SUDECO
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO CENTRO-OESTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Política de Segurança da Informação e Comunicação da Superintendência do Desenvolvimento do Centro-Oeste - SUDECO

Cleber Ávila Ferreira
Superintendente

Comitê Gestor de Segurança da Informação e Comunicação

Leila Raquel Santana Almeida
(Gestora do CGSI)

Adriano de Souza Bezerra

Fabiane Aparecida da Silva Lima

Igor Outeiral da Silva

Priscilla Marotta Gardino

Thiago Correia Borges

Thiago Grudner Cuerda

Revisão
Kainã Aguiar Ferreira

Março de 2015

Brasília | DF

SUMÁRIO

1. INTRODUÇÃO

“Política de Segurança da Informação e Comunicação: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações”.

Inciso I do art. 2° da IN GSI/PR N° 01/2008, de 13 de junho de 2008.

A Política de Segurança da Informação e das Comunicações (POSIC) tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito da Superintendência do Desenvolvimento do Centro-Oeste. (SUDECO).

O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, na SUDECO.

Tal documento considera as recomendações e práticas propostas pelo Decreto n° 3.505/2000, pela IN GSI/PR n° 01/2008, pela norma internacional ABNT NBR ISO/IEC 27002:2005 e alinha-se, ainda, às demais leis e normas vigentes sobre o tema e às diretrizes estratégicas do órgão.

Considerando o disposto no art. 3° do Decreto n° 3.505/2000, são objetivos genéricos da Política de Segurança da Informação para a Administração Pública Federal a serem estabelecidos por todos os órgãos e entidades públicas em suas respectivas Políticas de Segurança da Informação:

A. Dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

B. Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

C. Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

D. Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

E. Promover as ações necessárias à implementação e manutenção da segurança da informação;

F. Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

G. Promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

H. Assegurar a interoperabilidade entre os sistemas de segurança da informação.

2. CAMPO DE APLICAÇÃO

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em toda a organização; Essa Política aplica-se a todos os servidores, colaboradores, estagiários da SUDECO e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da SUDECO.

Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

3. PRINCÍPIOS E OBJETIVOS

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são objetivos da Política de Segurança da Informação da SUDECO:

A. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.

B. Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação.

C. Apoiar a implantação das iniciativas relativas à Segurança da Informação.

D. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

São princípios da Política de Segurança da Informação da SUDECO:

A. Toda informação produzida ou recebida pelos agentes públicos, em resultado da função exercida e/ou atividade profissional contratada, pertence à SUDECO. As exceções devem ser explícitas e formalizadas entre as partes.

B. Todos os recursos de informação da SUDECO devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

C. 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, com vistas à redução dos riscos dos seus ativos de informação.

D. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade.

E. A SUDECO pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pelo instituto.

F. Cada usuário é responsável pela segurança das informações dentro da SUDECO, principalmente daquelas que estão sob sua responsabilidade.

G. Com o objetivo de reduzir o risco de descontinuidade das atividades do órgão e de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, deverão ser implantados planos de contingência e de continuidade para os principais serviços e sistemas; tais planos deverão ser implantados, revisados e testados periodicamente.

H. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, 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.

I. A gestão da segurança da informação na SUDECO será realizada por comitê multidisciplinar, ora designado Comitê Gestor de Segurança da Informação e Comunicação (CGSIC).

J. Deverá constar em todos os contratos da SUDECO, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na SUDECO, inclusive provenientes de organismos internacionais; deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, entrega de declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição.

K. Esta Política de Segurança da Informação será implementada na SUDECO por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

4. COMPETÊNCIAS E RESPONSABILIDADES

4.1 Competências

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	Servidores públicos, servidores sem vínculo, demais funcionários e colaboradores internos.	Todos os agentes públicos, que fazem uso dos recursos informacionais e computacionais da SUDECO.
USUÁRIO EXTERNO	Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pela SUDECO e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
GESTORES	Superintendente, Diretores, Coordenadores e demais cargos de chefia.	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TI	Divisão de Tecnologia da Informação (CGSLTI)	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.
GESTOR DE SIC	Gerência técnica	Servidor responsável pela gestão da segurança da informação em todos os seus aspectos.
COMITÊ DE SIC	Alta Administração	Equipe técnica responsável por implementar e administrar as soluções de segurança da informação.

