Instituto do Patrimônio Histórico e Artístico Nacional
Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação
Subcomitê de Segurança da Informação e Comunicação

POSIC

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Brasília, março de 2018.

Serviço Público Federal

Ministério da Cultura

Instituto do Patrimônio Histórico e Artístico Nacional

Presidente

Kátia Santos Bogéa

Chefe de Gabinete

Rafael Arrelaro

Departamento de Planejamento e Administração

Marcos José Silva Rêgo

Departamento de Patrimônio Material e Fiscalização

Andrey Rosenthal Schlee

Departamento de Patrimônio Imaterial

Hermano Fabrício Oliveira Guanais e Queiroz

Departamento de Cooperação e Fomento

Marcelo Brito

Departamento de Projetos Especiais

Robson Antônio de Almeida

COMITÊ GESTOR DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Marcos José Silva Rêgo
Presidente do COGESTI

SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Darlan Henrique da Silva Venturelli
Coordenador Geral de Tecnologia da Informação
Departamento de Planejamento e Administração

William de Castro Feitosa
Coordenador Geral de Logística, Convênios e Contratos
Departamento de Planejamento e Administração

Aleksandra Pereira dos Santos
Coordenadora Geral de Gestão de Pessoas
Departamento de Planejamento e Administração

Jurema Kopke Eis Arnaut
Coordenadora Geral de Pesquisa e Documentação
Departamento de Cooperação e Fomento

EQUIPE TÉCNICA DE ELABORAÇÃO E REVISÃO

Delson Pereira da Silva
Coordenador Técnico de Governança e Projetos de TI

Sérgio Porto Carneiro
Chefe de Divisão de Infraestrutura Tecnológica

Bruno Filgueiras Soares
Chefe de Divisão de Sistemas de Informação

Adriano Campos Ávila
Analista em Tecnologia da Informação

Alexandre Olimpio Barbacena
Analista em Ciência e Tecnologia

Ana Cristina França de Queiroz Cavalcanti Lima
Analista I

Humberto Mattos Carvalho
Analista em Tecnologia da Informação

Jane Adriana de Souza
Analista em Tecnologia da Informação

ÍNDICE

1 Apresentação

Segurança da Informação e Comunicação (SIC) é a disciplina dedicada à proteção das informações de forma a manutenção de seus atributos e a proteção contra danos que possam comprometer a organização ou gerar perdas. Por sua vez, a **Política de Segurança da Informação e Comunicações** (POSIC) é o documento formal que estabelece diretrizes corporativas e orientações para a proteção dos ativos de informação e a gestão da segurança da informação e comunicações:

"Política de Segurança da Informação e Comunicações: documento aprovado pelo órgão ou entidade da Administração Pública Federal, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo 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]

No âmbito governamental a PoSIC contempla as recomendações e práticas propostas pelo Decreto nº 3.505/2000, pela Instrução Normativa nº 01/2008/ GSI/PR e à norma internacional ABNT ISO/IEC 27002/2005. Dessa forma, considerando o disposto no art. 3° do Decreto n° 3.505/2000, são **objetivos genéricos** da Política de Segurança da Informação e Comunicações (POSIC) para a Administração Pública Federal a serem estabelecidos por todos os órgãos e entidades públicas:

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 e Comunicações;

d) Estabelecer normas jurídicas necessárias à efetiva implementação da Segurança da Informação e Comunicações;

e) Promover as ações necessárias à implementação e manutenção da Segurança da Informação e Comunicações;

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 e Comunicações;

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 Comunicações; e

h) Assegurar a interoperabilidade entre os sistemas de Segurança da Informação e Comunicações.

No âmbito desta **POSIC** considera-se:

a) Gestão de segurança da informação e comunicações: processo abrangente de gestão que desenvolve ações e métodos que visam a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, táticos e operacionais, não se limitando ao âmbito da tecnologia da informação e comunicações.

b) Ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os processos de negócio, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

c) Gestão de ativos de informação: processo abrangente de gestão que inventaria e mapeia os ativos de informação institucionais, identificando, no mínimo e de forma inequívoca, seu conjunto completo de informações básicas (nome, descrição e localização), seus respectivos responsáveis (proprietários e custodiantes), seus requisitos legais e de negócio, sua classificação, sua documentação, seu ciclo de vida, seus riscos associados e seus controles de SIC implementados, bem como os outros ativos de informação relacionados;

d) Gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso essas ameaças se concretizem, de forma a fornecer uma estrutura para que se desenvolva uma resiliência organizacional capaz de recuperar perdas de ativos de informação a um nível aceitável pré-estabelecido, por intermédio de ações de prevenção, resposta e recuperação, de forma a salvaguardar os interesses das áreas envolvidas, a reputação, a marca da organização e suas atividades de valor agregado.

