregadores com as entidades e órgãos nacionais do Sistema Indústria.

9.5 Os prestadores de serviço somente estarão vinculados às regras desta Política de Segurança da Informação na medida e no limite em que as obrigações e sanções aqui descritas estiverem previstas nos seus contratos com as entidades e órgãos nacionais do Sistema Indústria.

9.6 Os casos omissos serão resolvidos pelo diretor de Serviços Corporativos.

DIRETORIA JURÍDICA-DF
Fabiola Pasini