4.2 Responsabilidades gerais

São responsabilidades gerais de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais da SUDECO:

A. Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.

B. Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do instituto.

C. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da SUDECO.

D. Manter-se atualizado em relação a esta POSIC e às normas e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação da instituição sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

4.3 Responsabilidades específicas

4.3.1 Usuários internos e externos

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar à SUDECO em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes.

Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. A SUDECO poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da política de SI ou das normas e procedimentos específicos dela decorrentes.

4.3.2 Gestores de pessoas e processos

Os gestores da SUDECO devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão.

Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação da SUDECO, tomando as ações necessárias para cumprir tal responsabilidade.

4.3.3 Área de Tecnologia da Informação

Quanto à gestão de segurança da informação, serão responsabilidades específicas da área de Tecnologia da Informação:

A. Zelar pela eficácia dos controles de SI utilizados e informar aos gestores e demais interessados os riscos residuais.

B. Negociar e acordar com os gestores níveis de serviço relacionados a SI, incluindo os procedimentos de resposta a incidentes.

C. Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

D. Gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes; para as trilhas geradas e/ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências.

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

F. Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações.

G. Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a SUDECO.

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

I. Nas movimentações internas dos ativos de TI, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

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

K. 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, responsável pelo uso da conta (a responsabilidade pela gestão dos "logins" de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades).

L. Proteger continuamente todos os ativos de informação do instituto 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.

M. Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da SUDECO ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas (quando tais ambientes forem acessados por terceiros, a responsabilização deve ser explicitada nas cláusulas dos instrumentos contratuais).

N. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente dedicados à visitação externa, exigindo o seu cumprimento dentro da autarquia.

O. Definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos.

P. Responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos2.

Q. Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da SUDECO, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do instituto.

R. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro.

S. 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; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança; e atividade de todos os usuários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails corporativos recebidos/enviados, upload/download de arquivos).

4.3.4 Gestor de Segurança da Informação

Em conformidade com o disposto no artigo 7° da IN GSI/PR n° 01/2008 incumbe ao Gestor de Segurança da Informação da SUDECO:

A. Promover cultura de segurança da informação e comunicações no âmbito de suas atribuições dentro da SUDECO.

B. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.

C. Propor recursos necessários às ações de segurança da informação.

D. Coordenar o Comitê Gestor de Segurança da Informação

E. Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação.

F. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República.

G. Propor normas internas relativas à segurança da informação.

4.3.5 Comitê Gestor de Segurança da Informação

É de responsabilidade específica do Comitê Gestor de Segurança da Informação:

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

B. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SUDECO.

C. Auxiliar na publicação e promoção da Política de Segurança da Informação, das normas, e procedimentos específicos decorrentes.

D. Promover a conscientização dos usuários em relação à relevância da segurança da informação para a SUDECO, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

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

F. Analisar criticamente incidentes de Segurança da Informação.

G. Disponibilizar as atas e os resumos das reuniões do Comitê Gestor de Segurança da Informação.

H. Buscar alinhamento das práticas de segurança da informação com as diretrizes corporativas da instituição.

I. Caberá, ainda, ao Comitê Gestor de Segurança da Informação propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos;

J. Avaliar os incidentes de segurança e propor ações corretivas;

K. Definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação e/ou das normas de segurança da informação complementares.

Em conformidade com o artigo 6° da IN GSI/PR n° 01/2008, compete ao Comitê Gestor de Segurança da Informação da SUDECO:

A. Assessorar o órgão na implementação das ações de segurança da informação.
B. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.
C. Propor alterações e revisar periodicamente a Política de Segurança da Informação da SUDECO, em conformidade com a legislação existente sobre o tema.
D. Propor, aprovar, alterar e revisar normas complementares e procedimentos internos de segurança da informação, em conformidade com a legislação existente sobre o tema.
E. Subsidiar o Comitê Gestor de Tecnologia da Informação da SUDECO nas decisões relativas à segurança da informação.