2 Dos objetivos e da abrangência

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 e Comunicações 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 e Comunicações.

c) Apoiar a implantação das iniciativas relativas à Segurança da Informação e Comunicações.

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.

Esta PoSIC e suas eventuais normas complementares aplicam-se em **toda a organização**, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação do Iphan em qualquer meio ou suporte.

Os princípios e diretrizes gerais desta PoSIC também se aplicam às entidades vinculadas ao Iphan e a quaisquer relacionamentos com outros órgãos e entidades públicos ou privados.

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.

Esta Política de Segurança da Informação e Comunicações será implementada no IPHAN por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do tipo de vínculo, nível hierárquico ou função.

3 Dos princípios

São **princípios** da Política de Segurança da Informação e Comunicações do IPHAN:

a) Todas as informações produzidas ou recebidas pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado do exercício de sua função e/ou atividade profissional contratada pertence ao IPHAN; as exceções devem ser formalizadas explicitamente entre as partes.

b) Todos os ativos de informação do IPHAN, inclusive os recursos comunicacionais e computacionais, devem ser utilizados que forma responsável, consciente e aplicados na consecução dos objetivos institucionais da instituição.

c) Com vistas ao melhor gerenciamento dos riscos associados aos ativos de informação, deverão ser criados e mantidos controles, registros de atividades e trilhas de auditoria para todos os processos e/ou sistemas que a instituição julgar necessário de modo que todos os eventos significantes dos processos e sistemas sejam rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo acontecimento.

d) Os sistemas, recursos e aplicações informacionais e comunicacionais do Iphan serão utilizados mediante controle de acessos gerenciados e monitorados com apoio de ferramentas tecnológicas adequadas e mediante processos suficientemente definidos com vistas a assegurar a devida proteção dos ativos de informação e da infraestrutura computacional da instituição. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

e) Cada usuário é individualmente responsável pela segurança das informações dentro da organização, principalmente daquelas que estejam sob sua guarda ou responsabilidade.

f) 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, serão implantados e gerenciados planos de contingência e de continuidade para os principais serviços e sistemas – tais planos serão ser implantados, revisados e testados periodicamente.

g) Todos os requisitos associados à segurança da informação e comunicações deverão ser identificados prioritariamente na fase de levantamento do escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

h) Segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.

i) Quando o objeto for pertinente, deverá constar em todos os contratos celebrados pelo órgão cláusula de confidencialidade e de obediência às normas internas de Segurança da Informação e Comunicações a ser observada pelas empresas fornecedoras e por todos os profissionais que vierem a desempenhar atividades profissionais no âmbito dos respectivos contratos, inclusive aqueles firmados junto a organismos internacionais.

4 Papéis e responsabilidades em SIC

4.1 Papéis

Tabela 1: Descrição de papéis em Segurança da Informação e Comunicações.

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 TIC	Coordenação Geral de Tecnologia da Informação (CGTI)	Unidade organizacional responsável pela gestão e operação dos recursos de TIC na organização e custodiante da informação.
GESTOR DE SIC	Gerência técnica	Responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
ETIR	Equipe técnica	Grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores.
SUBCOMITÊ DE SIC	Alta Administração	Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

4.2 Responsabilidades gerais

São **responsabilidades gerais** e comuns a todos os usuários e gestores de serviços de rede de dados, *internet*, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação do IPHAN:

a) Zelar pela 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 corporativos de informação e comunicação – utilizando-os sempre de forma ética, legal e consciente.

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

4.3 Responsabilidades específicas

4.3.1 Usuários internos e externos

Todo prejuízo ou dano decorrente da não obediência às diretrizes e normas referenciadas nesta *Política de Segurança da Informação e Comunicações* e nas normas e procedimentos específicos dela decorrentes é de inteira responsabilidade do usuário (interno e/ou externo) que o der causa.

Os **usuários externos** devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos vigentes de segurança da informação e comunicações. O IPHAN poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento desta POSIC ou das normas complementares e procedimentos específicos dela decorrentes.

