SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA CULTURA
INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DISPÕE ACERCA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL.

PSI

Brasília/DF, outubro de 2013.

IPHAN Instituto do Patrimônio Histórico e Artístico Nacional
Ministério da Cultura
GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Política de Segurança da Informação do IPHAN

Ministério da Cultura

Instituto do Patrimônio Histórico e Artístico Nacional

Jurema de Sousa Machado

Presidente

Comitê Gestor de Tecnologia da Informação

Marcos José Silva Rego

Presidente do COGESTI

Coordenação Geral de Tecnologia da Informação

Carlos Augusto Pessoa Machado

Coordenador Geral de Tecnologia da Informação

Equipe de Elaboração

Delson Pereira da Silva

Analista em TI

Equipe de Revisão

Carlos Augusto Pessoa Machado

Coordenador Geral de Tecnologia da Informação

Sérgio Porto Carneiro

Chefe de Divisão de Infraestrutura Tecnológica

Outubro de 2013

Brasília | DF

SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

1. INTRODUÇÃO.

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição. A *Política de Segurança da Informação* (PSI), por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.

"Política de Segurança da Informação e Comunicações: 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.

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; deverão ser observados por todos servidores, colaboradores, fornecedores e prestadores de serviço e se aplicam à informação em qualquer meio ou suporte.

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* do IPHAN:

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* do IPHAN:

A. Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao IPHAN. As exceções devem ser explícitas e formalizadas entre as partes.

B. Todos os recursos de informação do IPHAN 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. Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de *login* de acesso único, pessoal e intransferível.

F. O IPHAN 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.

G. Cada usuário é responsável pela segurança das informações dentro do IPHAN, principalmente daquelas que estão sob sua responsabilidade.

H. 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.

I. 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.

J. A gestão da segurança da informação no IPHAN será realizada por comitê multidisciplinar, ora designado *Comitê de Segurança da Informação.*

K. Deverá constar em todos os contratos do IPHAN, 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 no IPHAN,

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[1].

L. Esta *Política de Segurança da Informação* será implementada no IPHAN 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. Papéis e Responsabilidades.

4.1 Papéis.

Tabela 1: Descrição de papéis em Segurança da Informação.

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	Servidores públicos, servidores sem vínculo, demais funcionários e colaboradores internos.	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do IPHAN.
USUÁRIO EXTERNO	Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pela IPHAN e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
GESTORES	Coordenadores, Coordenadores Gerais, Diretores, Superintendentes e demais cargos de chefia.	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TI	Coordenação Geral de Tecnologia da Informação (CGTI)	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.
GESTOR DE SI	Gerência técnica	Servidor responsável pela gestão da segurança da informação em todos os seus aspectos.
EQUIPE TÉCNICA DE SI	Equipe técnica de SI	Equipe técnica responsável por implementar e administrar as soluções de segurança da informação.
COMITÊ DE SI	Alta Administração	Comitê Temático, vinculado ao Comitê Gestor de TI, responsável pelas decisões de alto nível relacionadas à gestão da 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 do IPHAN:

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 do IPHAN.

D. Manter-se atualizado em relação a esta PSI e às normas e procedimentos relacionados, buscando

[1] Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no IPHAN estão presentes no ENCARTE I e ENCARTE II.

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 ao IPHAN 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. O IPHAN 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 executivos do IPHAN 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 do IPHAN, 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 o IPHAN.

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. Informar previamente o Gestor de SI sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante.

J. 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.

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

L. 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).

M. 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.

N. Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do IPHAN 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).

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

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

Q. Responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos[2].

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

S. 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.

T. 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* 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 do IPHAN**:

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

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 de Segurança da Informação* e a Equipe Técnica de Segurança da Informação (ETSI).

[2] O uso, manuseio e guarda de assinaturas de certificados digitais individuais é de responsabilidade de seus respectivos portadores.

E. Realizar 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 Equipe Técnica de Segurança da Informação.

É de responsabilidade específica da **Equipe Técnica 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 do IPHAN.

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

D. Promover a conscientização dos usuários em relação à relevância da segurança da informação para o IPHAN, 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 em conjunto com o *Comitê de Segurança da Informação*.