5. DIRETRIZES GERAIS

5.1 Tratamento da informação

Diretrizes específicas e procedimentos próprios de tratamento da informação corporativa deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. A informação utilizada pela SUDECO é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;

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

C. Arquivos pessoais e/ou não pertinentes às atividades institucionais da SUDECO (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

D. Normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Federal – considerando as competências regimentais.

E. Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação dessa Norma;

F. Todos os procedimentos que possibilitam a proteção da informação e a continuidade de seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos;

G. Toda informação crítica para o funcionamento da SUDECO deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada. A CGSLTI é responsável pela definição dessa criticidade.

5.2 Contas de Acesso e senhas

Diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e autenticação do usuário;

B. O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação da SUDECO.

C. O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica.

D. As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

E. Competirá à Divisão de TI o cadastramento/exclusão/modificação de contas de login dos colaboradores da SUDECO nas situações de ingresso/desligamento/realocação;

F. Todos os usuários devem assinar um termo de responsabilidade pela utilização da conta de acesso. Este termo deve ser entregue no momento do ingresso do colaborador na SUDECO;

Utilização de Contas de Acesso e Senhas

A conta de acesso é o instrumento para identificação do usuário na rede SUDECO e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese;

Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;

5.3. Acesso Físico e Lógico

A. Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos do DTI e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

B. Todo o pessoal envolvido em trabalhos de apoio, tais como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

C. O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável;

D. Os computadores e sistemas da SUDECO devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

E. O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

F. O Suporte Técnico da SUDECO poderá ter permissão de acesso remoto às estações de trabalho dos usuários quando necessário.

5.4 Acesso Remoto Externo

A. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que,

oficialmente, executem atividade vinculada à atuação institucional da SUDECO e que necessitam deste serviço para execução de suas atividades institucionais, desde que autorizados mediante solicitação formal;

B. Os administradores da rede da SUDECO lotados no DTI, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais da SUDECO quando necessário;

C. A liberação de acesso remoto, só será efetivada após avaliação e aprovação pelo DTI, para que se evitem ameaças à integridade e sigilo das informações contidas na rede SUDECO. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança da rede da SUDECO;

5.5. Correio Eletrônico

Diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

A. O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários da SUDECO, independentemente de seu vínculo funcional.

B. O uso do correio eletrônico da SUDECO é para fins corporativos e relacionados às atividades do usuário no âmbito da autarquia.

C. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais da SUDECO;

D. São usuários do serviço de correio eletrônico corporativo os membros e servidores da SUDECO, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional da SUDECO;

5.6. Serviço de Backup

Os procedimentos próprios ao serviço de backup (cópia de segurança) deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. O serviço de backup deve ser automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

B. A solução de backup deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros).

C. A administração das mídias de backup deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade.

D. A execução de rotinas de backup e restore deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

5.7. Data Center

Os procedimentos para administração do centro de processamento de dados (data center) deverão ser fixados em norma própria, considerando as seguintes diretrizes gerais:

A. A administração de dados e de serviços de data center é tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.

B. O acesso físico ao data center deverá ser feito por sistema forte de autenticação, mediante uso de solução de TI própria. O acesso físico por meio de chave apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

C. O acesso ao data center por visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado, que deverá preencher a solicitação de acesso prevista em norma própria, bem como assinar Termo de Responsabilidade.

D. Deverá ser executada, em frequência predeterminada, auditoria dos acessos ao datacenter – por meio de relatório do sistema de registro próprio.

E. A lista de funções com direito de acesso ao data center deverá ser constantemente atualizada, de acordo com os termos de norma própria, salva em diretório de rede. No caso de desligamento de usuários que possuam acesso ao data center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de usuários autorizados.

F. A função de administrador do datacenter – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TI.

5.8. Monitoramento e Auditoria do Ambiente

Para garantir a aplicação das diretrizes mencionadas nesta POSIC, além de fixar normas e procedimentos complementares sobre o tema, a SUDECO poderá:

A. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

B. 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;

C. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

D. Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso.

E. Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

5.9. Utilização da Internet e Intranet

Diretrizes específicas e procedimentos próprios de controles de uso e acesso a Internet deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

A. Todas as regras corporativas sobre uso de Internet e intranet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação da SUDECO deverá sempre ser privilegiada.

B. Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão.

C. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a SUDECO, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores.

