PALMARES
FUNDAÇÃO CULTURAL

PORTARIA Nº 207 DE 23 DE DEZEMBRO DE 2009

Dispõe sobre as Diretrizes Básicas de Segurança da Informação no âmbito da Fundação Cultural Palmares.

**O PRESIDENTE DA FUNDAÇÃO CULTURAL PALMARES**, no uso de suas atribuições que lhe confere o art. 18 do Decreto nº 6.853 de 15 de maio de 2009, publicado no DOU de 18 de maio de 2009, e CONSIDERANDO a necessidade de instituir Política de Segurança da Informação no âmbito da Fundação; **Resolve**:

Art. 1º. Dispor sobre as Diretrizes Básicas da Política de Segurança da Informação da Fundação Cultural Palmares – FCP.

Parágrafo único. As ações a serem implementadas com base nas Diretrizes Básicas da Política de Segurança da Informação estabelecidas neste documento são a salvaguarda dos dados, informações e materiais sigilosos de interesse da FCP e do Estado Brasileiro, bem como dos sistemas computacionais e as áreas e instalações onde tramitam, além da preservação da inviolabilidade e da intimidade da vida privada, da honra e da imagem das pessoas.

## Título I
## Das Disposições Gerais

### Capítulo I
### Do Escopo

Art. 2º. As Diretrizes Básicas da Política de Segurança da Informação da FCP referem-se:

I – aos aspectos estratégicos, estruturais e organizacionais, preparando a base para a elaboração dos demais documentos normativos que as incorporarão;

II – procedimentos, processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços ofertados pela Tecnologia da Informação.

## Capítulo II
## Das Responsabilidades

Art. 3º. As diretrizes, normas e procedimentos de segurança deverão ser cumpridos por todos os usuários, nos termos desta Política.

Parágrafo único: O não cumprimento das determinações da Política de Segurança da Informação sujeitará o infrator às penalidades previstas em lei.

Art. 4º. A Coordenação Geral de Gestão Interna tem as seguintes responsabilidades relacionadas à Política de Segurança:

I – Supervisão, atualização e revisão da Política de Segurança da FCP;

II – Análise, aprovação, acompanhamento e avaliação dos programas, planos, projetos e ações de segurança da FCP.

Art. 5º. A Divisão de Tecnologia da Informação tem as seguintes responsabilidades:

I – Proposição de diretrizes, normas e procedimentos de segurança da informação para a FCP;

II – Planejamento, coordenação e execução de programas, planos, projetos e ações de segurança na FCP;

III - Supervisão, análise e avaliação da efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação da FCP;

IV– Recepção, organização, armazenamento e tratamento adequado de todas as informações de eventos e incidentes de segurança no ambiente da FCP;

V – Relato de ocorrências, eventos e incidentes de segurança da informação, na forma de relatório detalhado e circunstanciado, ao dirigente da Coordenação Geral de Gestão Interna;

VI – Coordenação e acompanhamento de auditorias de segurança da informação da FCP.

Art. 6º. O Chefe da Divisão de Tecnologia da Informação tem as seguintes responsabilidades:

I – Homologação e autorização do uso de sistemas de processamento de informações no ambiente operacional da DTI;

II – Suspensão, a qualquer tempo, de acesso do(s) usuário(s) a recursos computacionais da FCP, quando evidenciados os riscos à segurança da informação, informando todos os incidentes a Coordenação Geral de Gestão Interna.

Parágrafo único: Caberá à Divisão de Tecnologia da Informação, a responsabilidade pela verificação e o cumprimento, com efetividade, da Política de Segurança da Informação.

## Capitulo III
## Da Conceituação

Art. 7º. Com o objetivo de esclarecer os conceitos de termos utilizados nesta Política de Segurança que possam gerar dificuldades de interpretação ou significados ambíguos, as seguintes definições são aplicadas:

I – Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

II – Classificação: processo que identifica informações de acordo com o seu valor, permitindo estabelecer o nível de segurança adequado para cada tipo de informação e decidir que controles e procedimentos são necessários para a seleção, tratamento, transmissão, armazenamento e descarte dessas informações.

III – Criticidade: grau de importância da informação para a continuidade dos negócios da Fundação (disponibilidade e integridade).