O desconhecimento das regras contidas nesta POSIC é **inescusável**, ou seja, a alegação de seu desconhecimento não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.

4.3.2 Gestores de pessoas e processos

Os gestores executivos do IPHAN devem manter postura exemplar em relação à segurança da informação e comunicações, 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 e Comunicações do IPHAN, tomando as ações necessárias para cumprir tal responsabilidade.

4.3.3 Área de Tecnologia da Informação e Comunicação

Quanto à gestão de segurança da informação e comunicações, serão responsabilidades específicas da área de **Tecnologia da Informação e Comunicação**:

a) Zelar pela eficácia dos controles de SIC utilizados e informar aos gestores e demais interessados os riscos residuais.

b) Negociar e acordar com os gestores níveis de serviço relacionados a SIC, 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 e Comunicações.

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 SIC 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 TIC, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

k) Gerir a capacidade de armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos.

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[1].

m) Proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos.

n) Zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais do IPHAN durante sua operação ou durante eventos de mudança de ambiente (de desenvolvimento para teste, homologação ou produção, por exemplo)[2].

o) Definir regras para instalação de *softwares* e *hardwares* no ambiente corporativo e demais ambientes vinculados, incluindo aqueles dedicados ao uso pelo público externo[3].

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[4].

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 de trabalho 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 TIC, 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).

---

[1] A responsabilidade pela gestão de usuários externos é atribuição do gestor do contrato ao qual estejam vinculados ou do gestor da unidade/setor em que o usuário externo esteja alocado.

[2] Sempre que houver necessidade de concessão de acessos à terceiros nos ambientes informacionais a possibilidade de responsabilização em virtude da ocorrência de incidentes de segurança deve ser explicitada em contrato ou instrumento equivalente.

[3] A área de TIC deverá manter lista de *softwares* homologados para uso no ambiente corporativo, indicando que foram avaliados e testados quanto à aderência às normas de segurança da informação e comunicação.

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

4.3.4 Gestor de Segurança da Informação e Comunicações

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

a) Promover cultura de segurança da informação e comunicação no âmbito de suas atribuições dentro do IPHAN.

b) Acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança da informação.

c) Propor recursos necessários às ações de segurança da informação.

d) Coordenar o Subcomitê de Segurança da Informação e Comunicação e a Equipe Técnica de Tratamento de Incidentes em Redes Computacionais (ETIR).

e) Realizar e acompanhar estudos de novas tecnologias no que tange aos aspectos relacionados à segurança da informação.

f) Manter contato com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República (DISC/GSI/PR).

g) Propor normas internas relativas à segurança da informação e comunicação.

4.3.5 Equipe de tratamento e resposta a incidentes em redes computacionais

São responsabilidades específicas da Equipe de Tratamento e Resposta e Incidentes em Redes Computacionais (ETIR) coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, apoiar a recuperação de sistemas, realizar análise de ataques e intrusões, cooperar com outras equipes e participar em fóruns e redes nacionais e internacionais. São **atribuições** da ETIR:

a) Gerenciar incidentes de segurança em redes computacionais;

b) Investigar e avaliar danos decorrentes de quebras de segurança;

c) Registrar todos os incidentes de segurança em redes de computadores, com a finalidade de assegurar registro histórico das atividades da ETIR;

d) Realizar tratamento da informação 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.

A estruturação da ETIR será tratada em norma complementar de forma a contemplar as exigências mínimas contidas na **Norma Complementar nº 05/IN01/DSIC/GSIPR**.

4.3.6 Subcomitê de Segurança da Informação e Comunicação

Em conformidade com a **Norma Complementar n° 03/IN01/DSIC/GSI/PR** compete ao Subcomitê de Segurança da Informação e Comunicação do IPHAN (COSEG):

a) Assessorar o órgão na implementação das ações de Segurança da Informação;

b) Constituir grupos de trabalho para de tratar temas e propor soluções específicas sobre Segurança da Informação e Comunicação;

c) Propor alterações e revisar periodicamente a Política de Segurança da Informação e Comunicações 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 e Comunicação, em conformidade com a legislação existente sobre o tema;

e) Subsidiar o Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação do IPHAN (COGESTI) nas decisões relativas à Segurança da Informação e Comunicação;

f) Propor investimentos relacionados à Segurança da Informação e Comunicação;

g) Propor procedimentos administrativos e definir medidas corretivas e punitivas cabíveis nos casos de descumprimento da Política de Segurança da Informação e Comunicações ou de suas normas e procedimentos complementares; e

h) Coordenar a Equipe Técnica de Tratamento de Incidentes em Redes Computacionais (ETIR).