D. Em conformidade com a Norma Complementar n° 17/IN01/GSI-PR, é vedada a terceirização completa da administração e da gestão de perfis de órgãos e entidades da APF nas redes sociais, assim entendida a terceirização que viole o disposto no item “B”.

E. Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de 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.

F. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

G. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

H. O DTI deverá prover o serviço de conexão à Internet implementando mecanismos de segurança adequados;

I. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pelo DTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede da SUDECO;

J. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio,

K. É vedado contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas da SUDECO;

L. O usuário poderá solicitar liberação de determinada página, com a devida justificada, mediante solicitação formal ao DTI;

M. Somente serão liberadas as páginas analisadas e autorizadas pelo DTI;

N. A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato ao DTI;

O. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pelo DTI, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

P. A Intranet deverá ser utilizada como mecanismo de divulgação de notícias e disponibilização de serviços de caráter institucional;

Q. O acesso à Intranet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

R. Os navegadores de Internet e Intranet utilizados no âmbito da SUDECO deverão ser homologados pelo DTI;

S. Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados ao DTI para que sejam solucionados.

5.10. Recursos Computacionais

A. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades na SUDECO;

B. A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que seja em um nível mínimo e que não viole a Política, as Normas Complementares e o Código de Ética da Instituição;

C. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade;

D. Os ambientes onde se encontram instalados ou guardados os recursos computacionais devem permanecer protegidos mesmo na ausência dos usuários;

E. É vedado aos usuários da SUDECO utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional;

F. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um Recurso Computacional;

G. Todos os equipamentos (estações de trabalho, notebooks, servidores, impressoras e outros) devem ter identificação padrão especificados pelo DTI.

H. Tendo em vista a preservação do ambiente computacional da SUDECO, é vedado aos usuários o fornecimento de informações a terceiros sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, ressalvada a possibilidade de disposição de tais informações pelo DTI, quando o desempenho de atividades institucionais assim exigir.

5.10.1. Estações de Trabalho

A. É vedado ao usuário abrir as estações de trabalho ou modificar a configuração do hardware;

B. O usuário, sempre que se ausentar da estação de trabalho deve bloqueá-la para impedir o acesso não autorizado;

C. O usuário deve informar imediatamente ao DTI, quando identificada violação da integridade do equipamento por ele utilizado;

D. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho;

E. O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho;

F. Não é permitida a conexão de estações de trabalho particulares, portáteis ou não, à rede da SUDECO, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma, devendo a estação de trabalho ser objeto de verificação de conformidade pelo DTI;

G. Arquivos salvos na unidade de disco local não terão garantia de recuperação.

H. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade do DTI, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de "usuário comum". Ressalva-se o caso de usuários da área técnica, devidamente autorizados, pelo DTI, que por força de suas funções e conhecimento técnico, se reservam ao direito de efetuar suas próprias instalações, bem como, a guarda e o uso oportuno das credenciais de administrador;

I. O compartilhamento de diretórios e arquivos em estações de trabalho somente deve ser realizado quando estritamente necessário para execução das atividades do usuário mediante solicitação formal ao DTI, devidamente justificada.

5.10.2. Equipamentos Portáteis

A. Os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para estações de trabalho;

B. O usuário, ao solicitar o empréstimo de equipamentos portáteis disponíveis na área de patrimônio, deve assinar Termo de Responsabilidade;

C. O usuário deve evitar armazenar informações confidenciais em equipamentos portáteis da SUDECO.

5.10.3. Servidores de rede

A. Todo equipamento servidor de rede deve estar instalado em salas apropriadas e construídas para este fim;

B. Somente os técnicos autorizados do DTI deverão ter acesso aos servidores de rede;

C. O usuário somente terá acesso ao servidor de rede com solicitação formal à TI e devidamente justificada;

5.10.4. Servidores de Arquivo

A. Nos servidores de arquivos locais devem ser gravados:
1) Documentos relacionados ao trabalho cotidiano e à produção jurídica e administrativa local, que demande compartilhamento ou resguardo institucional;
2) Pastas particulares de correio eletrônico, exclusivamente das contas corporativas da unidade.