IV – Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

V – Gestor: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir ou alterar a sua classificação nos graus de sigilo, criticidade e perfil de acesso dos demais usuários e processos.

VI – Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

VII – Ativo: além da própria informação, todo o recurso utilizado para o seu tratamento, tráfego e armazenamento. São exemplos de ativos associados com sistemas de informação: base de dados e arquivos, documentação de sistema, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, softwares, sistemas, ferramentas de desenvolvimento e utilitários, estações de trabalho, servidores de rede, equipamentos de comunicação (roteadores, switches etc.).

VIII – Usuário: órgãos e servidores públicos, empregados, agentes públicos, consultores, estagiários, entidades não-governamentais e empresas privadas que utilizem, de forma autorizada, informações da FCP.

IX – Informação: 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.

X – Informação confidencial: aquelas cujo conhecimento e divulgação possam ser prejudiciais ao interesse do País.

XI – Informação Reservada: aquelas que não devam, imediatamente, ser do conhecimento do público em geral.

XII – Informação Pública ou Ostensiva: aquelas cujo acesso é irrestrito, disponível para divulgação pública através de canais autorizados pela entidade gestora.

XIII – Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

XIV – Acesso Privilegiado: é aquele que permite ao usuário sobrepor controles do sistema de informação, e somente deve ser concedido àqueles que o necessitam para a condução de suas atividades.

XV – Administrador de Serviços: usuário que possui acesso privilegiado para a utilização e disponibilização por força de suas funções, de recursos restritos de Tecnologia da Informação.

XVI – Medidas de Proteção: medidas destinadas a garantir o sigilo, a inviolabilidade, a integridade, a autenticidade, a legitimidade e a disponibilidade dos dados e informações com o objetivo de prevenir, detectar, anular ou registrar ameaças reais ou potenciais a dados e informações.

XVII – Não-repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

XVIII – Plano de Contingência: descreve as ações que uma organização deve tomar para assegurar a continuidade dos processos críticos em caso de falhas nos sistemas, incluindo a ativação de processos manuais, duplicidade de recursos e acionamento de fornecedores.

XIX - Termo de Responsabilidade: acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao usuário e Administrador de Serviço quanto ao sigilo e a correta utilização dos ativos de propriedade da FCP.

## Título II
## Das Diretrizes

### Capítulo IV
### Da Amplitude

Art. 8º. Conjunto de medidas de proteção que têm como objetivo garantir a aplicação dos Princípios de Segurança da Informação.

I – A segurança é direcionada contra a destruição, modificação ou divulgação indevida das informações, quer acidental ou intencional, e no impedimento de fraudes.

II – A informação deve ser tratada como um patrimônio, devendo ser protegida no acesso, tráfego, uso e armazenamento, de acordo com sua classificação em graus de confidencialidade e criticidade.

III – Toda a informação deve ter uma classificação que defina seu grau de confidencialidade e criticidade para a FCP, para o Estado e para as pessoas.

IV – Todos os mecanismos de proteção utilizados para a segurança das informações da FCP devem ser mantidos para preservar a continuidade de seus negócios.

V – As diretrizes são destinadas a preservar a credibilidade e o prestígio da Instituição na prestação dos seus serviços.

VI – A Política de Segurança deve ser conhecida e seguida por todos os usuários da FCP.

VII – Os diversos níveis gerenciais devem zelar pelo cumprimento destas Diretrizes de Segurança da Informação no âmbito de sua competência.

VIII – Registros e informações sigilosas devem ser protegidos contra perda, destruição e falsificação, sendo retidos de forma segura para atender requisitos legais e regulamentares.

IX – O cumprimento das normas de Segurança da Informação da FCP será auditado periodicamente, de acordo com os critérios definidos pela Divisão de Tecnologia da Informação.

X – As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança.

## Capítulo V
## Dos Requisitos

Art. 9º. A Política de Segurança da Informação deverá atender aos requisitos preconizados, em conformidade com:

I – Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II – Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a Proteção da Propriedade Intelectual do Programa de Computador;

III – Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

IV – Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

V – Lei nº 3.505. de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VI – Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

VII – NBR/ISO/IEC 27001:2006 - Sistemas de Gestão de Segurança da Informação.

