



Fundação 193

INSTITUIÇÃO DE APOIO AO CBMDF



POLÍTICA DE GESTÃO E SEGURANÇA DA INFORMAÇÃO



POLÍTICA DE GESTÃO E SEGURANÇA DA INFORMAÇÃO

Dispõe sobre as
diretrizes da Política de
Gestão e Segurança da
Informação.

**Brasília/DF
Julho/2025**

SUMÁRIO

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

- Seção I – Dos objetivos
- Seção II – Da abrangência
- Seção III – Das referências
- Seção IV – Das definições
- Seção V – Dos princípios
- Seção VI – Das responsabilidades

CAPÍTULO II – DIRETRIZES DO SISTEMA DE GESTÃO E SEGURANÇA DA INFORMAÇÃO

- Seção I – Da garantia e do controle de acesso
- Seção II – Da segurança física e do ambiente de recursos humanos
- Seção III – Do plano de continuidade
- Seção IV – Da conformidade
- Seção V – Da gestão de riscos de segurança da informação e da gestão de incidentes
- Seção VI – Da segurança em Tecnologia da Informação
- Seção VII – Da conscientização e capacitação

CAPÍTULO III – GESTÃO DOCUMENTAL

- Seção I - Programa de Gestão Documental

CAPÍTULO IV – DISPOSIÇÕES FINAIS

- Seção I – Das penalidades
- Seção II - Disposições finais

O Conselho de Curadores da Fundação 193, no uso das atribuições que lhe confere o inciso II do art. 18º do Estatuto e o inciso II do art. 25º do Regimento Interno, resolve:

Art. 1º. A Fundação de Apoio ao CBMDF, denominada Fundação 193, implementará práticas relacionadas à gestão e à segurança da informação.

Parágrafo Único. A Política de Gestão e Segurança da Informação traz diretrizes para o estabelecimento, implementação, operacionalização, monitoramento, manutenção e melhoria da proteção dos ativos de informação com base na avaliação dos riscos inerentes à gestão e à segurança da informação e com vistas a alcançar os objetivos propostos pela Fundação 193.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

Dos objetivos

Art. 2º. A Política de Gestão e Segurança da Informação tem por objetivo estabelecer princípios, responsabilidades e competências relativas à gestão e à segurança da informação, assegurando a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações, bem como minimizar os riscos de falhas, danos, acessos indevidos ou prejuízos que possam comprometer a continuidade do fluxo de informações.

Art. 3º. As diretrizes da Gestão da Informação visam preservar as informações relacionadas à imagem, à memória e aos objetivos estratégicos da Fundação 193, trazendo orientações gerais para a

estruturação do processo de gestão de documentos e para a proteção das informações custodiadas pela Fundação nos aspectos relativos ao ambiente de produção, tramitação e guarda de documentos.

§ 1º A produção, tramitação e guarda da informação deverá ser realizada com eficiência e eficácia, de modo seguro e transparente, alinhadas aos requisitos legais e exigências dos órgãos reguladores e fiscalizadores.

§ 2º A Gestão da Informação contemplará os critérios e procedimentos para a preservação física e digital do acervo institucional.

Art. 4º. As diretrizes da Segurança da Informação buscam proteger os ativos de informação independentemente de onde eles se encontrem, com vistas ao resguardo de sua integridade, confidencialidade, disponibilidade e autenticidade, protegendo as informações produzidas e custodiadas pela Fundação nos aspectos relativos ao ambiente físico e de tecnologia da informação.

Seção II

Da abrangência

Art. 5º. As disposições desta Política aplicam-se a todos os dirigentes, gestores, empregados e demais usuários que tenham acesso a informações e documentos, bem como ao ambiente de tecnologia da informação da Fundação 193.

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos e humanos.