B. As permissões de acesso deverão ser concedidas em nível de grupos;

C. É proibida a exposição de material de natureza pornográfica e racista, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

D. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas para garantir o backup dos mesmos;

E. Não é permitido criar ou remover arquivos e pastas fora da área alocada ao departamento. Caso esteja em desacordo, o arquivo ou pasta será excluído sem aviso prévio;

F. É vedada a gravação de dados e informações de natureza particular;

G. Identificada ocorrência em desacordo com o disposto nos itens antecedentes, o DTI poderá, após notificar o responsável e resguardar as evidências necessárias, excluir ou isolar arquivos, revogar acessos ou requisitar o equipamento, relatando o fato imediatamente à autoridade responsável pela apuração da infração;

5.10.4. Ativos de Rede

A. As portas dos switches somente devem estar ativas se utilizadas e inventariadas;

B. Os switches e access points devem possuir controle de acesso;

C. Todo roteador utilizado na rede da SUDECO deve prover, no mínimo, o uso de ACLs (Access lists) e o filtro de pacotes;

D. Todo ativo de rede deve estar em local seguro. Os switches departamentais devem estar instalados em racks devidamente fechados e seguros;

E. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado;

F. As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pelo DTI;

G. À SUDECO reserva o direito de realizar investigações em qualquer dos equipamentos que integrem a sua rede local.

5.10.5. Rede Sem Fio

A. A utilização da rede sem fio para acesso à rede da SUDECO somente será efetuada com autenticação utilizando mecanismos de protocolo seguro;

B. Qualquer equipamento que utilize a rede sem fio da SUDECO deve respeitar as regras estabelecidas para Estações de Trabalho e Notebooks, inclusive, quando justificados, os equipamentos particulares;

C. Somente os técnicos autorizados do DTI devem estabelecer os procedimentos e configurações de segurança de rede sem fio;

D. O acesso à rede wi-fi pelos agentes públicos da SUDECO será feito mediante preenchimento de cadastro, apenas no primeiro acesso;

E. Os visitantes da SUDECO terão acesso por meio de senha gerada diariamente.

5.10.6. Impressoras

A. Somente os usuários previamente autorizados poderão ter acesso aos recursos de impressão;

B. A configuração da impressora na estação de trabalho do usuário somente deverá ser realizada pelos técnicos autorizados pelo DTI;

C. Os usuários não devem deixar informações críticas, sigilosas ou sensíveis da instituição em equipamentos de impressão, de tal forma que pessoas não autorizadas possam obter acesso a elas.

5.10.7. Utilização de Software

A. Na SUDECO, só será permitida a utilização de softwares homologados pelo DTI, respeitando os direitos autorais e contratuais dos fabricantes, e que sejam necessários para a execução das atividades dos usuários;

B. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pelo DTI;

C. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação da SUDECO e o suporte para o mesmo;

D. A instalação e a utilização de software estão sujeitas ao cumprimento dos seguintes requisitos:

1) Quantidades de licenças de uso adquiridos;
2) Conformidade com a área de atuação do setor interessado;
3) Compatibilidade com os softwares utilizados;
4) Desempenho do ambiente computacional; e
5) Impacto entre a necessidade de instalação e a demanda de outros setores.

E. É vedado efetuar réplicas dos softwares adquiridos pela SUDECO, bem como promover esta prática com outros programas;

F. É vedado utilizar softwares que, por algum motivo, descaracterizem os propósitos da instituição ou danifique de alguma forma o ambiente instalado, tais como jogos eletrônicos e outros.

G. A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida ao DTI;

H. O DTI poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma;

5.10.8. Manutenção e Configuração

A. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante abertura de chamado à DTI;

B. Nas dependências físicas da SUDECO somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares;

C. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração, deverá estar devidamente identificado;

D. O usuário deve estar ciente da saída do equipamento de seu local de trabalho caso seja necessária a retirada do mesmo para manutenção;

E. A saída do equipamento deverá ser autorizada pela área de patrimônio;

F. O usuário deve manter o número, do registro do chamado ou número do documento de solicitação formal, do pedido de suporte por ele realizado para controle e acompanhamento do respectivo chamado.