O Subcomitê de Segurança da Informação e Comunicação é uma estrutura permanente formalmente instituída e subordinada ao Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação (COGESTI) do Iphan, composto pelos titulares (ou respectivos substitutos) das seguintes **áreas**:

a) Coordenação Geral de Tecnologia da Informação do Departamento de Planejamento e Administração (CGTI/DPA);

b) Coordenação Geral de Logística, Convênios e Contratos do Departamento de Planejamento e Administração (CGLOG/DPA);

c) Coordenação Geral de Gestão de Pessoas do Departamento de Planejamento e Administração (COGEP/DPA);

d) Coordenação Geral de Documentação e Pesquisa do Departamento de Articulação e Fomento (COPEDOC/DECOF).

5 Diretrizes Gerais.

5.1 Tratamento da informação

As diretrizes específicas e os procedimentos próprios de tratamento da informação corporativa serão regulamentados em norma complementar considerando as seguintes **diretrizes gerais**:

a) Documentos corporativos imprescindíveis às atividades dos usuários deverão ser salvos em **dispositivos de rede**. Os arquivos gravados localmente, nos computadores dos usuários, não serão cobertos pelo serviço de *backup* (cópias de segurança) estando sujeitos a perda e a não-recuperação.

b) Arquivos pessoais e/ou não pertinentes às atividades laborais do servidor (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os dispositivos de rede, pois podem sobrecarregar a capacidade de armazenamento e conter vulnerabilidades e riscos de segurança. Caso identificados, esses arquivos serão excluídos de forma imediata e definitiva 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 físico e lógico serão regulamentados em norma complementar considerando as seguintes **diretrizes gerais**:

a) Como condição imprescindível à concessão de acessos aos ativos de informação o usuário deverá firmar termo de compromisso de ciência das normas gerais de segurança da informação e comunicação contidas nesta política.

b) O controle de acesso deverá observar, na configuração das contas e concessão de credenciais de acesso o princípio do menor privilégio, que define que pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

c) 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.

d) Os gestores, administradores e operadores dos recursos computacionais poderão, pela característica de suas credenciais (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários – observadas as restrições quanto ao acesso à informações invioláveis e mediante estrita necessidade do serviço.

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

f) 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 Corporativo

Diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico corporativo (*e-mail*) serão regulamentados em norma complementar considerando as seguintes **diretrizes gerais**:

a) O correio eletrônico corporativo é uma **ferramenta** comunicacional de trabalho de uso obrigatório no âmbito do IPHAN.

b) O correio eletrônico corporativo é destinado para uso exclusivo em **serviço** e relacionado estritamente às atividades profissionais do usuário no âmbito desta Autarquia Federal.

c) O correio eletrônico corporativo pode ser **monitorado** a qualquer tempo pela Administração, não cabendo ao usuário do serviço alegar ofensa ao sigilo das comunicações telemáticas[5].

5.4 Serviço de *backup* e *restore*

Os procedimentos próprios ao serviço de *backup* (cópia de segurança) e *restore* (restauração de cópia de segurança) serão regulamentados em norma complementar, considerando as seguintes **diretrizes gerais**:

a) O serviço de *backup* e *restore* 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-cofre.

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*) serão

[5] Conforme Parecer n° 55/2018/PROC/PF-IPHAN/PGF/AGU.

regulamentados em norma complementar considerando as seguintes **diretrizes gerais**:

a) A administração de dados e de serviços de *data center* é tarefa tecnicamente complexa cuja gestão é competência exclusiva da área de TIC.

b) O acesso físico ao *data center* deverá ser feito por sistema de autenticação forte, mediante uso de solução de TIC adequada. 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 complementar.

d) Deverá ser executada, em frequência predeterminada, auditoria dos acessos ao *data center* – por meio de relatório do sistema de registro próprio.

e) A lista de usuários com direito de acesso ao d*ata center* deverá ser constantemente atualizada. Ocorrendo o 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*ata center* – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a *servidor público efetivo,* preferencialmente vinculado à área de infraestrutura de TIC.