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

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

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

Também será atribuição da *Equipe de Segurança da Informação* atuar, quando necessário, com atribuições de ***Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais*** (ETIR) da qual trata a *Norma Complementar 05 IN01/DASIC/GSIPR*.

4.3.6 Comitê de Segurança da Informação.

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

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 do IPHAN, 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 do IPHAN nos decisões relativas à segurança da informação.

O *Comitê de Segurança da Informação* deverá ser formalmente instituído pelo **Comitê Gestor de Tecnologia da Informação do IPHAN**, como **Comitê Temático** (segundo art. 4°, inc. I da Portaria IPHAN

nº 235, de 20/07/2010) e integrado por gestores com nível hierárquico gerencial – nomeados **formalmente** para participar do grupo. Sua composição deve incluir um membro de cada uma das seguintes áreas: Presidência, Auditoria Interna, Procuradoria Federal, Departamento de Planejamento e Administração, Departamento de Patrimônio Material e Fiscalização, Departamento de Patrimônio Imaterial e Departamento de Articulação e Fomento.

O *Comitê de Segurança da Informação* deverá reunir-se ordinariamente em periodicidade a ser instituída por portaria específica, mas encontros adicionais poderão ser realizados sempre que for necessário deliberar sobre algum incidente grave ou realizar deliberação relevante.

Caberá, ainda, ao *Comitê de Segurança da Informação* propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos; avaliar os incidentes de segurança e propor ações corretivas; definir as medidas cabíveis nos casos de descumprimento da *Política de Segurança da Informação* e/ou das normas de segurança da informação complementares.

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. 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.

B. Arquivos pessoais e/ou não pertinentes às atividades institucionais do IPHAN (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.

C. 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.

5.2 Controles de Acesso.

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 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 do IPHAN.

B. A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

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.

5.3 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 do IPHAN, independentemente de seu vínculo funcional.

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

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

E. As mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres.

F. Os *backups* críticos para o bom funcionamento dos serviços do IPHAN exigem uma regra de retenção especial, a ser prevista nos procedimentos específicos e de acordo com as normas de classificação da informação pública, seguindo ainda as determinações fiscais e legais existentes no país.

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

5.5 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

na 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 d*ata 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 d*atacenter* – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a *servidor público efetivo,* preferencialmente vinculado à área de infraestrutura de TI.

5.6 Monitoramento e Auditoria do Ambiente.

Para garantir a aplicação das diretrizes mencionadas nesta PSI, além de fixar normas e procedimentos complementares sobre o tema, o IPHAN **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 nas 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.

5.7 Uso e acesso a *internet*.

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* 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 do IPHAN deverá sempre ser privilegiada.

B. Perfis institucionais mantidos nas *redes sociais*[3] 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, o IPHAN, 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

[3] Estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

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 a assegurar o cumprimento de sua *Política de Segurança da Informação*.

5.8 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* do IPHAN 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*. 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*.

5.9 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* do IPHAN 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 o IPHAN 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 o IPHAN 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, o IPHAN 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.

5.10 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 do IPHAN 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, a *Equipe Técnica de Segurança da Informação*, 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 Equipe Técnica de Segurança da Informação 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 do IPHAN.

6. PENALIDADES.

O IPHAN, 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 o IPHAN 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 o IPHAN 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 o IPHAN 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 do IPHAN.

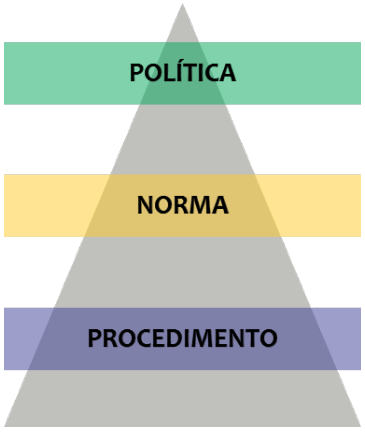


Figura 1: Estrutura normativa de Gestão de Segurança da Informação.

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 servidores, colaboradores, estagiários, aprendizes e prestadores de serviços do IPHAN quando de sua admissão, e também publicadas na *Intranet corporativa*, de maneira que seu conteúdo possa ser consultado a qualquer momento.

7.2 Aprovação e revisão.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação do IPHAN deverão ser aprovados segundo as seguintes instâncias:

Tabela 2: Responsáveis pela aprovação e revisão da estrutura normativa de Segurança da Informação.