5.10.9. Controle e Administração de Recursos Computacionais

A. Todo recurso computacional deve ser identificado e inventariado;

B. O DTI deve garantir a qualidade e disponibilidade dos serviços, identificando e informando a necessidade de aquisição de novos recursos de informática;

C. Novas implementações, aquisições, alterações e atualizações de recursos computacionais (incluindo hardware ou software) devem ser homologadas antecipadamente pelo DTI através do preenchimento do documento de oficialização de demanda (DOD);

D. Os recursos computacionais devem ser monitorados e administrados pelo DTI;

5.10.10. Telefonia Fixa

A. A SUDECO utiliza a tecnologia VOIP (Voice over Internet Protocol - voz sobre IP) que permite a transmissão de voz por Protocolo de Internet (IP) transformando sinais de áudio analógicos em digitais e podem ser transferidos através da internet.

B. Os equipamentos de telefonia fixa, móvel e de internet móvel (modens) são destinados ao uso exclusivo de assuntos de interesse da instituição.

C. Cada usuário terá um ramal próprio podendo ser por meio de telefone IP ou via softphone com uso do headset.

5.11. Gestão de Riscos

Nos termos da Norma Complementar 04/IN01/DSIC/GSIPR, a Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos".

As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações da SUDECO deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação e Comunicação. Esse processo deverá ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação, contemplando inclusive as contratações de soluções de TI – para as quais deverá ser elaborado um Plano de Tratamento de Riscos.

5.12. Gestão de Continuidade

Nos termos da Norma Complementar 06/IN01/DSIC/GSIPR, "a implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação".

O órgão deverá elaborar e manter Programa de Gestão de Continuidade de Negócios, aqui entendido como o "processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção".

O Programa de Gestão de Continuidade de Negócios da SUDECO deverá ser composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

A. **Plano de Gerenciamento de Incidentes (PGI):** plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes.

B. **Plano de Continuidade de Negócios (PCN):** documentação dos procedimentos e informações necessárias para que a SUDECO mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em casos de incidentes.

C. **Plano de Recuperação de Negócios (PRC):** documentação dos procedimentos e informações necessárias para que a SUDECO operacionalize o retorno das atividades críticas à normalidade.

Os planos acima definidos deverão ser testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Para subsidiar a elaboração de seu Programa de Gestão de Continuidade de Negócios, a SUDECO deverá definir quais são suas atividades críticas, ou seja, quais são as atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios deverão ser executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, incluindo as pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicações.

5.13. Tratamento de Incidentes em Redes Computacionais

Nos termos da Norma Complementar 05/IN01/DSIC/GSIPR, "Tratamento de Incidentes de Segurança em Redes Computacionais é o serviço 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".

A ocorrência de incidentes de segurança em redes de computadores da SUDECO deverá ser comunicada ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.Gov), conforme procedimentos a serem definidos pelo próprio centro, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

No tratamento de incidentes em redes computacionais, o CGSIC, responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

A. Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

B. O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

C. Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros da CGSIC tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da SUDECO.

6. PENALIDADES

A SUDECO, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais a SUDECO responderá com a aplicação de todas as medidas administrativas, cíveis e judiciais cabíveis.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SUDECO e/ou terceiros. Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

7. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Os documentos que comporão a estrutura normativa de gestão de segurança da informação serão divididos em três categorias:

A. **Política – nível estratégico:** constituída do presente documento, define as regras de alto nível que representam os princípios básicos que a SUDECO decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.
B. **Normas – nível tático:** especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política.
C. **Procedimentos – nível operacional:** instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades da SUDECO.

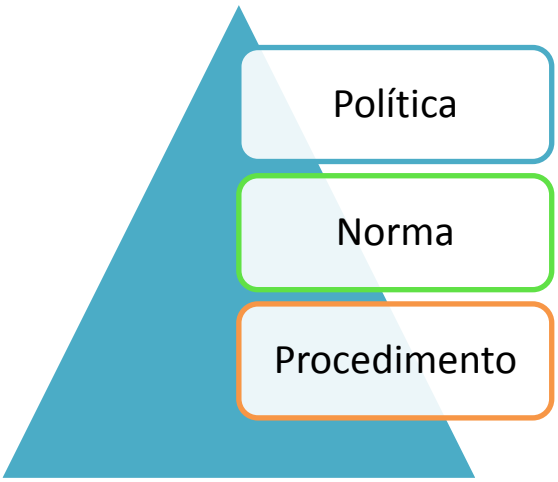

Figura 1: Estrutura normativa de Gestão de Segurança da Informação.