5.6 Monitoramento e Auditoria do Ambiente

Para garantir a aplicação das diretrizes mencionadas nesta POSIC, 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 e Comunicações*;

c) Realizar, a qualquer tempo e sem prévio aviso, inspeções físicas nos equipamentos e instalações 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 e sem prévio aviso, qualquer *software* ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

5.7 Acesso e uso de *internet*

Diretrizes específicas e procedimentos próprios de controles de uso e acesso à *Internet* serão regulamentados 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*[6] devem, preferencialmente, ser administrados

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

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 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 e Comunicações***.**

5.8 Gestão de Riscos de SIC

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 e Comunicações. Esse processo deverá ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, 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 de Segurança da Informação**: 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 TIC**: documentação dos procedimentos e informações necessárias para que o IPHAN mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas de TIC, num nível previamente definido, em casos de incidentes.

c) **Plano de Recuperação de TIC**: documentação dos procedimentos e informações necessárias

para que o IPHAN operacionalize o retorno das atividades críticas de TIC 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 pela **ETIR** ao **Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal** (CTIR.Gov), conforme procedimentos 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 de Tratamento a Incidentes em Redes Computacionais (ETIR),** 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 computacionais, havendo indícios de ilícitos criminais, a ETIR 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 Das infrações e penalidades aplicáveis

O IPHAN, ao gerir e monitorar seus ativos de informação e comunicação, pretende garantir a integridade destes. 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 superior hierárquico.

O uso de qualquer recurso em inobservância às 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.

O **Código Penal Brasileiro** (Decreto-Lei n° 2848/1940) tipifica como crime o ato de "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (art. 154-A), assim como comete crime "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (art. 154-B).

7 Estrutura Normativa de Gestão de Segurança da Informação e Comunicações

Os documentos que comporão a estrutura normativa de gestão de Segurança da Informação e Comunicações 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 complementares – 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 complementares e na política, permitindo sua aplicação direta nas atividades cotidianas do IPHAN**.**

7.1 Divulgação e acesso à estrutura normativa

Os documentos integrantes da estrutura normativa de Gestão de Segurança da Informação e Comunicações deverão ser divulgados a todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços do IPHAN quando de sua admissão e também publicados em repositório eletrônico de documentos de maneira que seu conteúdo possa ser consultado a qualquer tempo.

7.2 Aprovação e revisão

De acordo com a **Norma Complementar nº 03/IN01/DSIC/GSI/PR** todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

Os documentos integrantes da estrutura normativa de gestão de Segurança da Informação e Comunicações do IPHAN deverão ser elaborados e aprovados pelas seguintes **instâncias competentes**:

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

CATEGORIA	NÍVEL DE APROVAÇÃO
POLÍTICA DE SIC	Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação
NORMAS COMPLEMENTARES DE SIC	Subcomitê de Segurança da Informação e Comunicação

Sempre que algum fato ou evento relevante motive, o prazo revisional estabelecido poderá ser antecipado conforme análise das partes competentes.

8 Referências Legais e Normativas

Tabela 3: Referências legais e normativas.

CLASSIFICAÇÃO	IDENTIFICAÇÃO	DATA	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.
Lei Federal	12.737/2012	30/11/2012	Dispõe sobre a tipificação criminal de delitos informáticos.
Lei Federal	12.965/2014	23/04/2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
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.
Instrução Normativa	04/2014/SLTI/MP	11/09/2014	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
Instrução Normativa	05/2017/SEGES	26/05/2017	Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.
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.
Portaria	235/2010/IPHAN	20/07/2010	Institui o Comitê Gestor de Tecnologia da Informação do IPHAN (COGESTI).

Portaria	92/2012/IPHAN	05/07/2012	Aprova o Regimento Interno do Instituto do Patrimônio Histórico e Artístico Nacional.
Portaria	104/2014/IPHAN	02/07/2014	Instituiu o comitê de SIC do Iphan, como estrutura de caráter permanente subordinada ao COGESTI.
Portaria	424/2017/IPHAN	13/11/2017	Aprova as alterações e a revisão do regimento interno do Comitê Gestor dos Recursos de Tecnologia da Informação e Comunicação do Iphan (COGESTI).

9 Disposições Finais

Para a uniformização da informação organizacional, esta Política de Segurança da Informação e Comunicações (POSIC) 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 preceitos e requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação e Comunicações constitui **violação às regras internas** da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.