Seção III

Das referências

Art. 6º. Devem ser utilizados como instrumentos de boas práticas técnicas e gerenciais, no que couber, as seguintes referências:

- I. Norma ABNT NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação;
- II. Norma ABNT NBR/ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de práticas para Controles e Segurança da Informação;
- III. Norma ABNT NBR/ISO 27005:2023 – Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação;
- IV. Guia de boas práticas em contratação de soluções de tecnologia da informação – Tribunal de Contas da União. Brasília, 2012;
- V. Código de Ética e de Conduta da Fundação 193;
- VI. Glossário de Documentos Arquivísticos Digitais. Conselho Nacional de Arquivos (CONARQ) – 8ª versão – 2020.

Seção IV

Das Definições

Art. 7º. Para fins desta Política, entende-se por:

- I. ASSINATURA DIGITAL: método de autenticação de informação digital tipicamente tratada como substituta à assinatura física;
- II. ATIVOS DE INFORMAÇÃO: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio da Fundação 193;

- III. AUTENTICIDADE: garante a identidade de quem envia a informação e a veracidade da fonte da informação;
- IV. CERTIFICADO DIGITAL: assinatura com validade jurídica que garante proteção às transações eletrônicas e outros serviços via internet, permitindo que pessoas e empresas se identifiquem e assinem digitalmente com segurança e agilidade;
- V. CONFIDENCIALIDADE: garantia de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- VI. CONTROLE DE ACESSO: processo computacional para autenticação da credencial de um integrante, autorizando o uso do recurso com base no seu perfil de acesso;
- VII. DADO: matéria-prima da informação, que isoladamente transmite uma mensagem ou representa algum conhecimento;
- VIII. DIRIGENTES: Diretores, Conselheiros Curadores e Fiscais e membros dos Comitês de Assessoramento Técnico da Fundação 193;
- IX. DISPONIBILIDADE: Garantia de que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário;
- X. DOCUMENTO: unidade de registro de informações, qualquer que seja o suporte ou formato;
- XI. EMPREGADOS: pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho;
- XII. COLABORADOR: pessoas devidamente cadastradas, que colaboraram de forma voluntária com suas habilidades, conhecimentos e atitudes na realização dos objetivos da Fundação;
- XIII. PRESTADOR DE SERVIÇO OU TERCEIRO: Parte contratada que tem acesso às instalações, recursos e informações necessárias para o

cumprimento de suas obrigações profissionais. Fazem parte dessa categoria: autônomos, terceiros, contratados diretos, cooperativas, pessoa jurídica ou pessoa física, subcontratado, terceirizado e quarteirizado.

XIV. FALHAS NA SEGURANÇA DA INFORMAÇÃO: causa potencial de um incidente ou fragilidade na gestão da segurança que pode resultar em dano para o fluxo de informação da Fundação;

XV. GESTÃO DA INFORMAÇÃO: diz respeito ao ciclo de atividade organizacional: a aquisição de informações a partir de uma ou mais fontes, a custódia e a trâmite de informações e a sua melhor disposição por meio de arquivamento ou eliminação;

XVI. GESTORES: diretores e coordenadores da Fundação 193;

XVII. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação;

XVIII. INFORMAÇÃO: todo o conjunto de dados devidamente ordenados e organizados de forma a terem significado;

XIX. INFORMAÇÕES CUSTODIADAS: informações sob a responsabilidade da Fundação 193 cedidas pelo seu proprietário em razão de contrato, acordo, convênio ou ajuste;

XX. INFORMAÇÃO PÚBLICA: refere-se à informação publicamente acessível, cuja utilização não infringe qualquer direito legal, ou qualquer obrigação de confidencialidade;

XXI. INFORMAÇÃO NÃO-PÚBLICA: aquela imprescindível à segurança das atividades da Fundação, e que diga respeito à intimidade, vida privada, honra e imagem, bem como que se enquadre nas hipóteses de sigilo previstas em legislação específica;

XXII. INTEGRIDADE: garantia de que o conteúdo da informação não sofreu violação ou alteração de maneira indevida;

XXIII. MEMÓRIA INSTITUCIONAL: conjunto de informações e documentos que caracterizam a identidade e a cultura organizacional;