## Capítulo VI
## Da Divulgação e Cumprimento

Art. 10º. A Política de Segurança da Informação será divulgada entre todas as Unidades Organizacionais da Fundação Cultural Palmares e cumprida por todos os seus usuários.

## Capítulo VII
## Da Capacitação e do Aperfeiçoamento

Art. 11º. Todos os usuários deverão ser continuamente capacitados para a utilização dos recursos de Tecnologia da Informação quando da realização de suas atividades.

Art. 12º. Os treinamentos a serem disponibilizados estarão compatíveis com as tecnologias atualmente implementadas no ambiente informatizado, e com as demais tecnologias que porventura venham a ser adotadas.

## Capítulo VIII
## Do Acesso, Proteção e Guarda da Informação

Art. 13º. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela FCP, é considerada como patrimônio da Fundação, e deve ser protegida conforme estabelecido na Política de Segurança da Informação.

Art. 14º. Todas as falhas de segurança da informação devem ser imediatamente relatadas pelos usuários à Chefia Imediata, que deverá encaminhar à Coordenação-Geral de Gestão Interna – CGGI para avaliação e determinação das providências que se fizerem necessárias.

Art. 15º. Todos os usuários que manipulem ou tenham acesso a informações sigilosas de propriedade da FCP, devem assinar termo de responsabilidade, que tem como objetivo garantir a confidencialidade e não-divulgação das informações.

## Capítulo IX
## Da Utilização de Recursos

Art. 16º. Os recursos disponibilizados são fornecidos com o propósito de garantir o desempenho de atividades pertinentes a FCP, sendo vedado aos usuários à utilização destes recursos para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a quaisquer pessoas físicas ou jurídicas, veicular opiniões discriminatórias e partidárias, ou qualquer outras atividades que contrariem os objetivos institucionais da Fundação.

Art. 17º. Todos os acessos à rede de dados da FCP serão gerenciados em todos os tipos de conexão, devendo os usuários ser identificados e ter acesso apenas às informações e aos recursos tecnológicos necessários ao desempenho de suas atividades.

Art. 18º. Todos os ativos empregados em Tecnologia da Informação na FCP serão inventariados, devendo-se identificar seus responsáveis, bem como definir suas configurações, manutenções e documentações que são pertinentes.

## Capítulo X
## Da Comunicação Eletrônica

Art. 19º. Toda a informação veiculada eletronicamente na infra-estrutura da FCP poderá ser controlada e monitorada.

Parágrafo único. A Política de Segurança da Informação deverá prever mecanismos que venham a garantir a proteção das informações quanto a questão de autenticação.

## Capítulo XI
## Da Tecnologia

Art. 20º. Todos os recursos de Tecnologia da Informação devem ser protegidos e conservados com o objetivo de preservar seus componentes internos e externos.

## Capítulo XII
## Da Segurança Física

Art. 21º. Como forma para restringir o acesso físico de pessoas não autorizadas às instalações da FCP, diversos controles serão estabelecidos.

Art. 22º. Todas as movimentações de equipamentos de informática serão devidamente informadas a Coordenação de Logística e registradas.

## Capítulo XIII
## Do Plano de Contingência

Art. 23º. Serão mantidos procedimentos que garantam a continuidade e a recuperação do fluxo de informações, observando as classificações de disponibilidades requeridas, de forma a não permitir a interrupção das atividades de negócio e proteger os processos críticos contra falhas e danos, devendo os mesmos atingir os 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 tempos determinados; e,

III – recuperação tempestiva das operações consideradas vitais para a FCP.

# Título IV
# Das Disposições Finais

## Capítulo I
## Da Avaliação e da Regulamentação

Art. 24º. O cumprimento desta Política será avaliado periodicamente, de acordo com

os critérios da Coordenação Geral de Gestão Interna.

Art. 25º. Fica a Divisão de Tecnologia da Informação - DTI autorizada a regulamentar os procedimentos necessários para a aplicação das disposições estabelecidas nesta Política.

Art. 26º. Esta Portaria entra em vigor na data de sua publicação.

**EDVALDO MENDES ARAÚJO**
**(Zulu Araújo)**

**B.A nº 12 de 31.12.2009**