7.1. Divulgação e acesso à estrutura normativa

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os agentes públicos e prestadores de serviços da SUDECO e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para efetiva aplicação da POSIC será disponibilizado Termo de Responsabilidade (Anexo I).

7.2. Aprovação e revisão

Os documentos integrantes da estrutura normativa de gestão de segurança da informação da SUDECO deverão ser aprovados em Reunião Colegiada e revisado pelo CGSIC.

A política de segurança, as normas e os procedimentos complementares serão revisados periodicamente segundo os prazos estabelecidos pelo Comitê Gestor de Segurança da Informação. Sempre que algum fato relevante ou evento motive, os prazos revisionais estabelecidos poderão ser antecipados – conforme análise e decisão do Comitê Gestor de Segurança da Informação.

8. REFERÊNCIAS LEGAIS E NORMATIVAS

CLASSIFICAÇÃO	IDENTIFICAÇÃO	DATA PUBLICAÇÃO	ASSUNTO
Lei Federal	8.159/1991	08/01/1991	Dispõe sobre a política nacional de arquivos públicos e privados.
Lei Federal	9.610/1998	19/02/1998	Dispõe sobre o direito autoral
Lei Federal	9.279/1996	14/05/1996	Dispõe sobre marcas e patentes
Lei Federal	10.406/2002	10/01/2002	Institui o Código Civil brasileiro
Decreto Lei	2.848/1940	07/12/1940	Institui o Código Penal brasileiro
Decreto	3.505/2000	13/06/2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto	7.845/2012	14/11/2012	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
Instrução Normativa	IN GSI/PR 01/2008	13/06/2008	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Norma Complementar	03/IN01/DSIC/GSIPR	30/06/2009	Diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
Instrução Normativa	IN SLTI/MP 04/2010	12/11/2010	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do SISP do Poder Executivo Federal.
Portaria	Portaria SUDECO nº 28	27/01/2015	Institui o Comitê Gestor de Segurança – CGSIC da Superintendência do Desenvolvimento do Centro-Oeste.

9. CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, considera-se:

Acesso Lógico: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação.

Acesso Remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário.

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função.

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização.

Ativo da Informação: os meios de armazenamento, transmissão e processamento, os sistemas e informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Ativo Sigiloso: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização.

Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes.

Autenticação: é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira.

Autenticidade (autoria): propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade, dotados de competência para tal.

Banco de Dados (ou Base de Dados): é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações.

Biometria: uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão.

Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso.

Bluetooth: tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos.

Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

Contingência: descrição de medidas a serem tomadas por uma organização, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação.

Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes.

Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

Criptografia: é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta").

CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.

Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador.

Data Center: é um ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (storages) e ativos de rede (switches, roteadores). O objetivo principal de um Data Center é garantir a disponibilidade de equipamentos que ofereçam serviços essenciais para o negócio da organização.

Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

DOD: Documento de Oficialização da Demanda. Este documento subsidia as informações necessárias para os processos de compra e distribuição de software e Hardware. É imprescindível o seu preenchimento pelas áreas que demandam a contratação de uma solução de TI.

Download (Baixar): copiar arquivos de um servidor (site) na internet para um computador pessoal.

Espelhamento: Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.

Gestão de Continuidade de Negócios: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia.

Gestão de Risco: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestor da Informação: pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades.

Gestor de Pessoas e Processos: aquele responsável pela liderança de um grupo de pessoas ou processos.

Gestor de Segurança da Informação e das Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Hardware: É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros.

Headset: É um equipamento formado por um fone de ouvido e um microfone acoplado com controle de volume para uso em microcomputadores.

HTTP (Hyper Text Transfer Protocol): (Protocolo de Transferência de Hipertexto) é uma linguagem para troca de informação entre servidores e clientes da rede.

HTTPS (HyperText Transfer Protocol Secure): (Protocolo de Transferência de Hipertexto Seguro) é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade.

Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informações Críticas: são as informações de extrema importância para a sobrevivência da instituição.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Instant Messenger (Mensageiro instantâneo): é uma aplicação que permite o envio e o recebimento de mensagens em tempo real.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Internet: rede mundial de computadores.

Internet Protocol (IP): é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados.

Intranet: rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito.

Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Logon: Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível.

Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

Plano de Contingência: Descrever as medidas a serem tomadas por uma organização, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada.

Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

Política de Segurança da Informação e das Comunicações (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede.

Proxy: é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas.

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Recursos Computacionais: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura.

Rede Corporativa: conjunto de todas as redes locais sob a gestão da instituição.

Replicação: é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento.

Roteador: equipamento responsável pela troca de informações entre redes.

Sala Segura: sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente.

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos.

Sistemas de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção.

Sistema de Segurança da Informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

Softphone: É um aplicativo multimídia que transforma o computador em um telefone multimídia, com capacidade de voz, dados e imagem. É possível fazer chamadas diretamente do computador através da Internet.

Software: são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros.

Streaming: transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet.

Switches: Um switch de rede é um equipamento eletrônico de comutação, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados.

Telefones IP: Aparelhos específicos que se conectam diretamente à rede de computadores recebendo voz, dados e imagens.

Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Tratamento de Incidentes de Segurança em Redes Computacionais: serviço 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.

Trilhas de Auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários.

Usuário: colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.

VLAN (Virtual Local Area Network ou Virtual LAN): (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local.

VPN (Virtual Private Network): (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Wireless (rede sem fio): rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

VOIP: (**Voice over Internet Protocol) Voz sobre IP** - corresponde à possibilidade de efetuar chamadas de voz e ou de vídeo através da Internet**.** Esta tecnologia consiste na conversão de um sinal de voz analógico num conjunto de sinais digitais, que posteriormente são enviados através da Internet.

10. DISPOSIÇÕES FINAIS

Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço da SUDECO – a fim de que seja cumprida dentro e fora da autarquia.

O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

11. IDENTIFICAÇÃO E APROVAÇÃO DAS UNIDADES RESPONSÁVEIS

Cleber Ávila
Superintendente

José Augusto Scalea
Diretor Administrativo

Carlos Gardel Ribeiro
Diretor de Planejamento e Avaliação

Everaldo Fernandes Benevides
Diretor de Implementação de Programas e Gestão de Fundos

ANEXO I

TERMO DE RESPONSABILDADE

IDENTIFICAÇÃO	
Nome:	
Documento: **( )SIAPE ( )CPF**	
Cargo:	
Departamento:	
Ramal:	
Email:	

TERMOS
O Agente Público acima qualificado declara ter pleno conhecimento de suas responsabilidades no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito da SUDECO, bem como sobre todas as informações que eventualmente ou por força de suas funções venham a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas da POSIC vigentes no ambiente desta superintendência ou que venham a ser implantadas a qualquer tempo por esta POSIC.
DE ACORDO
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE RESPONSABILIDADE é assinado pela parte declarante em 02 (duas) vias de igual teor e um só efeito.

IDENTIFICAÇÃO E ASSINATURA DO DECLARANTE
_____ Nome Cargo

ANEXO II

TERMO DE COMPROMISSO

A **Superintendência do Desenvolvimento do Centro-Oeste** - SUDECO, sediada no **Setor Bancário Norte**, **Quadra 01, Bloco F, 19º andar Ed. Palácio da Agricultura, Brasília/DF**, **CNPJ n.° 13.802.028/0001-94**, doravante denominado CONTRATANTE, e, de outro lado, ***<CONTRATADA>***, sediada no ***<ENDEREÇO>*****, CNPJ n.° *XXX***, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º *XXX* doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta - DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I - sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II - tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III - sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I –A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I –Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e

outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições

constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro de BRASÍLIA/DF, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Brasília, __ de _____ de 20xx..

DE ACORDO	
CONTRATANTE	**CONTRATADA**
_____ Nome Cargo **Matrícula:**	_____ Nome Cargo **CPF:**
Testemunha 1	**Testemunha 2**
_____ Nome Cargo **Matrícula:**	_____ Nome Cargo **CPF:**

SUDECO
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO CENTRO-OESTE