XXIV. PARTES ENVOLVIDAS: participantes, assistidos, beneficiários, patrocinadores, conselheiros deliberativos e fiscais, membros de comitês de assessoramento técnico, diretores, gerentes, coordenadores, empregados e colaboradores, sociedade, prestadores de serviços, bem como entidades ligadas à Fundação 193;

XXV. RECURSOS COMPUTACIONAIS: conjunto de *hardware* e *software* em que dados e informações são processados, armazenados ou transmitidos;

XXVI. RISCOS DE SEGURANÇA: probabilidade da ocorrência de um incidente de segurança da informação ponderado com o respectivo impacto;

XXVII. SEGURANÇA DA INFORMAÇÃO: visa garantir a integridade, a confidencialidade, a acessibilidade e a autenticidade das informações, bem como minimizar os riscos de falhas, danos, acessos indevidos ou prejuízos que possam comprometer a continuidade do fluxo de informações;

XXVIII. SEGURANÇA FÍSICA E PATRIMONIAL: visa prevenir danos e interferências nas instalações da Fundação 193 que possam causar perda, roubo ou comprometimento das informações;

XXIX. SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO: serviços disponíveis na rede corporativa, acessíveis por meio de credencial da rede, tais como intranet, internet, correio eletrônico, servidor de arquivos e sistemas corporativos;

XXX. SIGILO: propriedade de que a informação não seja revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XXXI. TERMO DE RESPONSABILIDADE DE ACESSO: instrumento a ser assinado por todos os usuários, em que dão ciência sobre as diretrizes da Política de Gestão e Segurança da Informação e se responsabilizam pelo acesso e uso dos recursos computacionais da Fundação 193; e

XXXII. USUÁRIOS: pessoa que utiliza bem ou serviço da Fundação 193, utilizando ferramentas ou dispositivos para se comunicar com os outros, escrever, disponibilizar ou publicar documentos; e

XXXIII. VIOLAÇÃO DA SEGURANÇA DA INFORMAÇÃO: qualquer fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.

Seção V

Dos princípios

Art. 8º. As ações relacionadas com a gestão e com a segurança de informação da Fundação 193 serão norteadas pelos seguintes princípios:

- I. CELERIDADE: oferecer respostas rápidas a incidentes e falhas de gestão e segurança da informação;
- II. CLAREZA: as regras, documentações e comunicações devem ser precisas, concisas e de fácil entendimento;
- III. CONTINUIDADE DAS ATIVIDADES: o serviço prestado pela Fundação 193 não pode sofrer interrupções repentinas e continuadas;
- IV. EFICÁCIA: relação entre os resultados alcançados e os planejados;
- V. EFICIÊNCIA: a adequação dos custos das ações de segurança da informação e comunicação ao valor das informações a serem protegidas;

- VI. ÉTICA: refere-se aos princípios morais, sendo pré-requisito e suporte para a geração de confiança
- VII. LEGALIDADE: ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, políticas e normas organizacionais, administrativas, técnicas e operacionais da Fundação 193;
- VIII. PESSOALIDADE: acesso aos ativos da informação é pessoal e intransferível;
- IX. UTILIDADE DO ACESSO AOS ATIVOS DE INFORMAÇÃO: deve ser concedido de acordo com a utilidade para o usuário e preservado com sigilo;
- X. PRIVACIDADE: garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais além da preservação da imagem da Fundação 193 e de suas partes envolvidas;
- XI. PUBLICIDADE: transparência no trato da informação, observados os critérios legais; e
- XII. RESPONSABILIDADE: usuário é responsável pelos atos que comprometam a segurança dos ativos de informação.