CATEGORIA	NÍVEL DE APROVAÇÃO
POLÍTICA	Comitê Gestor de Tecnologia da Informação
NORMA COMPLEMENTAR	Comitê de Segurança da Informação
PROCEDIMENTO	Coordenação Geral de Tecnologia da Informação

A política de seguranças, as normas e os procedimentos complementares serão revisados

periodicamente segundo os prazos estabelecidos pelo *Comitê 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 de Segurança da Informação*.

8. Referências Legais e Normativas.

Tabela 3: 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 IPHAN	235/2010	20/07/2010	Institui o Comitê Gestor de Tecnologia da Informação do IPHAN - COGESTI - com a finalidade de deliberar sobre o planejamento, orçamentação, investimentos, priorização e gerenciamento de riscos de toda a Política de Tecnologia da Informação do IPHAN.
Portaria IPHAN	92/2012	05/07/2012	Aprova o Regimento Interno do Instituto do Patrimônio Histórico e Artístico Nacional.

9. 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 do IPHAN – 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.

10. Identificação e aprovação das unidades responsáveis.

COORDENAÇÃO GERAL DE TECNOLOGIA DA INFORMAÇÃO	DATA
ASSINATURA CARLOS AUGUSTO PESSOA MACHADO Coordenador Geral de Tecnologia da Informação	

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO	DATA
ASSINATURA(S) MARCOS JOSÉ SILVA RÊGO Presidente do Comitê Gestor de Tecnologia da Informação	

ENCARTE I. Termo de Compromisso de Confidencialidade e Segurança da Informação.

IPHAN

TERMO DE COMPROMISSO
CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO CONTRATO:

N° do Contrato	**Digite n° do Contrato**
Nome da Empresa Contratada	**Digite Nome da Contratada**
CNPJ da Contratada	**Informe objeto CNPJ**
Objeto resumido	**Informe objeto resumido**
Vigência Contratual	**Informe vigência**

TERMOS:

O <Contratante>, sediado em <Endereço Contratante>, CNPJ n.º <CNPJ Contratante>, doravante denominado **CONTRATANTE**, e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ n.º <CNPJ Contratada>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do CONTRATO N.º <n° contrato / ano> 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 DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES**, 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 - segundo o Decreto n° 7.845/2012, de 14/11/2012, que 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.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

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

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. 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, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, 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.

§1° – Comprometem-se as partes 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.

§2° – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente

envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;

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 Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§1° – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2° – 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 DE COMPROMISSO bem como da natureza sigilosa das informações.

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

§3° – 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.

§4° – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO DE COMPROMISSO.

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

§5° – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, 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.

§6° – 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 Proprietárias 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 Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO 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 Sexta – 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 legislação em vigor que trata desse assunto, podendo 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 Sétima – DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.

§1° – 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.

§2° – O disposto no presente TERMO DE COMPROMISSO 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, tais 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 DE COMPROMISSO 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 DE COMPROMISSO, 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 ao CONTRATO PRINCIPAL;

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

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da cidade de CIDADE (UF), 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.

OBSERVAÇÕES:

Digite observações, se houver.

DE ACORDO:

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

CONTRATANTE	**CONTRATADA**
Local, dia/mês/ano. **ASSINATURA**	**Local, dia/mês/ano.** **ASSINATURA**
Nome do Responsável pelo Contratante Cargo / Matrícula Coordenação / Departamento	Nome do Responsável pela Contratada Cargo / CPF Identificação da contratada

ENCARTE II. Termo de Ciência Individual de Confidencialidade e Segurança da Informação.

IPHAN	TERMO DE CIÊNCIA INDIVIDUAL CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO CONTRATO	
N° do Contrato:	
Empresa Contratada:	
CNPJ:	
Objeto Resumido:	
Vigência Contratual:	

TERMOS

O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo n° / , bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.

OBSERVAÇÕES

Digite observações, se houver.