Seção VI

Das responsabilidades

Art. 9º. A gestão e segurança da informação da Fundação 193 será exercida conforme a seguir:

- I. CONSELHO DE CURADORES: responsável por aprovar a Política de Gestão e Segurança da Informação, e proporcionar as condições necessárias para o adequado gerenciamento documental;

- II. DIRETORIA EXECUTIVA: responsável por aprovar o Programa de Gestão Documental e zelar pelo cumprimento da Política de Gestão e Segurança da Informação;
- III. COMITÊ DE COMPLIANCE: órgão consultivo composto pelas Diretorias vinculadas à Diretoria Executiva, responsável por propor ações de implementação da gestão eletrônica de documentos e acompanhar a gestão integrada da informação, promovendo o intercâmbio entre as diversas áreas da Fundação;
- IV. DIRETORIA DE PROJETOS: responsável pela conformidade e pelo acompanhamento e implementação do Programa de Gestão Documental da Fundação 193, tratando da gestão da informação no que se refere ao acesso, à tramitação eficiente dos documentos, ao arquivamento e à preservação da memória institucional;
- V. DIRETORIA DE TECNOLOGIA E INOVAÇÃO: responsável por gerenciar o Arquivo Digital, por promover a cultura da Segurança da Informação Tecnológica, bem como por gerir as regras de proteção dos equipamentos de infraestrutura tecnológica, propondo a revisão nas respectivas normas;
- VI. DIRETORIA ADMINISTRATIVA: responsável pela segurança física e patrimonial das instalações da Fundação e pela gestão integrada do Protocolo Geral e do Arquivo Central;
- VII. DIRETORIA DE COMUNICAÇÃO: responsável pela divulgação interna e externa das informações, de acordo com as diretrizes da Fundação 193, bem como de acordo com o previsto no Plano Estratégico Institucional e no Plano de Ação Anual da Fundação 193;
- VIII. ÁREAS GESTORAS: responsáveis por gerenciar o cumprimento desta Política no âmbito de sua Gerência, bem como manter a área de

tecnologia informada acerca dos níveis de acessos referentes aos usuários sob sua supervisão; e

IX. USUÁRIOS: responsáveis pelo cumprimento desta Política e demais normativos relacionados à gestão e à segurança da informação, por meio do uso de forma responsável, profissional, ética e legal dos ativos de informação, respeitando os direitos e as permissões de uso concedidas pela Fundação 193.

CAPÍTULO II

DIRETRIZES DO SISTEMA DE GESTÃO E SEGURANÇA DE INFORMAÇÃO

Seção I

Da garantia e do controle de acesso

Art. 10. Qualquer falha na segurança da informação relacionada à garantia ou ao controle de acesso aos sistemas tecnológicos identificada por qualquer usuário, deve ser imediatamente comunicada ao seu superior imediato, que a encaminhará à Diretoria de Tecnologia e Inovação para avaliação e determinação das ações que se fizerem necessárias.

Art. 11. O acesso aos Sistemas de Informação da Fundação 193 deve ser controlado de acordo com o valor, sensibilidade, criticidade da informação, e deve considerar aspectos de restrições legais e normativas.

Art. 12. O processo de controle de acesso à informação tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

§ 1º O acesso às informações não-públicas produzidas ou custodiadas pela Fundação 193 deve permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso a informações não-públicas por quaisquer usuários é condicionado ao aceite de termo de sigilo e responsabilidade.

Art. 13. Todos os usuários que manipulem ou tenham acesso a informações sob custódia ou de propriedade da Fundação 193, devem garantir a confidencialidade e o sigilo dessas informações, de acordo

com os requisitos legais, de negócio e de segurança da informação disciplinados em normativos específicos.

Parágrafo único. Deve-se adotar comportamento seguro, evitando assuntos sigilosos em ambientes sociais e particulares, impressão, transmissão, compartilhamento e transporte para fora das instalações da Fundação 193 de informação sem autorização.

Art. 14. As violações de segurança da informação devem ser comunicadas à Diretoria Administrativa e devidamente registradas, sendo analisadas periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

Art. 15. A Fundação deve estabelecer em seus contratos, acordos, convênios ou ajustes, cláusulas específicas sobre sigilo, em especial quando informações forem disponibilizadas à terceiros, que assegurem a observância desta Política e suas normas.