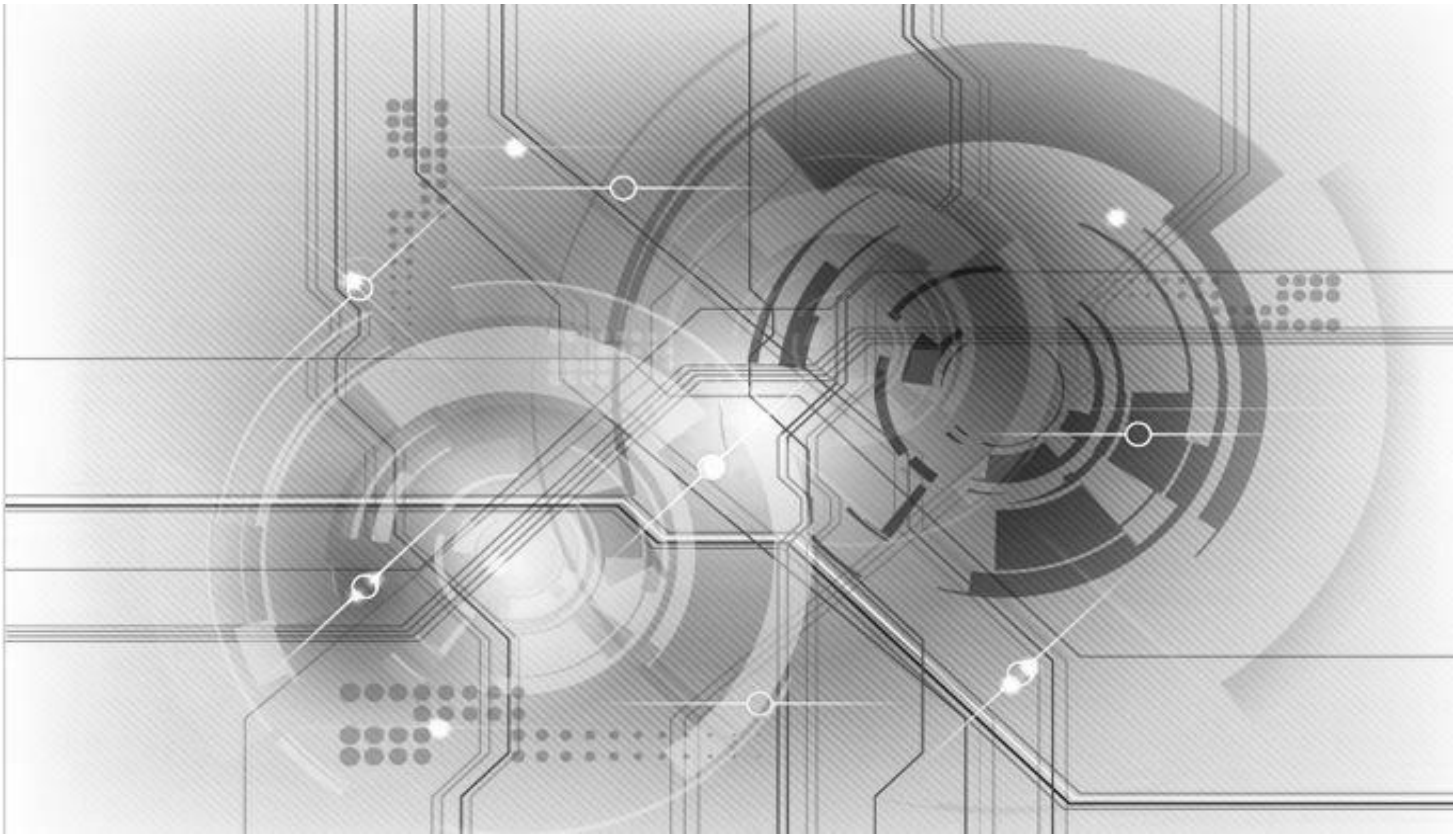
DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pela(s) parte(s) declarante(s) em 02 (duas) vias de igual teor e um só efeito.

Local, dia/mês/ano.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome: Identidade: CPF: Função:	Assinatura:
Nome: Identidade: CPF: Função:	Assinatura:
Nome: Identidade: CPF: Função:	Assinatura:
Nome: Identidade: CPF: Função:	Assinatura:



SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA CULTURA
INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL
DEPARTAMENTO DE PLANEJAMENTO E ADMINISTRAÇÃO
EDIFÍCIO IPHAN | SEPS 713/913 ASA SUL |BLOCO D – 1° ANDAR | BRASÍLIA – DF | CEP 70.390-135 | www.iphan.gov.br