Seção II

Da segurança física e do ambiente

Art. 16. A segurança física e patrimonial, disposta em normativo específico, tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações da Fundação 193 que possam causar perda, roubo ou comprometimento das informações.

Parágrafo único. Compete à Diretoria Administrativa planejar, estabelecer, monitorar e revisar periodicamente os procedimentos de segurança física da Fundação 193.

Art. 17. Para garantir a segurança física e do ambiente, serão estabelecidos, no mínimo, os seguintes controles:

- I. prevenir o acesso físico indevido e sem autorização, bem como danos e interferências nas instalações e informações da Fundação 193;
- II. assegurar que dirigentes, gestores, empregados e quaisquer outros usuários da Fundação entendam suas responsabilidades e assinem termos de segurança da informação, com a finalidade de reduzir os riscos de burla, erros humanos, furto, roubo, fraude ou uso indevido dos ativos de informação da Fundação 193; e
- III. realizar reuniões com pessoas alheias ao quadro funcional da Fundação em salas adequadas, evitando, quando aplicável, o trânsito indevido de pessoas no ambiente operacional de trabalho.

Seção III

Do plano de continuidade

Art. 18. Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos de forma a não permitir a interrupção das atividades de negócios e a proteger os processos críticos contra falhas e danos, devendo atender aos seguintes objetivos:

- I. avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços;
- II. contingência e recuperação do funcionamento normal dentro de períodos de tempo determinados; e
- III. recuperação tempestiva das operações consideradas vitais.

Seção IV

Da conformidade

Art. 19. Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto à disponibilização de informações, bem como ao uso e disseminação de informações protegidas por leis tais como: dados pessoais, informações relativas à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais, patentes e marcas registradas ou aquelas classificadas como sigilosas.

Art. 20. Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com a legislação e com os normativos internos da Fundação 193.

Art. 21. Os Sistemas de Informação da Fundação 193, além de disponibilizar os registros em prazos e formatos que atendam às exigências legais, devem protegê-los contra perda, acesso indevido, destruição e falsificação, visando à salvaguarda dos dados.

Seção V

Da gestão de riscos de segurança da informação e da gestão de incidentes

Art. 22. A gestão de riscos e incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

Parágrafo único. Os dirigentes, gestores, empregados e quaisquer outros usuários da Fundação são responsáveis por:

- I. informar imediatamente à Diretoria de Tecnologia e Inovação os incidentes com a segurança da informação de que tenham ciência ou suspeita;
- II. colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação.

Seção VI

Da segurança em Tecnologia da Informação

Art. 23. Compete à Diretoria de Tecnologia e Inovação monitorar e revisar periodicamente os procedimentos acerca do uso de recursos de Tecnologia da Informação, controle de acesso, e-mail, uso da internet, uso de antivírus, acesso remoto e acesso a serviços de Tecnologia da Informação por fornecedores.

Parágrafo Único. Deverão ser adotadas medidas preventivas e de proteção contra acesso tecnológico indevido (intrusão) e ataques cibernéticos, a serem disciplinadas por normativo específico.

Art. 24. A assinatura digital de documentos deve ser realizada preferencialmente por meio de certificado digital, sendo permitida a utilização de usuário (*login*) e senha fornecidos mediante procedimento de cadastro no qual esteja assegurada a adequada identificação do interessado.

§ 1º O procedimento de cadastro tratado no *caput* deste artigo deverá ser regulamentado em ato normativo próprio, devendo envolver, no mínimo:

- I. endereço eletrônico para realização de cadastro do interessado;
- II. endereço da unidade responsável pela validação presencial dos documentos exigidos;

- III. informações sobre procedimentos para alteração e redefinição de senha de acesso, em caso de perda;
- IV. informações sobre a responsabilidade do usuário quanto a guarda e sigilo da senha de acesso; e
- V. informações sobre regras de cancelamento e bloqueio dos usuários.

Seção VII

Da conscientização e capacitação

Art. 25. As diretrizes básicas da Política de Gestão e Segurança da Informação devem ser divulgadas pelos meios e formas de comunicação adotados pela Fundação, garantindo que todos tenham consciência de seu conteúdo e as pratiquem.

Art. 26. Os dirigentes, gestores, empregados e demais usuários devem ser continuamente capacitados sobre o uso dos ativos de informação por ocasião da realização de suas atividades.

Art. 27. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado e com as demais que porventura venham a ser adotadas.

CAPÍTULO III

GESTÃO DOCUMENTAL

Art. 28. De forma complementar à Política de Gestão e Segurança da Informação, a Diretoria Executiva da Fundação 193, fixará em ato normativo como deverá ser realizada a gestão documental bem como sua classificação e temporalidade.

Art. 29. Compete a todos gestores, empregados e colaboradores que tenham acesso a informações da Fundação 193, executar os procedimentos relativos à gestão dos acervos sob sua responsabilidade:

- I. protocolar, tramitar e controlar os documentos produzidos e recebidos no âmbito de sua área de atuação;
- II. aplicar a gestão documental definida pela Diretoria Executiva;
- III. proceder à avaliação e tramitação dos documentos;
- IV. atender às solicitações de consulta e empréstimo dos documentos sob sua guarda; e
- V. preservar os documentos produzidos e recebidos no desempenho das funções e atividades da Fundação.

Parágrafo Único. O uso e manutenção de dados, documentos e informações digitais de conteúdo institucional devem ser armazenados nos servidores de rede, observando os padrões de arquivamento digital estabelecidos em normativo específico.

Seção I

Programa de Gestão Documental

Art. 30. O Programa de Gestão Documental da Fundação, a ser proposto no âmbito do Comitê de Gestão Documental, tem por objetivo a implementação de sistema tecnológico e de ações relativas à produção, recebimento, assinatura e tramitação de documentos eletronicamente,

bem como organizar o Protocolo Geral e o Arquivo Central de documentos, devendo disciplinar no mínimo:

- I. Recuperação da informação, com a verificação da pontualidade em que documentos e informações são acessados pelos funcionários da Fundação para execução dos seus processos de negócio;
- II. Segurança da informação, com a análise das vulnerabilidades que os sistemas (informatizados ou não) apresentam em relação à custódia e acesso à informação;
- III. Estudo de usuários, com a verificação de necessidades informacionais dos empregados da Fundação 193 para a execução dos seus processos de negócio durante a rotina de trabalho;
- IV. Preservação e conservação de documentos, com a análise de diretrizes e ações da Fundação em relação à integridade e manutenção de seus acervos; e
- V. Memória institucional, com a verificação de riscos em relação a informações e documentos que caracterizam a identidade e a cultura organizacional.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Seção I

Das penalidades

Art. 31. O descumprimento das disposições constantes nesta Política de Gestão e Segurança da Informação e nas normas complementares sobre gestão e segurança da informação caracteriza infração funcional, a ser apurada em procedimento administrativo disciplinar e civil, sem prejuízo a responsabilidade penal.

Seção II

Disposições finais

Art. 32. Todos os procedimentos referentes à Política de Gestão e Segurança da Informação adotados pela Fundação 193 deverão ser publicados para conhecimento de seus usuários.

Art. 33. As informações produzidas e as soluções tecnológicas desenvolvidas por quaisquer usuários da Fundação 193, no exercício de suas atribuições, são patrimônio intelectual da Fundação e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento da autoria, se for o caso.

Art. 34. Os casos não previstos e as dúvidas surgidas na aplicação desta Política serão submetidos à Diretoria Executiva após análise da Diretoria de Projetos.

Art. 35. À Diretoria Executiva caberá editar normas e orientações complementares que se fizerem necessárias à execução do disposto nesta Política.

Art. 36. Esta Política entra em vigor na data de sua publicação.